OPEN MARKETS INSTITUTE

AI in the Public Interest: Confronting the Monopoly Threat

NOVEMBER 2023

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

AUTHORS:

Barry Lynn, Max von Thun, Karina Montoya

EDITOR:

Anita Jain

CONTRIBUTORS:

Philip Longman, Courtney Radsch, Daniel Hanley, Ezmeralda Makhamreh

SPECIAL THANKS TO:

Ian Brown, Amba Kak, Michelle Meagher, Johnny Ryan, Nicolas Moës, Nick Shaxson, Kris Shrishak, Matthias Spielkamp, Andrew Strait, Sarah West

EXECUTIVE SUMMARY

Since bursting into public view a year ago when OpenAI released its ChatGPT generative AI "chatbot," the latest generation of Artificial Intelligence (AI) technologies has been celebrated by many observers as a revolutionary breakthrough in computing. Boosters have claimed that AI will accelerate drug discovery, help reduce carbon emissions, improve government efficiency, improve the quality of work, and help us manage our finances. They have told us to envision AI as our personal online agent, mental health aide, friend, even digital lover, ever vigilant for our welfare. And that's just for starters. Many of the most profound changes of the age of AI, we are assured, have yet even to be imagined.

Many others, including leading technologists, loudly warn that AI also or even mainly poses extreme, even existential, threats to individuals and society as a whole. These include disrupting democracy through misinformation and propaganda, starving the free press and warping public debate, the theft of the properties and ideas of independent businesses and individual creators, increased levels of digital addiction and depression, and the manipulation and exploitation of individuals as they seek to do business with one another or simply get through their lives. Others, meanwhile, warn of mass unemployment and the wholesale destruction even of many high-skilled jobs, including those of writers, computer coders, and doctors. Some respected experts believe AI poses grave threats to national security, especially when put to use by the Chinese state. Recently a group of industry leaders said AI may even pose a "risk of extinction" akin to pandemics and nuclear weapons.

Governments around the world have responded with a wide variety of actions, including hearings, studies, and early-stage regulation. In Europe this includes the EU's flagship Artificial Intelligence Act, and an in-depth study of competition in foundation models by the UK's competition authority. In the United States, the Senate has convened high-profile meetings with the top executives of the corporations that dominate AI technology and infrastructure. The Biden Administration published a Blueprint for an AI Bill of Rights and then in late October published a far-reaching Executive Order that targeted AI-related harms and threats across society. Many of the private individuals and corporations who helped to develop and/or now control AI technologies have loudly embraced the idea that some forms of regulation are necessary, and some are actively working to shape whatever new rules emerge.

To the extent that any common assumptions underpin such regulatory efforts, two stand out. First, that AI is a new technology, hence we need to carefully develop new forms of regulation and even new regulatory institutions designed to strike the right balance between control and innovation. Second, that AI has so disrupted the competitive landscape that many, if not most, of the existing efforts by law enforcers and legislators to address the power, structure, and behaviors of Google, Amazon,

Microsoft, Meta, and other immense monopolists may no longer be necessary and may actually be counterproductive, such as by blocking smart innovations.

There is, however, another way to understand the promise, threats, and practical regulatory challenges we face in managing the advent of AI. This is to view the challenge through the lens of the already existing powers, structures, and behaviors of the corporations that control the foundational technologies and capacities underpinning AI. Doing so guides us to a simple set of conclusions and directs us toward practical, proven, and constructive solutions that will enable us both to minimize the political and social threats posed by AI, while also maximizing the promise of these technologies to improve the lives of individuals and society as a whole.

When viewed through this lens, what we see is that:

I. AI is a function of concentrated technological capacities and capabilities

Today's leading AI models are largely being commercialized by a handful of corporations able to exploit unique technological capabilities. For instance, although foundation models are trained on datasets collected from the open internet, Google, Microsoft, Amazon, Meta, and Apple each control extensive private caches of data that give them unassailable advantages over potential rivals. Similarly, Google, Microsoft, and Amazon control a wide variety of computing and cloud capabilities, data management technologies, and other capacities and expertise that further cement their dominance.

II. Monopolists are exploiting existing advantages to shape and speed the rollout of AI

The existing market dominance of these five corporations is based – in addition to their control of data and computing and cloud capabilities – on the power and reach of the online platforms they already control, their sophisticated models for manipulating and exploiting the behaviors of businesses and individuals, and other technological and commercial chokepoints they have forged and honed over two decades. Over the same period, these corporations have developed a vast and far-reaching system of political relationships, lobbying power, and legal expertise to protect and expand these monopoly positions. These dominant positions and concentrations of power give these corporations vast abilities both to accelerate the development and commercial rollout of AI technologies, and to shape and manipulate today's public debate over how to design, use, and regulate AI.

III. Monopolists are using AI to further entrench their existing dominance.

AI is enabling these dominant corporations to dramatically increase the quality and quantity of the many competitive advantages they already enjoy vis-à-vis potential rivals in ways that only deepen the moats that surround their search and mapping engines, social media platforms, digital advertising systems, e-commerce platforms, email and operating systems, and more. This includes, foremost, by radically amplifying their abilities to:

- Engage in sophisticated, personalized, and highly profitable manipulation and exploitation of individuals and businesses who depend on their services for communication and commerce.

- Misappropriate or simply outright steal information and other digitizable properties developed by smaller businesses and individuals, including notably journalism, music, books, photography, art, and even the most personal skills and attributes of particular individuals, while making it even harder than in recent years to track the theft.

- Further entrench their already formidable control over the development and application of critical technologies and key digital infrastructure.

IV. Monopolists control the direction, speed, and nature of AI innovation

These corporations already broadly control the direction, speed, and nature of innovation in many if not most of the key technologies in the internet tech stack. In addition to cloud capacity, computing technologies, and data, this includes chokeholds over computer and mobile phone operating systems, the standards and governance of the World Wide Web, and increasingly even the design and commercialization of semiconductors. These existing concentrations of power, in combination with their emerging dominance in AI, give this same handful of corporations the ability to determine when, how, and in whose interests AI is developed and rolled out. Their control over AI's 'upstream' infrastructure means they can easily identify any serious potential rival in its earliest stages and then move swiftly to crush, sidetrack, co-opt, or simply acquire the upstart.[1] In short, these corporations are already shaping the entire 'downstream' ecosystem to serve their own short-term private interests in ways that will in many instances prevent other companies and individuals from using AI to solve urgent challenges and improve people's lives.

V. AI amplifies many of today's most dangerous monopoly harms.

These corporations are exploiting AI to rapidly boost many of their existing abilities to engage in the personalized manipulation and exploitation of individuals and companies that depend on the platforms and services they control. This is already worsening a number of political, economic, and social harms, including:

- **Suppression of trustworthy information.** In recent years**,** these corporations have restructured critical communications and commercial systems more dramatically than any previous period in history. They have done so in ways that severely reduce an individual's ability to gather, report, verify, share, and make practical political and economic use of trustworthy information. Specific harms include diversion of advertising revenue and readers away from publishers, the routine manipulation of the information and services delivered to individuals and businesses, distortion and censorship of public conversation and debate, and degradation of essential services.

- **Propaganda and misinformation.** The extreme explosion of propaganda and misinformation in recent years is largely a function of the reach and power of the corporations that control the main communications and commercial platforms on the internet, combined with business models designed to directly manipulate what individuals buy, where they go, what they read, and how they act politically. With some exceptions, it is not Facebook and Google that are leveraging their own platforms to spread propaganda and disinformation, but rather state-level and private actors who pay to use their platforms to manipulate the thinking and actions of individuals and organizations. The introduction by these gatekeepers of generative AI capabilities dramatically boosts the ability of these actors to personalize propaganda and misinformation in ways that geometrically increase its political, social, and psychological effects.

- **Addiction to social media, gaming, and gambling.** Growing use of social media, gaming and other online services has been associated with gambling-like addiction, depression and other serious harms to mental health, particularly among minors. These problems are magnified by our collective dependence on the products and networks of a few underregulated monopolistic platforms, whose business models prioritize screen time and viral content over quality information and engagement. Generative AI's unprecedented ability to customize and target bespoke content to individual users appears already to be reinforcing these harmful effects.

- **Manipulation of workers and contractors.** Dominant tech corporations have a long track record of surveilling workers themselves as well as giving other employers the ability to do so. Examples include Amazon's aggressive surveillance of its warehouse workers and delivery contractors, and workplace tools provided by Microsoft and Google that enable invasive monitoring of individual workers. Digital surveillance and AI also give employers the ability to manipulate workers through the payment of differential wages, particularly in employment in the so-called "gig economy." There is a significant risk that generative AI increases these surveillance capabilities, while also giving employers new opportunities to manipulate workers through tailored content.

- **Monopolistic extortion of sellers.** Monopolization of key commercial gateways – especially e-commerce platforms but also cloud computing, app stores, and other platforms – has given a handful of corporations the power to decide who gets access to the market, and on what terms. Through their control of these gateways, Amazon, Apple, and Google are able to extract extortionate fees from sellers, set the terms and conditions governing how they do business, and degrade or cut off access at will.[2] This gatekeeper power also stifles criticism from sellers, who understandably fear retribution. These abuses are set to be magnified by concentration in the cloud computing platforms and foundation models upon which the majority of AI tools will be built.

- **Reduced security and resilience.** As growing numbers of businesses, industries, and governments incorporate AI into their services and operations, the risks to security and resilience from extreme concentration in the core infrastructure upon which AI depends will rapidly increase. We already have seen this threat play out in the highly concentrated cloud computing systems, especially those run by Amazon. While outright failure of these systems is the most obvious threat, cyberattacks, rogue algorithms, and faulty data would have equally systemic implications.

- **Degradation of essential communications and commercial services.** While initially praised for providing innovative new services, many of the platforms developed by today's tech monopolies have deteriorated in quality over time.[3] Examples include increasingly inaccurate search results on Google, the crowding out of genuine sellers with paid advertisements on Amazon, and replacement of organic content with algorithmic recommendations on social media networks such as Instagram and Facebook. Generative AI is already accelerating this process in numerous ways through the creation at ever-faster speeds of low-quality and inaccurate content[4] which crowds out useful and genuine material.

VI. Competition law, rules, and regulations are our most immediately effective tools.

History teaches that our economies and societies have faced many revolutionary communications and transportation technologies in the past, including the railroad, telephone, electricity, and the internet. It also teaches that the only way to prevent powerful private corporations from exploiting these new technologies in ways that upset basic political or social balances is to use antitrust and other forms of competition law to carefully regulate the behavior, structure, and internal governance of both individual corporations and entire industries. Doing so has repeatedly empowered the public as a whole to take full advantage of these great advances in science and engineering. Doing so has also repeatedly made it easier to use health, safety, consumer, and other regulatory regimes to help protect the interests and wellbeing of individuals, communities, and the public as a whole.

Our broad failure thus far to apply these lessons to the digital gatekeepers that dominate our online and offline lives has already resulted in a wide array of extreme harms to our democracy, individual liberty, and prosperity. In recent years this has begun to change, thanks to a revolution in antimonopoly lawmaking in Europe and in law enforcement in the United States. But this work remains far from done, and the advent of AI makes it all that much more urgent to complete the job.

BROAD RECOMMENDATIONS:

Our report sets out broad recommendations for enforcers and policymakers in four key areas:

I. Establish a clear hierarchy of goals for regulatory action, to help prioritize the use of limited resources.

Given limited resources, and the scale of the challenge at hand, it is crucial that lawmakers and regulators establish a clear hierarchy of goals for regulatory action. The top priority should be tackling threats to individual liberty and democratic institutions, which are essential if we are to break and harness the power of the online gatekeeper corporations that now threaten us. This in turn implies a close and immediate focus on the many ways in which the *existing power* and *existing behaviors* of these immense, privately controlled gatekeepers threaten our ability to communicate and debate, gather and share news, and do business directly with one another. Questions of technological innovation should be of secondary importance compared to making these platforms safe for democracy, although given sufficient resources, law enforcers can *also* focus simultaneously on promoting an open and competitive political economy. Indeed, many actions that would protect our core political rights and interests would also begin to provide individuals and businesses with greater opportunity to promote innovation and to master AI and other new technologies in the public interest.

II. Make aggressive use of existing law, and invest in legislation and new regulatory institutions only where there's a clear need and reasonable chance of success.

Many governments already possess wide-ranging powers that can be deployed now to prevent today's monopolists from using AI to further cement their power and to more effectively exploit and manipulate individual people and organizations, and indeed to begin to unwind dangerous existing concentrations of capacity and control. These powers include competition law and policy, trade policy, consumer protection laws, privacy regulation, and copyright protection. This approach is especially important in the United States, where there is an extremely vast and robust collection of powerful laws and regulatory regimes to address such threats, built up and refined over the course of more than two centuries, and where longstanding gridlock in Congress makes it unlikely the institution will pass new competition laws soon.

III. Accelerate efforts to adapt existing competition law to address today's threats.

Law enforcers and lawmakers are engaged in the most fundamental and comprehensive rethinking of competition policy since the Chicago School revolution of the early 1980s and, in some respects, since the New Deal. In the United States, Europe, and elsewhere, they are scrambling to restore traditional pre-Chicago School goals, principles, and analysis, as we see in the new draft merger guidelines published by the Department of Justice and Federal Trade Commission. They are also moving to adapt and update those regimes for the digital age, as we see in new European laws such as the Digital Markets Act and Digital Services Act and in the wide-ranging lawsuits by both the federal and state governments in the United States against Google, Amazon, and Facebook. This effort is still, however, in its early stages. It is vital to immediately extend this effort to cover such factors as control of data and computing

capacity, including directly in relation to AI. It is also vital to move swiftly to integrate this effort with legal and regulatory regimes that intersect with antitrust, including communications, trade, privacy, copyright, and consumer protection, among others.

IV. Ensure that dominant corporations in control of essential platforms and services treat all users the same.

A core tenet of modern competition policy is the requirement that private corporations that control essential services do not discriminate in the delivery of these services, and provide equal access to all comers. As Senator John Sherman said in a speech in favor of the U.S. antitrust law that bears his name, such regulations lie "at the foundation of the equality of all rights and privileges." Today this principle is especially important when addressing the actions and business models of essential communications and commercial platforms, as well as all essential AI infrastructure including cloud computing capacity and foundation models.

IMMEDIATE ACTIONS:

Our report sets out specific recommendations for enforcers and policymakers to take immediate action in eight key areas.

I. Ban all discrimination by powerful gatekeeper platforms in the delivery of essential services to individuals and businesses.

II. Recognize cloud computing as an essential infrastructure, separate ownership and control from the largest gatekeeper platforms, and regulate it as a utility.

III. Recognize that any data collected by large platforms in their capacities as essential services is public in nature, and establish a public-interest regime to govern access.

IV. Aggressively enforce copyright laws to protect the properties of authors, creators, and other independent publishers from misappropriation and misuse by gatekeeper corporations, and establish a trustworthy and transparent system for auditing the use of copyrighted material in AI systems.

V. Clearly map how the structures, behaviors, and business models of the largest gatekeepers threaten national security, including by enabling foreign surveillance and interference. Use government investment and procurement policies to break chokepoints and promote security.

VI. Reverse gatekeeper efforts to control AI development through mergers, investments and partnerships and block similar deals in future.

VII. Establish bright-line rules to limit digital exploitation of workers and contractors, including a complete ban on biometric surveillance and automated manipulation.

VIII. Increase strategic collaboration between competition law enforcers and data protection and privacy regulators.

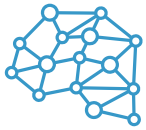
What are we talking about when we talk about AI?

The contemporary discussion around AI may be confusing given the multiplicity of terms in use. Below are some basic definitions of terms used frequently throughout this report.

Algorithm: A set of mathematical instructions or rules that, especially if given to a computer, will help to calculate an answer to a problem (Cambridge)

Artificial intelligence: Umbrella term for a range of algorithm-based technologies that solve complex tasks by carrying out functions that previously required human thinking (UK Information Commissioner's Office)

Foundation models: Models trained on broad data (generally using self-supervision at scale) that can be adapted to a wide range of downstream tasks (Stanford)



General purpose AI: Largely synonymous with foundation models; refers to an AI system that can be used in and adapted to a wide range of applications for which it was not intentionally and specifically designed (European Parliament)

Generative AI: Describes algorithms and applications that can be used to create new content, including audio, code, images, text, simulations, and videos (McKinsey)

Large language model: AI systems trained on significant amounts of text data that can generate natural language responses to a wide range of inputs (Ada Lovelace Foundation)

Machine learning: The study of how computer agents can improve their perception, knowledge, thinking or actions based on experience or data (Stanford)

Figure 1:AI glossary

I: THE STATE OF DEBATE ON COMPETITION POLICY AND AI

With this report, the Open Markets Institute seeks to bring together two debates that have largely been kept separate thus far: that of the promise and perils of AI, and of the harms of monopoly power in the digital age.

As the rest of this report will make clear, it is our belief that to design appropriate solutions that place the development of AI in service of the public interest, we need to view this technological development through the lens of the power and structure of dominant corporations and competition policy. The real and urgent harms posed by AI cannot be fully understood or addressed without bringing to the forefront of the debate the existing monopoly power of corporations such as Google, Microsoft, and Amazon, as well as the well-developed debate and many already existing tools and proposals to address their power and behavior.

A REVOLUTION IN ANTIMONOPOLY THINKING AND ENFORCEMENT

Over the last decade, there has been a profound change in attitude towards the power and structure of large private corporations. The 'libertarian' or 'neoliberal' philosophy that has guided political economic regulation since the 1980s promoted a laissez-faire approach to large corporations and financial institutions. But in recent years the people of the United States and many other nations have come to conclude that the resulting concentration of power, control, and capacity poses a wide and growing variety of grave threats to our democracy, national security, prosperity, and the environmental sustainability of human society. This has been especially true of the corporations that have captured control over dominant online communications and commerce, particularly Google, Amazon, Microsoft, Meta, and Apple.

As a result, lawmakers and law enforcers in the United States, Europe, and elsewhere are now engaged in a revolutionary rethinking of the purpose and processes of competition policy. For the last generation, the 'Chicago School' philosophy of legal theorists such as Robert Bork and Richard Posner generally supported the concentration of power and control based on the idea that doing so would help drive down prices and thereby better promote the 'welfare' of the consumer. Today, by contrast, policymakers are increasingly using antimonopoly enforcement to protect democracy and individual liberty, and to break or neutralize any concentration of power that threatens workers, entrepreneurs, farmers, and local communities.

These changes are well captured in the present efforts of the U.S. Department of Justice and Federal Trade Commission to draft new 'guidelines' to govern how these agencies will interpret the legality of particular types of deals. We also see this new thinking in the growing number of large enforcement actions in the digital economy. In the last few years, antitrust enforcers have brought major legal cases against monopolists including Google, Meta, and Amazon, taken action to block anti-competitive takeovers, and passed or proposed new competition legislation to outlaw abusive conduct. Viewed in a broad historical context, it is clear that the United States, Europe, and much of the rest of the world is in the midst of the most important debate about how to address concentrations of corporate power and control since the Second World War, and in certain respects, since the Progressive Era in the United States at the turn of the last century.

In the United States, the idea that existing competition policy tools could be used to rein in the power of the

new 'robber barons' – including the largest of online gatekeeper corporations – did not arise spontaneously. On the contrary, it is the result of a long and carefully developed effort to shine a light on the threats posed by concentration of power and control, and the many existing tools available to help protect democracy and security.

A few moments stand out, including:

- A major speech delivered by Senator Elizabeth Warren on June 29, 2016, in the U.S. Capitol. The speech, hosted by the Open Markets Institute, traced the decline of competition in American markets and kickstarted efforts to scrutinize and tackle market concentration by policymakers in both major U.S. parties;

- The 2019 Cicilline Committee hearings and subsequent 2020 report detailing the monopolistic practices of Google, Facebook, Amazon, and Apple;

- The first major lawsuits against Google and Facebook in 2020 by the DOJ, FTC, and the attorneys general of almost every U.S. state and territory.

After President Joe Biden took office in January 2021, his Administration reinforced and accelerated these efforts. Most important was the President's July 2021 signing of a landmark Executive Order that called for the complete overturn of the Chicago School philosophy of competition policy, and an unprecedented 'whole-of-government approach' to promoting competition across the U.S. economy. Around this same time, President Biden also appointed Lina Khan to chair the Federal Trade Commission and Jonathan Kanter to serve as Assistant Attorney General to the Department of Justice's Antitrust Division.

During these same years, lawmakers and enforcers across Europe also ratcheted up efforts to address the concentration of power and control, especially within the tech sector. Although this includes important litigation – especially by the UK's Competition and Markets Authority and the Bundeskartellamt antitrust agency in Germany – the most important advances were through legislation. These include the EU's General Data Protection Regulation, Digital Markets Act and Digital Services Act, Section 19a of Germany's foundational competition law, and the UK's Digital Markets, Competition and Consumers Bill.

These efforts have been strongly opposed, especially by the corporations that would be most affected. Dominant corporations across many industries have benefited enormously from the past several decades of pro-monopoly competition policy. They are naturally reluctant to give up the power and privileges that resulted, and they have launched a wide variety of legal and political challenges and threats against lawmakers and enforcers working to rebuild traditional systems of democratic checks and balances within the political economy.

But in many ways, the battle is only beginning. And already, it is being dramatically reshaped by the rapid adoption of AI technologies by many of these same corporations, as well as by how these corporations and their close allies are using fear of AI to reshape the debate about how to address their existing power, structures, and behaviors.

DIVERSION AND DISTRACTION IN THE AI DEBATE

If we want to truly understand how AI is being designed and implemented, and the likely consequences of this, the first factor we must consider is who controls and owns the underlying technology. Contrary to what proponents of technological determinism might claim, AI – and technology in general – is not the result of any sort of natural evolution but rather the result of a series of technical, business, and political decisions by human actors, above all those who control the most

powerful corporations. One thing this means is that the AI technologies and services that have been introduced in recent months and years by Microsoft, Google, Amazon, and companies they control are very different in key respects than would be the case if AI systems were created and implemented by a diverse ecosystem of actors, including startups, SMEs, large companies, and public and non-profit actors.

Yet so far, the debate on what to do about AI has paid little attention to the role played by concentrated power and control. While the role of the likes of Microsoft, Google, and Amazon in funding and developing AI systems is acknowledged, there have been few attempts to seriously grapple with how the economic and political power of these corporations is already shaping the form that much AI technology is taking, and the impact it will have on our societies.

Consider ongoing efforts to ensure AI is used ethically and responsibly. Proposed interventions range from greater algorithmic transparency and mandatory efforts to reduce bias, to auditing and human oversight of AI-driven or assisted outputs and decisions. Notable examples of this approach include the EU's AI Act, which imposes stringent regulatory obligations on high-risk AI applications, and the Biden administration's Blueprint for an AI Bill of Rights, which sets out five principles to guide the design, use, and deployment of automated systems.

These and similar forms of regulation that aim to prevent AI from being used to harm, exploit, and discriminate against people are clearly necessary. But they will only be effective if accompanied by aggressive enforcement of competition policy to prevent a few firms from dominating everything from the nature of the technology to access to the technology. One lesson of the many recent efforts to enforce privacy regulations on these same corporations is that no matter how well rules are designed on paper, regulators will struggle to enforce them on corporations that can treat fines as a cost of doing business. By contrast, by preventing control over AI from becoming concentrated, we both increase the effectiveness of AI regulation, while decreasing the ability of any single actor to inflict systemic harm.

Just as important is the fact that many of the harms highlighted by those calling for regulation to ensure the ethical and responsible use of AI are already widespread across our societies. Indeed, these harms are the direct result of the business models these same corporations developed to exploit their gatekeeper positions over public communications and commerce. Although AI will make many of these problems worse, the fact that they are already widespread demonstrates that AI is not the fundamental source of the problem. Here again, the only way to get at the root is to view the problem through the lens of antimonopoly laws, especially those designed to set strict rules on *how* gatekeeper corporations behave vis-à-vis the companies and individuals that depend on their services.

Even more dangerous are narratives that, intentionally or unintentionally, deflect debate away from both present AI harms and the market concentration driving or amplifying them. Two in particular are worth examining in more detail. The first is the suggestion that policymakers, regulators, and law enforcers should focus primarily on the idea that these technologies pose long-term "existential risks." The second is the argument that measures to regulate AI or rein in the corporations behind it risks giving China the competitive advantage.

There is nothing outlandish about the idea that, as the capabilities of technological systems grow, so do the risks they pose to individuals and society. But the rise of generative AI has resulted in a disproportionate focus on far-flung risks such as human extinction and malicious "superintelligence," despite little concrete evidence that current or future AI models possess such capabilities. Nonetheless, this narrative is routinely promoted by

certain tech industry figures (including OpenAI CEO Sam Altman, DeepMind CEO Demis Hassabis, and tech billionaire Dustin Moskowitz) and policymakers including British Prime Minister Rishi Sunak and UN Secretary General António Guterres.

There is no reason why human beings cannot focus simultaneously on both existing real harms and hypothetical but potentially more serious risks in the long term. In practice, however, policymakers and law enforcers have limited resources and limited bandwidth, meaning a focus on one set of harms will divert attention and energy from another. Given clear evidence that many of the existing threats posed by the largest gatekeeper corporations – including misinformation, manipulation, discrimination and copyright theft – *already* pose existential threats to our democracies and our abilities to communicate and make decisions, and that AI is *already* amplifying and accelerating these problems, it makes sense to prioritize tackling these threats first. Doing so will, if anything, help ensure that the existential threats of tomorrow never come to pass.

There is another more cynical way to interpret the emphasis on existential risks by many in the technology industry. This is to see these warnings as an intentional attempt to deflect attention away from present harms being inflicted by the same large companies and individuals raising the alarm. Moreover, the narrative around existential risks is giving dominant AI companies (i.e. the only ones theoretically capable of producing models that pose these hypothetical risks) unprecedented access to policymakers and policy discussions, dramatically increasing their ability to shape policy debates and potential interventions.

Equally questionable is the alarmism about potential threats to Western democracies posed by the AI prowess of the Chinese state and Chinese corporations. Tech industry leaders have frequently and for many years now referenced technological competition with China as a reason to weaken or abandon efforts to enforce antimonopoly and other law against their corporations, albeit with little success. Over the last year or so, however, the advent of AI has helped these arguments finally find a receptive audience, especially in Washington.[5] To cite just one example, in April 2023 former Google CEO Eric Schmidt said he didn't support a pause in AI research "because it will simply benefit China."[6]

We can acknowledge the importance of remaining globally competitive – and be concerned about how the authoritarian Chinese state will deploy AI against our nations and communities – without allowing these deceptive arguments to distract us from existing efforts to make behavior by the gatekeeper corporations safe for democracy. Tackling concentration in AI, and putting sensible guardrails on how the technology is used, will not only ensure safety and resilience but also promote innovation in the market, all of which are essential if the technology is to be rolled out at scale in a way that benefits both individuals and society. Abandoning our values in the hopes of "competing" with China will not only therefore be counterproductive, but undermine the West's legitimacy in providing a democratic, pluralistic alternative to China's centralized totalitarian model.

II: A FEW PLATFORM MONOPOLIES BROADLY CONTROL AI

Ever since the boom in generative AI caught the public's attention, some have sought to portray it as evidence that competition is alive and well in digital markets. Yet this is misguided for several reasons.

First, prowess in AI – particularly when it comes to large-scale models – is heavily dependent on access to advanced technological capabilities and data, both of which are highly concentrated in the hands of a few gatekeeper corporations. This gives these platforms a huge advantage that is nearly impossible for others to overcome.

Second, while the landscape for advanced AI models may at first glance appear to resemble a thriving marketplace of both large incumbents and innovative challengers, this initial impression fails to survive even a cursory scrape of the surface. Already, dominant platform monopolies own, fund, and/or provide the underlying infrastructure for almost every significant player on the market.

Third, competition among a few already dominant platforms is not the same as competition within genuinely diversified digital markets. For example, while Microsoft might be able to use AI to eat into Google's market share in search, the market would at best still be dominated by two colossal, sprawling corporations. The hegemony that a tiny handful of unaccountable corporations maintains over online communications and commerce – and indeed almost every aspect of our digital lives – would remain unchallenged.

GENERATIVE AI IS A FUNCTION OF CONCENTRATED TECHNOLOGICAL CAPACITIES AND CAPABILITIES

The sheer quantity of resources needed to train cutting-edge AI models inevitably rewards scale and incentivizes companies to move swiftly to establish and maintain dominance over the market. Other than the largest gatekeeper corporations, few actors have the necessary computing power (including both cloud capacity and access to the most advanced semiconductors), data, and technical expertise needed to develop advanced AI. Moreover, it is precisely because the giants possess so much data and computing power that they have chosen to steer AI innovation in a direction that makes maximum use of those assets. These concentrated resources are in large part the result of extreme levels of concentration in digital markets, fortified by a variety of monopolistic conduct that most governments largely ignored until recently.

A deeper look at a few links in the AI "supply chain" or "tech stack" help illustrate the problem.

Computing power. Just three companies (Amazon, Google, and Microsoft) control over two-thirds of the $600 billion (measured in annual revenue) global cloud market, ensuring these corporations have access to computing capabilities and storage capacity which no other actors enjoy.[7] Even gatekeeper corporations without cloud arms, namely Meta and Apple, find themselves reliant on the cloud oligopoly for their computing needs. The current emphasis on large-scale AI models, which use approximately 100 times more computing capacity than other types of models, means that access to huge amounts of computing power is essential for any corporation that wants to prosper in this business.[8] Then there are the exorbitant costs of training advanced models. OpenAI's GPT-4 model, housed on Microsoft's Azure cloud infrastructure, is reported to have cost over $100 million to train.[9] These are costs that only the very largest companies, or those backed by them, can afford.[10]

The supply of the advanced semiconductors essential to training cutting-edge AI models is similarly monopolized. Nvidia, a corporation which originally rose to prominence producing graphics chips for gaming, now enjoys a near-monopoly designing chips used to train large-scale AI models.[11] Nvidia's chips are in turn manufactured by another monopoly, Taiwan Semiconductor Manufacturing Company (TSMC), which produces 90% of the world's advanced semiconductors.[12] As a result of skyrocketing demand, Nvidia's market capitalization has soared from $145 billion as recently as January 2020 to over $1 trillion as of November 2023, illustrating investors' confidence in its increasingly untouchable market position.

This power translates into astronomical prices for the most advanced semiconductors. Nvidia's flagship AI chip, the H100, costs approximately $40,000[13], which, combined with the fact that thousands are needed to train advanced models, puts it beyond the reach of all but the largest corporations.[14] Moreover, the lack of alternatives in this segment of the market has already resulted in shortages, with powerful platform monopolies (and the startups partnered with them) best placed to secure critical supplies. Increasingly the gatekeepers are vertically integrating into the semiconductor design business directly. Amazon, Apple, Google, and Meta have all developed in-house semiconductors purpose-built for (among other things) AI operations, with Microsoft set to follow suit imminently.[15]

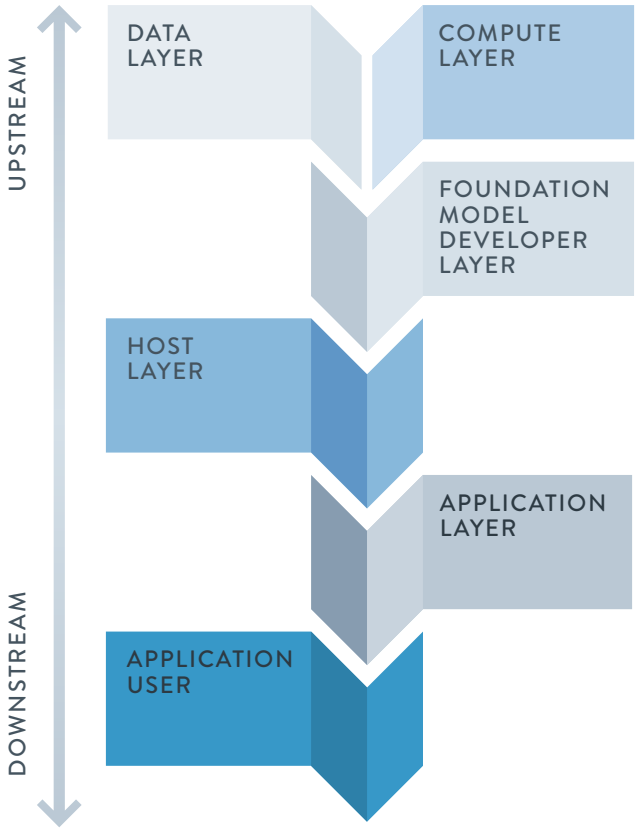


Figure 2: Overview of the generative AI supply chain

Control of and access to data is another advantage enjoyed by today's tech giants. Thanks to their huge scale and business models based on invasive collection of personal data, the dominant gatekeeper corporations have amassed vast quantities of highly personal and specific data, which can in turn be used to train and fine-tune their AI models. This is in addition to the vast amounts of non-personal data which the tech giants have acquired through their enterprise and cloud computing services, which provide them with additional insights and capabilities that further entrench their centrality in the AI ecosystem. This includes data from their cloud customers and data generated by connected devices and sensors, such as smart speakers.

Some have suggested that the huge data advantage enjoyed by the biggest gatekeeper corporations is less relevant when it comes to generative AI, because foundation models are trained primarily on the open web rather than proprietary datasets. But this theory does not hold up under close scrutiny, for two main reasons.

First, the tech giants have the advantage of being able to train their models on both the open web *and* their own vast proprietary datasets, giving them a huge advantage over those who must rely only on the former. This advantage is likely to become increasingly important as websites, publishers, and creators begin to restrict access to their content in response to mass trawling

by AI models.[16] Second, even where access to data is comparable, the dominant gatekeeper corporations control far greater computing capabilities, enjoy better access to specialized expertise, and have developed vast experience in scraping, labeling, and analyzing data.

Smaller specialized AI models and applications, tailored to specific purposes, will continue to exist in this landscape, but by definition will not garner the scale needed to challenge the giants. Even here, the tech monopolies could in many cases hold the advantage, primarily through their ownership of personalized, specialized datasets in areas such as health, finance, and transport e.g., Google's ownership of mapping and Fitbit data and Amazon's access to sensitive health data via its recent acquisition of One Medical.

DOMINANT PLATFORM MONOPOLIES ARE USING THEIR POWER TO CO-OPT AND ELIMINATE RIVALS

Despite the huge advantages of the dominant gatekeeper corporations, the market for cutting-edge AI applications might at first glance appear to be a diverse and competitive one. Major players participating in the AI race include OpenAI, Google, DeepMind, Meta, Microsoft, Amazon, and leading startups such as Stability AI, Anthropic, Cohere, and Hugging Face. Yet what becomes quickly clear when one begins to dig beneath the surface is that, whoever is ultimately left standing, the biggest platform monopolies are in prime position to maintain their dominance, both over their existing lines of business and over AI.

An April 2023 report by the AI Now Institute aptly summarizes the current landscape: "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."[17]

Take **OpenAI**, arguably the leading contender in the race thanks to its popular ChatGPT chatbot and GPT large-language model. While ostensibly an independent company, OpenAI has to date received over around $13 billion worth of investment from **Microsoft**. In return, according to media reports (the exact terms of the deal remain confidential), Microsoft received a 49% stake in the company and the right to three-quarters of OpenAI's profits.[18] The "partnership" between the two companies also requires OpenAI to rely exclusively on Microsoft's Azure cloud platform to power its services. Meanwhile, Microsoft has been allowed to integrate OpenAI's models across its entire sprawling suite of products.[19]

One recent estimate put the cost (primarily consisting of computing resources) to OpenAI of running ChatGPT at $700,000 per day, or around $21 million per month.[20] And as mentioned above, GPT-4 reportedly cost over $100 million to train. These are costs very few independent startups can afford, and a key reason behind OpenAI's decision to accept a position of dependence on Microsoft.

Given this dependence, it is questionable whether OpenAI can truly be considered an independent player in the market. The partnership has also blunted Microsoft's force as an independent competitor in the market, with the corporation winding down some its own in-house AI products, including its flagship AI-driven assistant Cortana.[21] Indeed, partnerships like Microsoft's have begun to attract the attention of antitrust agencies, with the head of Germany's competition authority recently warning that in some cases cooperation agreements should be seen as "mergers in all but name."[22]

The company's status was described well by Elon Musk, who took part in the founding of OpenAI, in a recent tweet:

"OpenAI was created as an open source (which is why I named it 'Open' AI), non-profit company to serve as a counterweight to Google, but now it has become a closed source, maximum-profit company effectively controlled by Microsoft. Not what I intended at all."[23]

Google/Alphabet's influence also extends far beyond its own PaLM model and Bard chatbot. The corporation purchased leading British AI research lab DeepMind back in 2014, facing little scrutiny from competition authorities at a time when takeovers by the largest platform monopolies were typically waved through by regulators. For a while, Google allowed DeepMind to continue operating as a largely independent entity and pursue its research free from commercial pressures. This independence paid off significantly, with DeepMind's AlphaGo program defeating Go world champion Lee Sedol in 2016, and its AlphaFold program making major breakthroughs in the science of protein folding. But in April 2023, with the AI arms race in full swing, Google announced that it was absorbing DeepMind directly into its AI-focused Brain division, ending the unit's independence and enlisting its employees in the service of Google's commercial goals.[24]

Google also announced this year that it was investing up to $2 billion into Anthropic, representing a significant share of the startup's total funding to date and giving Google a significant ownership stake – in addition to Google's status as the main provider of Anthropic's cloud capacity.[25] While not as large as Microsoft's investment in OpenAI (which itself started as a smaller initial investment), Google's presence as a major financial and infrastructural backer will certainly influence the development of Anthropic's technology and commercial strategy.

Google is also attempting to position itself as the cloud provider of choice for generative AI startups, with CEO Sundar Pichai recently boasting that "more than 70% of gen AI unicorns are Google Cloud customers."[26] It also operates the TensorFlow software development library, a leading tool for machine learning developers which helps Google ensure that AI innovation benefits the corporation's vast array of operations and interests. Incidentally, TensorFlow's main competitor, PyTorch, was created by Meta.

Google and Microsoft are taking the most aggressive steps to dominate the emerging AI ecosystem and co-opt, if not eliminate, potential challengers. But other platform monopolies are quietly making moves of their own.

In February of this year **Amazon** announced a major partnership with Hugging Face, a hub for open-source machine learning and AI innovation.[27] The deal gives developers on Hugging Face access to Amazon's cloud infrastructure, chips, and software, while embedding them in Amazon's ecosystem. Amazon Web Services has also reached a similar deal with open-source AI company Stability AI.[28]

Then there is Amazon's new service Bedrock, which allows customers to access different foundation AI models – including Anthropic, Stability AI, and Amazon's own models – but only within the confines of the AWS walled garden.[29] Amazon has even announced a generative AI accelerator to entice startups to build their products using its tools and on its platform, all the while locking in their dependence on its cloud infrastructure and services. And it is also following the lead of Microsoft and Google by investing directly in AI developers, in this case a $4 billion play on Anthropic. One of the catches to the deal is that the startup must use Amazon's cloud infrastructure and semiconductors.[30]

The approach being taken by **Meta**, meanwhile, has been to open up its model, Llama, to the wider developer community by permitting a degree of fine-tuning that closed models such as OpenAI's GPT and Google's PaLM do not offer. While at first unintentional – Meta had sought to limit access to a pre-vetted list of researchers and organizations before the entire model leaked[31] – Llama's

Figure 3: How gatekeeper corporations are using partnerships, investments, and acquisitions to establish control over AI

Company	Partnerships	Major investments	Acquisitions
amazon	• Hugging Face (2023) • Stability AI (2023 • AI21 Labs (2023) • Anthropic (2023)	• Hugging Face (2023, amount undisclosed) • Anthropic (2023, up to $4 billion)	• Evi (2013; $26 million) • Orbeus (2015; fee undisclosed) • Harvest.ai (2017; $20 million) • Snackable AI (2023; fee undisclosed)
			• Perceptio (2015; fee undisclosed • Lattice Data (2017; $200 million) • Regaind (2017; fee undisclosed) • Laserlike (2018; fee undisclosed) • Silk Labs (2018; fee undisclosed) • Fashwell (2019; fee undisclosed) • Vilynx (2020; $50 million) • Voysis (2020; fee undisclosed) • Xnor.ai (2020; $200 million) • AI Music (2022; fee undisclosed) • WaveOne (2023; fee undisclosed)
Google	• Cohere (2021 onwards) • Anthropic (2023) • Character.ai (2023) • Midjourney (2023) • Runway (2023)	• Anthropic (2023; Up to $2 billion) • Runway (2023; amount undisclosed) • Hugging Face (2023, amount undisclosed)	• DeepMind (2014; $400 million) • Moodstocks (2016; fee undisclosed) • Halli Labs (2017; fee undisclosed) • Onward (2018; fee undisclosed) • Alter (2022; $100 million) • Phiar (2022; fee undisclosed)
Meta	• Microsoft (2023)		• Atlas ML (2019; fee undisclosed) • Bloomsbury AI (2018; $30 million) • AI.Reverie (2021; fee undisclosed)
Microsoft	• OpenAI (2019 onwards) • Meta (2023)	• OpenAI (2019, 2021, 2023; over $10 billion) • Builder.ai (2023; amount undisclosed) • Inflection AI (2023; amount undisclosed)	• Swiftkey (2016; $250 million) • Maluuba (2017; $140 million) • Bonsai (2018; fee undisclosed) • GitHub (2018; $7.5 billion) • Lobe (2018; fee undisclosed) • Nuance (2022; $20 billion)

open model has led to a flurry of experimentation on top of Meta's underlying technology. Most recently, Meta announced that it would be building on this by making its next model, Llama 2, available free to businesses and researchers on what it claims is an "open-source" basis, although this is disputed (more on this below).[32]

At first glance, these initiatives from Meta and Amazon may look like a tacit acknowledgement of the need to coexist alongside, rather than dominate, a flourishing and diverse AI ecosystem. But they should be seen for what they really are: attempts to control the technology by owning the underlying infrastructure on which AI depends. Just as the gatekeeper corporations' control of app stores and online marketplaces allows them to exploit countless independent sellers and small businesses, their control of the cloud infrastructure, foundation models, and marketplaces needed to design, train, host, and run AI applications will give them similar power to steer the technology in a direction conducive to their interests.

Of the dominant gatekeepers, the one major outlier thus far is **Apple**. So far, unlike Google, Meta, Amazon, and Microsoft, Apple has not announced any AI models or applications of its own, nor major partnerships with prominent AI startups. In many ways this is unsurprising, given that Apple's core strengths lie in hardware and operating systems, not applications. Apple also recently announced the launch of its cutting-edge Vision Pro virtual reality headset, suggesting it is betting on a different area of emerging technology.

But neither can Apple cannot be written off at this early stage. Quite the contrary. Apple has acquired more AI startups than any other tech giant (see Figure 3) and has recently been hiring actively for positions focused on large language models.[33] Its dominance in hardware, operating systems, and app stores will surely allow it to exert significant power over how consumers and businesses interact with AI models and applications, including extracting value from those interactions.

COMPETITION IS NOT ONE CLICK AWAY

It should be clear by now that there is little prospect of independent AI companies surviving, let alone thriving, without becoming dependent on the largest gatekeeper corporations in one way or another. But there are other arguments used to claim that AI is competitive, which also require close examination.

One is that "open-source" AI will increasingly exert real competitive pressure on the dominant platform monopolies. An internal Google memo, leaked in May of this year, claimed that when it comes to AI models, Google and OpenAI have "no moat" and are set to be usurped by open-source alternatives, an argument echoed by others.[34] Yet as has been pointed out by numerous observers, the open-source AI landscape is not as open as it seems.[35] [36]

As we saw earlier, Llama, one of the most popular models for open AI innovation, is owned by tech giant Meta. And indeed, the open-source community has already made clear that given the restrictions Meta has placed on Llama's commercial use, the release terms do not meet the widely-accepted definition of open source developed by the Open Source Initiative.[37] Furthermore, Meta has suggested that it may look to further substantially limit access in the future to a small pool of partners with "strong credentials" based on safety risks, which the tech giant would be able to unilaterally define.[38]

In fact, a move from open to closed AI models is already well underway. While never truly open source, OpenAI previously provided public information on its large language models, information that has been helpful to companies and developers working on their own AI models. Yet upon on the launch of its latest GPT-4 model, OpenAI announced that it would not be publishing any details about the "architecture, hardware, training compute, dataset construction, training method, or similar," citing the "competitive landscape" and "safety implications."[39]

With Meta already failing to meet the definition of open-source, OpenAI shutting off what limited information it provided, Google's model being closed to start with, and other players dependent on the giants' support for their survival, the prospects of a real competitive challenge from open source models look slim. While there may be some limited fine-tuning of models developed and released by the largest platform monopolies, these modest third-party efforts will struggle to keep up with developments taking place inside these corporations' own lavishly watered walled gardens. Meanwhile, the dependence of open-source developers on the technological capabilities of the dominant gatekeeper corporations means that the latter will be in a position to snuff out any real competition from the former.

Additionally, openness – if not open source – in AI models can actually serve to reinforce, rather than challenge, dominant platforms' power. As a recent paper by David Gray Widder, Sarah Myers West, and Meredith Whittaker explains, while "some tech companies initially fought open-source, seeing it as a threat to their own proprietary offerings, more recently these companies have tended to embrace it as a mechanism that can allow them to entrench dominance by setting standards of development while benefiting from the free labor of open source contributors." The authors argue that while truly open-source AI does exist, the term is frequently used inaccurately or misleadingly, and is increasingly being instrumentalized by large companies to entrench their dominance and fend off regulation.[40]

The trajectory of other, mature digital markets provides an indication of what we might expect to see with open-source models in the context of AI. While Linux in PC operating systems, Mozilla Firefox in web browsers, and Android in mobile operating systems (to name a few better known examples) all promised to bring a new level of openness and transparency to key technologies, all – in different ways – were unable to challenge or supersede the tech giants.

Both Linux and Firefox have received praise for their reliability, customizability, and security, yet they have struggled to overcome the vastly superior financial resources of the largest gatekeeper corporations, let alone the ability of these corporations to exploit their control of wider ecosystems to lock in users and self-preference their own products. As for Android, while initially created by a consortium of developers, it is Google's proprietary version that has come to dominate the market, along with the closed apps Google has built on top of it. Google achieved this dominance in part through anti-competitive practices, including incentivizing hardware manufacturers to avoid installing versions of Android not approved by Google.[41]

While the past is never a perfect guide to the future, the failure to date of open-source solutions to take on dominant platforms across a range of markets should make us wary of claims that the wall surrounding the dominant gatekeeper corporations will soon be breached by open-source solutions. This isn't to say that we shouldn't take steps to promote genuine open source efforts, and prevent attempts to quash them. But alone, they are unlikely to meet the scale of the monopoly threat.

Another argument is that fierce rivalry between the largest platform monopolies is proof of a healthy and competitive market. Microsoft's campaign to dislodge Google from its dominant position in search using OpenAI's technology is one example, with excited predictions that Bing could supersede Google Search within a couple of years.[42] The tech giants are deploying AI against each other in other areas too, including online advertising, office software, e-commerce, cloud computing, social media, and more.

But it is important not to confuse limited competition on a handful of fronts among a handful of dominant platforms with a truly diverse digital ecosystem in which large corporations control few if any key chokepoints. In this hypothetical world, an ever-changing cast of incum-

bents and challengers perpetually vie for supremacy, with no single platform succeeding in gaining a permanent chokehold over any particular market or technology. Seen from this perspective, Microsoft replacing Google as the dominant search provider, or coexisting alongside Google in a search duopoly, would hardly be an improvement on the status quo. The search market would remain highly concentrated, and no genuinely new player would have succeeded in breaking into the cozy club dominated by the same companies over many years. The same could be said of Apple or Amazon gaining more of the digital advertising pie, or Meta launching a popular online shopping platform.

Indeed, a recent analysis of trends in U.S. tech stocks since the 1960s found that while in the past, each new technological wave brought fresh players to the fore, since the early 2000s a few massive corporations have succeeded in entrenching themselves at the top. This is reflected in the fact that today, the five largest tech companies represent roughly 20% of the value of the entire S&P 500, compared to around 1.3% in 2000. The average age of the market leaders is creeping up quickly, from around 12 years in the early 2000s to closer to 40 today.[43] In the case of AI, dominance by these same corporations thus far looks all but inevitable.

What's more, this burst of AI-fueled competition between the tech giants is likely to gradually settle into established "spheres of influences" mirroring those we are familiar with from today's tech landscape. Over the last 15 years, the largest platform monopolies have shown a strong preference for avoiding direct conflict with one another's key bastions of power, in favor of peaceful co-existence. Examples of this preference in action include the tens of billions of dollars Google pays Apple every year to remain the default search engine on iPhones and Macs, and the 'Jedi Blue' agreement between Google and Meta designed to strangle competition to their digital advertising duopoly. Meanwhile Apple and Meta, which do not have their own cloud computing arms, depend on Google, Microsoft, Amazon, and Nvidia for their needs.

Such cartel-like behavior even includes markets that should be easy to challenge; some years back, both Google and Apple abandoned efforts to break into the sale of books and compete head-on with Amazon, after initially making large investments in that business. This dynamic is already becoming evident in AI too, with Meta recently announcing Microsoft as its preferred partner for the rollout of its Llama 2 model.[44]

Finally, as discussed in the next section, the sheer scale of the largest gatekeepers is likely to magnify the harms arising from AI, even more so when those platforms are aggressively competing against each other. A more competitive AI landscape, as measured by the plurality of actors involved, would help dilute the tech giants' power. But unregulated competition in a market in which powerful corporations already enjoy immense power over their customers is highly likely to result not in better services for the companies that depend on the giants, but in more efficient exploitation of those customers.[45]

III: AI REINFORCES EXISTING MONOPOLY POWER AND HARMS

The previous section demonstrated how success in AI today is a function of pre-existing concentration in the technology supply chain. In this section, we explain why AI is set to reinforce this logic of concentration further, and amplify monopoly harms.

MONOPOLISTS ARE USING AI TO FURTHER ENTRENCH THEIR EXISTING DOMINANCE

The combination of monopoly power and AI has already unleashed a vicious cycle in which concentration begets more concentration. The dominant gatekeeper monopolies are exploiting AI to reinforce and expand many of the already existing concentrations of economic power and technological resources they control. The basic process is relatively simple. The largest models – backed by the most data, computing power, and expertise – produce the best results. This in turn attracts the most users, entrenching the existing dominance and profitability of the corporations deploying them. The winners are then able to extract higher profits and collect more and more data, which empower them to further refine their AI models and applications, every day digging the moats around their monopolies that much wider and deeper.

This dynamic is not new. Control over data has long been a major factor in how today's dominant gatekeeper corporations were able to establish and fortify their monopolies over online activities including search, social media, advertising, e-commerce, and cloud computing. But AI risks taking this logic of concentration to a new and more extreme level.

Large-scale AI systems may also come to exhibit the network effects that characterize many of the markets mentioned above. As with search engines, people are likely to gravitate towards the AI models and applications that are most effective at responding to their prompts, which in turn will be those trained on the largest amounts of data and computing power.[46] And as with social media platforms or mobile operating systems, consumers and businesses may prefer to use the same AI tools and services as their peers, particularly if those tools are promoted by and integrated with systems those users are already locked into.

For example, Amazon could exploit its powerful position in cloud computing infrastructure and services to make it easier for businesses to collaborate internally and with other companies using its preferred AI tools within the AWS ecosystem (while simultaneously making it harder to collaborate outside it). Meanwhile Microsoft and OpenAI could seek to limit AI-driven collaboration outside of Microsoft's vast array of products and services (including chatbots, email, operating systems, cloud computing, and office software).

It is important to note that network effects are not inherently negative, as there are obvious benefits to both individuals and the public as a whole when many people use the same service. But left unchecked, this dynamic is likely to result in a very small number of corporations holding extreme power over how individual businesses and citizens interact with and are acted upon by AI. Relatedly, absent broad rules requiring the gatekeeper corporations to provide the same quality service to every customer, another result is that these giant corporations are free to engage in politically and economically dangerous forms of manipulation and extortion of each individual user.

Should the present concentration of control over AI remain unchallenged, or get even worse, a handful of all-powerful firms would be able to influence the work,

Figure 4: The self-reinforcing cycle of AI concentration

experiences, and fates of hundreds of millions or even billions of people simply by tweaking the parameters of their systems. By controlling AI models themselves, or the cloud platforms upon which AI models and applications are built and accessed, these gatekeepers can, from one moment to the next, suddenly change the information people receive in response to their queries, or the services provided to small businesses. They can do so across their platforms, in ways that affect every user the same. Or they can do so in ways that target specific individual people and companies, either arbitrarily, out of a desire to extract more money from these captive users, or in retribution for public opposition.

The dominant gatekeepers and their supporters push back against these arguments by claiming that high degrees of concentration in the AI supply chain create a host of benefits, from economies of scale and lower prices for consumers, to greater safety and increased competitiveness with China. But the past two decades of technological development have shown us that their services are anything but free or low-cost, and in fact are designed to drive up the prices users pay across the internet.[47] Meanwhile the largest gatekeeper corporations have completely failed to live up to their promises on safety, and in recent months have been abandoning many of their few modest efforts to protect users. And it should be clear that competing with autocratic China

cannot entail allowing tech monopolies to further disrupt democracy at home.

STEERING DEBATE AND INNOVATION THROUGH ECONOMIC AND POLITICAL POWER

The present efforts by the gatekeepers to dominate AI are made possible by the enormous financial and political advantages they have built up by exploiting their monopoly power. Not only do they already dominate almost all key links in the AI services and technology supply chains, they also are shaping the policy debate on whether and how to regulate AI in ways that protect and promote their existing interests. This is largely thanks to their vast lobbying and influence systems,[48] as well as to a carefully curated public narrative that their technical expertise is free from conflicts of interest[49] and that the technologies they control evolve in certain directions naturally, even inevitably,[50] largely outside the influence of power, profit, and politics.

In the U.S., OpenAI, Microsoft, Google, and others have publicly and repeatedly called for regulation while simultaneously attempting to steer the focus of any actual potential regulation away from existing harms (including those caused by their existing suite of platforms, products, and business models) towards abstract and speculative future threats. OpenAI CEO Sam Altman, for example, expressed strong support for regulation in his testimony before the U.S. Congress, only to later threaten to pull OpenAI's services out of Europe if the EU's AI Act proved too burdensome.[51] OpenAI has also lobbied aggressively behind the scenes to water down the EU legislation.[52]

But the political influence of the platform monopolies is not only about shaping ongoing legislative efforts. It is also about ideological capture of key sources of information and advice for policymakers. As recently revealed by *Politico*,[53] a powerful network of billionaires and corporations is pouring tens of millions of dollars into promoting the idea that AI poses a variety of apocalyptic threats to society, and that policy should focus on these long-term threats as opposed to present-day harms. To back this effort, this network is paying to place staffers with "technical expertise" in the offices of key senators and House committees, federal agencies, and think tanks.

Through their monopoly power, the tech giants are also in a position to determine the direction, speed, and nature of AI innovation. A useful case study is the role Google and Facebook have played in restructuring the entire news and advertising industries to serve their interests.[54] Over the past two decades, Google aggressively acquired the businesses and technologies necessary to capture almost complete control of the underlying infrastructure publishers and advertisers use to do business with one another. Then Google, with Facebook following close behind, exploited this control to divert scores of billions of dollars away from news publishers and broadcasters and into their own vaults, simultaneously starving news media in the United States and around the world and concentrating enormous political and economic power.[55]

The two corporations have used countless tools to achieve this, including Google's Accelerated Mobile Pages, Google News, Google Ad Manager, Facebook Video and Instant Articles, and Facebook Ad Network. But the result is that "innovation" has been used to reinforce their monopoly power in search, social media, and advertising at the expense of other actors in the supply chain. For example, a recent close study of Google's business in Switzerland concluded that news content contributes to around 40% of the corporation's entire revenues in that country, indicating the extent to which the company's control over platforms and advertising infrastructure has diverted advertising dollars away from news media.[56]

It isn't difficult to imagine how the tech giants – who already have far more power over AI than they initially did over other industries – will seek to use AI technologies in

ways that reinforce their existing areas of dominance. Instead of harnessing the technology to solve urgent social challenges and improve people's lives, the digital gatekeepers will be far more inclined to use it to entrench their existing monopolies and to put the pursuit of short-term commercial benefit over the economic and political wellbeing of our societies. Their influence over how AI innovation unfolds is likely to extend to all corners of the realms they control. Through their control of key inputs such as cloud computing, foundation models, and programming tools – the "upstream" infrastructure powering the rest of the AI supply chain – the gatekeepers will also have the power to define innovation for many, if not most, of the industries developed by entrepreneurs operating "downstream."

AI IS AMPLIFYING TODAY'S MONOPOLY HARMS, AND IS CREATING NEW ONES

The chokehold that a few corporations possess over key digital markets – including online search, video streaming, social media, and digital advertising – has resulted in an extensively documented array of threats and harms that legislators and regulators have struggled to understand and master. This ranges from democracy-disrupting disinformation[57] and the exploitation and manipulation of children,[58] to the mass expropriation of content creators and small businesses.[59]

With these same monopolies driving the latest AI boom both directly and through their control over other actors, we should not be surprised to see these same harms and threats become even more extensive and disruptive in the days and years ahead.

Already, there have been plenty of warnings about how the race to profit is leading even these fantastically rich corporations into reckless and dangerous behaviors and actions. Take the case of Timnit Gebru, a former Google researcher who has compared the AI boom to a "gold rush" and was fired from the corporation for suggesting that the drive towards ever-larger models was coming at the expense of safety.[60] In the event, Gebru's warnings proved to be only too prescient. This was made especially clear by Google's rushed launch of its Bard chatbot earlier this year, which was heavily criticized by employees for putting the pursuit of profit above ethical considerations, and where the corporation reportedly overruled warnings from its safety team that Bard could cause serious harm.[61] Much the same apparently occurred inside Microsoft, which ignored similar warnings from OpenAI about integrating its technology into its Bing search engine without full and careful testing.[62]

The rest of this section explores the different ways in which monopoly power in AI reinforces existing monopoly harms, both now and in the future.

DISTORTION OF PUBLIC DEBATE

Over the past two decades**,** the platform monopolies have restructured critical communications and commercial systems more dramatically than in almost any previous period in history. They have used acquisitions and other monopolistic strategies to concentrate these activities on the platforms they own and control, then exploited their power to radically alter how we communicate with each other and consume information. While new forms of communications technology can provide many benefits to individuals and society as a whole, our failure to carefully regulate the power and behaviors of these corporations left them free to exploit these new technologies in ways that have disrupted basic democratic and social institutions and the checks and balances governing them. Specific harms include diversion of advertising revenue and readers away from publishers, distortion and censorship of public conversation and debate, dissemination of extreme, false, and misleading content, and degradation of essential communications services.

Generative AI, reinforced by the monopoly power of the dominant gatekeeper platforms, appears already to be

amplifying these harms in several ways.
Perhaps most dramatically, generative AI tools are reducing the cost and time needed to produce false and misleading information.[63] Chatbots like ChatGPT are already demonstrating an almost unlimited capacity to generate false information and narratives on various topics. To cite just one example, researchers at NewsGuard successfully prompted ChatGPT to claim, in the voice of anti-vaccine advocate Joseph Mercola, that Pfizer secretly added organic compounds to vaccines to lower health risks for children.[64] The capabilities of generative AI models and tools are so wide-ranging that they are already being used to produce pornographic deep fake videos of real women (without their consent)[65] and fake videos of terrorist attacks on critical infrastructure.[66] The models have also demonstrated a worrying ability to fabricate sources and carefully embed them in convincing prose.

Of course, the problem of technology being used to create and disseminate false and problematic content is not new. Conspiracy theorists, propagandists, and other distorters of the truth have long been early adopters of new technologies to spread false information. But generative AI is taking an existing crisis of trust in news and making it dramatically more acute by suddenly and drastically cutting the time, cost, and skill needed to create such misinformation. Combined with the systemic scale of the social networking and communications platforms controlled by these same corporations, and their generalized failure to prevent their customers from disseminating harmful content on those networks, generative AI is swiftly destroying our ability to trust what we read and view on our screens.

Generative AI also poses a clear threat to the survival of a financially independent press, building on the damage already inflicted on news media by the dominance and business models of Google, Facebook, and Twitter. This is because when ChatGPT, Bard, Bing, and other chatbots scrape and aggregate text from the web to *learn* to generate the best answers to user prompts, they are doing so by processing information largely provided by news organizations, blogs, and independent websites.[67] Their answers also greatly reduce the need to go to the original source, thus preventing publishers from receiving traffic and ultimately compensation for their content.

To make matters worse, Google is in the process of incorporating detailed AI-generated results into its search engine – the so-called Search Generative Experience – which will further reduce the flow of traffic and revenues to third-party websites while entrenching even deeper Google's advertising dominance and monopoly power.[68] If websites and publishers respond by restricting access and putting up paywalls (as indeed they already are), then the amount of reliable and up-to-date information available to the public will shrink further, while results produced by generative AI tools will continue to degrade the overall quality of what is available.[69] Meanwhile, plans by Google and Meta to reinforce their advertising dominance through generative AI threaten to further weaken the financial health of the media industry, while also making it yet harder for individuals to find and share trustworthy information.

EVER MORE EXTREME TARGETED MANIPULATION AND DISCRIMINATION

Surveillance advertising, whereby dominant tech companies intrusively collect huge quantities of sensitive personal data in order to more accurately target information and advertising at users, accounts for the vast majority of revenues for Google and Meta. Today, most digital advertising across the web is underpinned by platforms and tools run by the two giants, and to a growing degree Amazon and Apple. Amazon's advertising business, which consists primarily of ads appearing within its search results, generated $38 billion in revenues in 2022 and is expected to continue growing.[70]

To protect this business model – which has jarringly

disrupted carefully crafted and long-established political and economic balances within the news media and advertising industries – the tech giants have spent much of the last 15 years constructing a narrative that disguises the invasive harvesting of personal data as a harmless and inevitable part of a thriving digital economy.[71] The commercial imperative to maximize users' exposure to targeted advertising has also been blamed for the platforms' failure to develop or even enforce effective content moderation practices. The basic idea is that to keep users online and collect as much data as possible, the gatekeeper corporations have an interest in promoting inflammatory and viral material over more nuanced and less addictive types of content.

The data-intensive nature of large-scale AI models and generative AI tools is already resulting in new forms and new degrees of violation of user privacy. A recent class action lawsuit launched in California alleges that OpenAI violated the privacy of millions of people when it harvested their social media comments, blog posts, and other content to train its models.[72] The company is also being investigated by the Federal Trade Commission (FTC) for its data security practices.[73] In Europe, ChatGPT was temporarily banned in Italy for leaking users' private conversations and payment information, while data privacy and consumer protection regulators in France, Germany, and Hungary have launched their own probes into the chatbot's compliance with the EU's General Data Protection Regulation (GDPR) and other laws.

The integration of generative AI with the surveillance-driven business models of Google, Meta, and others is now taking this targeted manipulation to another level entirely. Combined with the large swaths of personal and non-personal data already controlled by these corporations – including data on what promotional and manipulative tactics have worked most effectively so far on each particular individual – generative AI is empowering the gatekeeper corporations and advertisers to create and disseminate content designed to manipulate individual customers with extreme precision, while also increasing the time they spend online and on particular online websites and platforms.[74] This in turn is reinforcing the tech giants' efforts to gather, store, and use personal data, further undermining our privacy. Researchers predict that this one-two punch of monopolistic scale and precise personalized manipulation will worsen the online addiction, anxiety, eating disorders, and other mental health issues associated with social media use.[75] [76]

More concretely, Google and Meta are already rolling out generative AI-powered services to advertisers.[77] This means that advertisers, instead of having to rely on a set number of images and captions for an advertising campaign, will be able to prompt AI to automatically generate images and text tailored to distinct small audiences and even particular individuals.[78] Generative AI thus threatens to further entrench the market dominance of the digital advertising giants, increasing their ability to target and manipulate users with a level of precision stratospherically beyond the reach of potential competitors.

Even if generative AI-powered advertising ends up not being as novel or effective as its purveyors claim, the sheer dominance of Google, Meta, and Amazon over online advertising means that these models are likely to become widespread regardless. This combination of dominance and inefficiency – and even outright sloppiness and destructiveness – is by no means new. Despite their ubiquity across today's digital advertising supply chain, there is little evidence that Google and Meta's platforms benefit publishers and advertisers, and plenty of evidence to the contrary. A July 2023 study by advertising research group Adalytics found that around 80% of Google's video-ad placements on third-party websites violated the corporation's own standards.[79] Facebook has repeatedly been accused of inflating the size of audiences

exposed to its ads[80] and allowing scam ads to proliferate on its networks.[81] As one former advertising executive turned critic recently put it, the industry's incentive structures are "fundamentally flawed" and its operating models "inherently conflicted."[82]

Generative AI-powered advertising also risks amplifying discrimination based on ethnicity, sex, religion, and other protected categories, including in relation to advertising for housing, credit, and employment opportunities. We have already seen how ad-targeting tools, as they are used today, can cause substantial harm to vulnerable communities. One well-known example is a Justice Department investigation of Facebook that found that the corporation allowed the placement of discriminatory housing ads that violated federal law.[83] A similar study by AlgorithmWatch showed that Facebook relies on crude gender stereotypes when deciding who to target with job ads.[84] It is not hard to see how generative AI, based on its ability to expedite hyper-targeted ads across these same flawed models, will make such discrimination far more prevalent and dangerous.

The same AI technologies that are empowering Google, Meta, and other dominant gatekeeper corporations to turbocharge their use of hyper targeted ads are also amplifying their ability to exploit their existing abilities to manipulate the behavior of individuals in a variety of other ways. This is true both in terms of what people buy and read, and how they vote and otherwise engage in political activity.

NON-DISCRIMINATION RULES AS ANTI-MONOPOLY POLICY: A SHORT HISTORY

A key contributor to the digital gatekeepers' power is the failure of U.S. and other regulators to apply traditional common carrier-style non-discrimination rules to the online gatekeepers, despite the fact that these corporations control many essential commercial and communications platforms. Until the 1980s, such rules provided perhaps the single-most important foundation for preventing the consolidation of power and control in the hands of the corporations that controlled vital networks. Such rules have traditionally provided the main basis for the protection of the properties of independent businesses and the individuals who depend on these services, and hence have also played a fundamental role in the protection of human liberty and democracy.

A useful recent example of how these laws and rules are designed to work is the 'net neutrality' regulations applied to internet service providers in the United States by the Federal Communications Commission in 2015. These rules were designed to ensure that executives at these corporations were not left free to exercise arbitrary power over the businesses that relied on their services, such as via threats to cut off, reduce, or otherwise alter the services and access they provide to specific customers. (Although the Trump Administration overturned these regulations in 2018, FCC Chair Jessica Rosenworcel has made clear that restoring them is a top priority.)[85]

The imposition of net neutrality rules on the backbone physical infrastructure of the internet was simply the latest example of a traditional approach to regulating the power of corporations that control essential services. In the United States, Congress has applied such regulation to every essential communications and commercial platform in the nation's history, including the telephone, telegraph, railroad, trucking, ocean shipping industries, and even the Postal Service. Through a related set of laws, U.S. policymakers also applied these same principles and rules to services such as retailing and warehousing.

The basic idea of such regulation is that every individual has a right to equal treatment by every provider of essential services, much in the same way that individuals have a right to equal justice before the state. A closely related idea behind such rules is the understanding that failure to enforce such equal access allows powerful gatekeeper corporations to all but routinely extract wealth and political favors from the businesses and people who rely on them to get to market – through the simple threat to close the gate to the market to anyone who does not bend to their wishes. Traditionally, such actions were viewed as extortionary in nature. Worse, policymakers believed that such relationships resulted in extremely dangerous concentrations of political power in the hands of gatekeeper corporations.

In the United States, the single most important example of such regulation is the Interstate Commerce Act (ICA) of 1887, through which the federal government applied such rules to the railroad corporations. In 1910, Congress then extended the ICA to cover also the telegraph, telephone, and wireless industries, as well as other essential services. The relative importance of such non-discrimination regulation is made clear by the fact that it was only three years after the ICA that Congress passed the Sherman Antitrust Act. Indeed, Senator Sherman himself, in the debate over the law that bears his name, reiterated the fundamental role of non-discrimination rules when he said: "It is the right of every man to work, labor, and produce in any lawful vocation *and to transport his production on equal terms and conditions and under like circumstances*. This is industrial liberty, and lies at the foundation of the equality of all rights and privileges." (*emphasis added).*

In the absence of strict non-discrimination requirements imposed on their operations (see table above) Google, Amazon, Meta, and the other platform monopolists built business models designed specifically to extort individual people and businesses in their capacities as sellers and publishers. In doing so, they have routinized behavior that would have been recognized as completely illegal as recently as the 1990s.

In addition, Google, Amazon, Meta, and the other platform monopolists have done something that previous generations of network monopolists could hardly imagine, which is to apply these same systems of tailored manipulation and discrimination to individual consumers. These gatekeeper corporations were able to do so by taking advantage of their rapidly growing abilities to gather, store, and manage data about the interests, behaviors, and actions of individual people.

Perhaps the most immediately useful explanation for how such a system works was provided by Hal Varian, now the chief economist at Google. In a paper he co-wrote in 2001, titled "Conditioning Prices on Purchase History," Varian described how the technologies and structures of online commerce were making it easier for sellers to charge different people different prices for the same product.[86] "The rapid advance in information technology now makes it feasible for sellers to condition their price offers on consumers' prior purchase behavior," Varian and his co-author wrote. Indeed, not only was such targeting now feasible, it was also "profitable to engage in this form of price discrimination."

Varian then provided a blunt recommendation to online sellers. "[I]f enough customers are myopic, or the costs of anonymizing technologies are too high... sellers will want to condition pricing on purchase history." For buyers his warning was even more blunt. "[P]urchasing at a high price ... guarantees that [you, the consumer] will face a high price in the future."

From the point of view of the individual buyer or customer, the overarching result is a system of economic exploitation and political manipulation that goes far beyond so-called 'dynamic' pricing models, whereby prices automatically adjust supposedly in response to fluctuations in supply and demand.

In the late 19th century, railroad bosses spoke of how they used discriminatory pricing strategies to charge businesses that relied on their services "all that the traffic will bear." Today, Google, Amazon, Uber, Ticketmaster, and a fast growing array of other corporations use amped up versions of these same practices to extract all that the individual consumer is willing to pay, increasingly through automated systems carefully designed to identify with extreme precision the size of this consumer surplus.

EXPLOITATION AND MANIPULATION OF SELLERS AND PUBLISHERS

The introduction of AI technologies is already rapidly increasing the ability of the gatekeeper platforms to more effectively manipulate sellers and publishers in much the same way it is boosting the ability of these corporations to manipulate and exploit the individual consumer. The FTC's new case against Amazon provides important insight into how this power is being put to work in today's digital political economy.[87]

But it is important also to understand the political effects of such power applied over long periods of time by these immensely powerful gatekeeper corporations, even to other extremely large and influential corporations, such as NewsCorp, the New York Times, Penguin Random House, and Paramount, as well as otherwise all-dominant manufacturers such as Procter & Gamble.

The tech giants have repeatedly shown us that their core goal is not merely to shut out challengers, nor is it mainly even to lock users and small businesses into using their products and services. Nor is it simply to exploit their

position as gatekeepers to extract wealth, properties, and ideas from the businesses, contractors, and individuals who depend on their platforms to get to market and to exchange their ideas. Rather it is also to impose various forms of politically useful influence and control over the businesses and individuals who depend on them to get to market.

The key political fact of political economics today is that the monopolization of essential commercial and communications platforms – as well as everything from search and mapping engines, social media platforms, digital advertising systems, e-commerce platforms, email and operating systems, app stores, cloud computing, and now AI infrastructure – has given this handful of corporations the power to decide who gets access to the market and on what terms. This control of these gateways gives Amazon, Apple, Google, and other platforms the ability to discriminate based on price and other factors, set the terms and conditions governing how they do business, and degrade or cut off access at will.[88]

This gatekeeper position *also* empowers these corporations to extract political value from these captive customers. One of the most obvious such benefits is the ability to stifle criticism from any seller or publisher who might choose to complain in public, through the threat of direct and perhaps commercially fatal retribution for speaking up.[89]

Perhaps the most useful model for understanding how such systems of control threaten our democracy and fundamental liberties is to focus on how Google, Facebook, Amazon, and now Twitter under Elon Musk have exploited their gatekeeper positions to cut off revenue and readers from even the most powerful news and information publishers in the world.

The first major instance of one of these platforms exploiting its power to cut off a publisher's access to market came in 2014 when Amazon stopped selling books published by Hachette, as part of an effort to force that company to pay more for Amazon's services.[90] A second example is Google's reported use of its control over Gmail to suppress the campaign literature of particular U.S. presidential candidates, while simultaneously boosting the advertising of their rivals.[91] Another example was the collapse of traffic from Facebook to *Wired* in February 2018, after that magazine published an article critical of Mark Zuckerberg.[92] More recently, Facebook cut off the ability of Canadians to share news with one another and threatened to do the same to Californians.[93]

Some of the most egregious examples have happened on Twitter in the year since Musk took full control. This includes the cutoff of access of individual journalists, researchers, entire news publications, and research and advocacy organizations.[94]

The ultimate political result of such a system – combining control over the gate with a de facto license to open or close the gate at will – was well captured by *Wired's* then executive editor Nicholas Thompson in 2018. "Every publisher knows that, at best, they are sharecroppers on Facebook's massive industrial farm," he wrote. "If Facebook wanted to, it could quietly turn any number of dials that would harm a publisher, by manipulating its traffic, its ad network, or its readers."[95]

The political effects of such exercises of power are obvious, which is to make every publisher today – and increasingly each individual employee of these businesses – think twice about criticizing or even questioning the power of Google, Meta, Amazon, or any other corporation that enjoys the power to arbitrarily, at a moment's whim, cut them off from revenue, readers, and markets.

And now AI is dramatically amplifying this existing ability of these already immensely powerful gatekeepers to suppress, censor, or simply choke off anyone whose actions or speech does not please them.

EXCLUSION OF RIVALS AND UNDERMINING OF INNOVATION

This same gatekeeping power also gives these dominant corporations the ability to suppress, exclude, and eliminate potential rivals through a variety of monopolistic tactics. While this is not the place for an exhaustive review, such practices include tying or bundling different products and services together; self-preferencing proprietary services through control over multiple layers of the supply chain; using data gathered from sellers to compete against them; restricting or denying access to data, infrastructure, and other critical inputs; and using acquisitions to extinguish or absorb future competitors.

Notable historical examples of such tactics include Microsoft's attempt to choke off rival internet browser Netscape by the bundling its own browser with its already dominant operating system,[96] Google's self-preferencing of its own services across the highly lucrative ad-tech supply chain,[97] Amazon's use of seller data to benefit its own retail business,[98] and Facebook's acquisitions of potential rivals Instagram and WhatsApp.

AI technologies have already empowered dominant gatekeepers to further perfect these practices. When it comes to tying, bundling, and self-preferencing – all of which are based on leveraging control over multiple markets and products to disadvantage rivals – the already existing power of Microsoft, Google, Apple, Meta, and Amazon across different product markets (including search, advertising, operating systems, cloud, and hardware) presents them with a myriad of opportunities both to extend their dominance over AI, and to simultaneously use AI to reinforce their existing dominance elsewhere.

Microsoft, for instance, has integrated OpenAI's technology into its Edge browser and Bing search engine,[99] and is beginning to do the same in relation to its dominant Office software, Windows operating system, Outlook email service, Azure cloud platform, and more. The same applies to Google, which is using AI to strengthen the moat surrounding its ubiquitous email, maps, shopping, and other services. Indeed, Google has already announced that only developers who use its cloud platform will be able to access the Pathways Language Model, one of its most powerful AI tools.[100] And it is in the process of integrating its Bard chatbot into its search engine, simultaneously reinforcing its search monopoly while also locking users into its AI tools.

As discussed earlier, Amazon is attempting to position itself as *the* platform for AI innovation by hosting AI models and services directly on its cloud infrastructure. Should Amazon succeed in securing this position, it could use this to exert power over and extract value from businesses dependent on that infrastructure, just as it does with sellers on its marketplace. It will also have the ability and incentive to self-preference its own AI models and tools and those produced by its partners and investees, such as Anthropic, and to copy or disadvantage potential competitive threats.

Another area where the largest gatekeepers are in a strong position to exploit their market power is through their control over the crucial inputs needed to train AI models, particularly computing power and data. This is not merely hypothetical. An early example of this is Microsoft's recent threat to cut off access to its Bing search-index data to smaller search engines such as DuckDuckGo that use this data to train their own AI applications.[101]

But in many, if not most, cases the behavior is likely to be more subtle; for example, an incumbent providing access to its AI capabilities could limit or downgrade this access in order to protect its market share. A recent study by the UK's communications regulator, Ofcom, found that leading cloud players use technical restrictions on interoperability to limit how well their platforms work with services offered by rivals, and that access often starts off open but narrows over time.[102]

THE THREAT TO CREATORS AND CREATIVE PROPERTY

For more than two decades, the authors and publishers of news, books, music, photography, and other forms of easily digitizable materials have fought with little success to protect their copyrighted properties and livelihoods from the power of the platform monopolists. This includes a long list of lawsuits against Google and other corporations for not preventing individuals and businesses from sharing copyrighted materials on platforms ranging from YouTube to Google News without permission. Such transmission of data all but eliminates the ability of copyright owners to get paid for their work, while also removing most of the incentives for consumers to pay for what they read, watch, and listen to.

Now the rapid rollout of generative AI is taking this existing suite of problems and amplifying it at an almost astronomical rate, in four specific ways.

The first new question posed by AI is how creators will be paid for the use of their materials in training foundation models and applications such as ChatGPT and search engines. The U.S. Copyright Office has launched an inquiry into these issues, to assess whether copyright laws need to be updated in response to AI. The IAC – one of the world's largest internet holding companies and home to digital publishers such as DotDash Meredith – recently warned in its comment to the Copyright Office that if generative AI firms don't pay publishers for copyrighted content, the technology will undercut not only the news media industry, but all kinds of other web publications that deliver reliable and safe information.[103]

A second new question posed by AI is whether it can be used to create art that until now has required human beings as producers – such as music, books, news, and films. For writers, this threat is so tangible that prohibiting the indiscriminate use of AI-generated text in screenwriting was a key demand during the five-month strike led this year by the Writers Guild of America, which successfully secured the guarantees it demanded.[104] As the Open Markets Institute put it in a letter to the U.S. Copyright office: "Enforcing copyright laws and requiring companies to meet their legal obligations – whether that is compensating rights holders or ensuring transparency of training data – are critical in order to protect human creativity and reward the labor that goes into it."[105]

A related set of questions arise over whether ideas and inventions generated by AI models should be granted patents, and if so, who gets the credit. These concerns are not just hypothetical. An analysis by the *Washington Post* of a major data set used by Google and Meta's main LLMs found that the biggest single category of websites were patent, business, and industrial sites including Kickstarter and Patreon, raising concerns that the technology may copy businesses' and creators' original ideas in suggestions to users.[106] Granting patent rights to AI models poses a wide variety of risks to the entire system of intellectual copyright. One potential risk is simply empowering large corporations to further reinforce their dominance. For example, a pharmaceutical corporation that owned the largest datasets on chemical structures and prescriptions could use AI to mass-generate patents for potential new drug compounds, driving market concentration and excluding rivals.

Finally, generative AI is enabling dominant retail platforms like Amazon and music streaming services like Spotify to host and promote AI-generated books, music, and similar products. Writers are reporting that Amazon is recommending AI-generated rip-offs of their own published books on its marketplace.[107] Meanwhile, the e-commerce giant refuses to disclose how many of these bogus publications it prevents from being published or how many it takes down.[108] Spotify not only generates revenues from AI-generated music that violates copyright[109] but hosts an undisclosed number of bots that act as listeners of both AI-generated song rip-offs and real artists – effectively reducing royalties for the latter.[110]

THE THREAT TO WORKERS AND JOBS

The debate on the impact of automation and AI on jobs long predates the emergence of generative AI. On the one hand, many of the fears surrounding the impact of specific technologies on employment – be it the automobile or ATMs – have proved to be overblown. On the other, there is clear evidence that automation over the past few decades has increased inequality[111] and disproportionately harmed specific communities,[112] even if it hasn't led to mass unemployment. There is ample evidence, meanwhile, that communities disproportionately impacted by automation have in turn become more politically polarized, undermining the integrity and stability of democracy.[113]

It is too early to say with certainty whether AI specifically (as opposed to automation more generally) will have a net positive or negative affect on employment. Studies diverge significantly in their predictions, with much depending on whether AI is implemented in a way that supports and augments human labor, or replaces and degrades it. Generative AI's generalized capabilities and ability to execute more complex tasks – including drafting essays, writing code, and creating images – could expose more 'white collar' work to automation, although the low-quality of much AI generated output to date puts this in doubt for the time being. What is clear however is that concentrated ownership of the technologies driving automation will result in similar concentration among the corporations and individuals that enjoy the financial rewards.

At the individual level, many of the dominant tech firms, and Amazon in particular, have a long track record of either surveilling workers themselves or giving other employers the tools to do so. Examples include Amazon's aggressive surveillance of its warehouse workers and delivery contractors,[114] Google spying on its white-collar employees,[115] and workplace tools provided by Microsoft and Google that enable invasive monitoring of individual workers.[116] These abuses, many of which are already enabled by AI, could foreseeably be made worse by generative AI. For example, these corporations and other employers could use chatbots and other generative AI tools to manipulate or coerce their staff, or to make decisions affecting employees that they are unable to grasp or challenge.

Automation also risks aggravating worker exploitation and inequality in the form of wage discrimination.[117] As documented by academic Veena Dubal, tech giants including Uber and Amazon increasingly compensate their workers and contractors based on sensitive data and performance indicators unknown to those workers, and which they therefore cannot control.[118] This not only subverts the principle of equal pay for equal work, but amplifies discrimination and impairs economic mobility. Further advances in AI, combined with the monopsony power that economic concentration gives dominant corporations over their workers, threaten to take these abusive practices to the next level.

THE THREAT TO RESILIENCE AND SECURITY

Allowing major companies and even industries to become dependent on a small number of technology giants for critical inputs not only concentrates control over technological innovation and the financial returns to that innovation in a few hands, it also concentrates many forms of physical and systemic risk.

The concentration of power and control over cloud computing capacity and foundation models by the largest gatekeeper platforms, for instance, poses a number of large threats to the resilience and security of many of the basic commercial and information systems on which our society depends. To give just one example, a major outage of Amazon's cloud services in June 2023 hit sectors including transportation and financial services, and organizations including Southwest Airlines, the U.S.

securities regulator, the New York Metropolitan Transportation Authority, and the Boston Globe.[119]

The severe disruptions caused by the Covid-19 pandemic, the Russian invasion of Ukraine, and other crises to global supplies of oil, gas, wheat, and semiconductors, and to ocean and rail freight systems, have amply demonstrated the dangers posed by extreme chokepointing of manufacturing and transportation capacities in a handful of companies and places. Drawing on that experience, it should be clear that to allow a few immensely powerful corporations to control both the leading large-scale AI models and the cloud infrastructure those models are trained and hosted on will concentrate risk as well as capacity and control, in ways that set up these highly centralized systems to fail in potentially catastrophic fashion.

A further level of risk is created as generative AI, and AI in general, is rapidly embraced by sectors generally understood to be systemically important, from financial services and energy to defense and transport. In financial services, for example, Goldman Sachs is exploring the potential of generative AI to classify millions of documents, including legal contracts,[120] while JPMorgan is developing a chatbot to help customers select their investments.[121] In energy, potential use cases include demand forecasting, grid management, energy trading, and supporting customers in monitoring energy usage,[122] while the U.S. military has confirmed it is exploring how generative AI can help it generate information and improve decision-making.[123] In the automotive space, Amazon has sought to promote the role of generative AI in autonomous driving systems.[124]

Outright failure of the generative AI services or cloud infrastructure provided by this oligopoly, with potentially existential cascading effects across key industries and systems, is the most straightforward threat to envision. But even without this worst-case scenario, systemic harm could be inflicted by serious flaws in AI models, including everything from faulty data to manipulation and sabotage by malicious actors.

Gary Gensler, chair of the influential U.S. Securities and Exchange Commission, has expressed deep concerns about these and related issues. Recently he warned that the dependence of financial institutions on models and data provided by Microsoft, Google, and other dominant gatekeeper corporations, as well as the fast-growing ability of AI to concentrate and exacerbate certain risks, threatens to trigger a financial crisis within a decade.[125] As he explained in a 2020 paper when he was teaching at MIT, reliance on the AI services of a few players would expose the financial sector to an extremely dangerous combination of single points of failure and the amplification of herd-like behavior among individual investors and other actors.[126]

Similar arguments can easily be applied to other activities, from AI-generated deepfakes and disinformation spreading at lightning speed on social media, to fatal accidents in AI-powered autonomous vehicles and inefficiencies or failures in an AI-regulated energy grid. One recent paper gave the hypothetical example of a foundation model used for the majority of medical diagnoses, which if flawed could lead to systematic misdiagnoses and misprescribed remedies – a problem that would be particularly catastrophic during a health emergency such as a pandemic.[127] The key point is not that AI should not be used in critical sectors, but that market concentration will greatly amplify problems when things inevitably go wrong.

IV: SOLUTIONS

As we have seen, today's digital monopolies are the driving force behind the latest advances in AI. They have achieved this position largely by buying up leading technologies and startups and leveraging their already enormous existing powers and capabilities to impose their particular AI strategies and business models on the world.

As we have also seen, these same online gatekeeper corporations are aggressively wielding these new technologies, as well as their control of most key links in the AI supply chain, to reinforce their existing monopolies across the digital economy. And, of perhaps greatest immediate concern, these corporations are also using these new technologies to amplify and accelerate many of their most dangerous present behaviors. This includes reinforcing business models based largely on manipulating and extorting almost every business and individual that depends on their services in ways that distort public discourse, threaten democracy, violate fundamental political liberties, undermine property rights, and degrade online services.

The tech giants' tightening grip over artificial intelligence technologies and infrastructure also puts them in prime position to shape the direction and nature of AI innovation. As it stands, a handful of giant corporations already have the power to largely determine – either directly or through the control they exert over other actors – what AI looks like, how it works, how it impacts our jobs and lives, and whose interests it serves. In this bleak vision of the future, the great majority of those affected by AI – be they citizens, businesses, workers, consumers, and even the state itself – will be dependent rule takers rather than independent rule makers.

Fortunately, a different future is possible, one in which today's gatekeepers no longer control and exploit the key platforms and technologies of AI. By imposing strict limitations on their behaviors and through careful restructuring of their businesses, the citizens of the United States, Europe, and other nations can repurpose these corporations to serve the public interest – or at least not work against it. This in turn would create the space for a broad democratization of AI and other technologies now monopolized by these corporations, in ways that empower a diverse set of actors - including independent businesses, universities, public bodies, civil society groups, and individual people - to play a far greater role in the design, use, and improvement of these technologies and services.

Bringing about this future will require us to accelerate our efforts to break and neutralize the power of the digital gatekeepers, a fact that has been largely ignored thus far in the debate on AI. The good news is that focusing on the intersection of AI and power teaches us that we can achieve most of our most important goals using already existing law and institutions.

AI REGULATION THUS FAR: NECESSARY FIRST STEPS BUT FAR FROM SUFFICIENT

Policymakers and experts are currently focusing their efforts on establishing regulatory frameworks that place guardrails around how AI is designed, brought to market, and deployed. Such guardrails include requiring organizations to scrutinize their algorithms for bias, introducing greater transparency on how their AI systems make decisions, and providing avenues for challenging automated decision-making, including through human review. But in these discussions, the question of *who* controls the technology – and how that *power* is used – rarely surfaces.

One of the earliest significant regulatory initiatives was the European Union's AI Act, published in April 2021,

which seeks to impose horizontal obligations on the use of AI by public and private actors. The most notable feature of the Act is its so-called "risk-based approach," according to which the toughest requirements apply to AI use cases perceived as posing "unacceptable" or "high" levels of risk, such as AI used in facial recognition or worker surveillance.

The AI Act's provisions range from outright bans for unacceptable use cases and mandatory risk assessments and security measures for high-risk AI, to light-touch transparency obligations for "limited risk" applications. At the time of publication, the Act has not yet completed its passage through the EU legislative process, and changes are to be expected. Significantly, the European Parliament is pushing to ensure the Act also applies to AI foundation models, a move which has faced opposition from certain corporations and EU Member States.[128]

In the U.S., the Executive Order on AI issued by President Biden in October 2023 demonstrated that the White House clearly intends to ensure safety and security in artificial intelligence. Key measures include developing standards on safe and trustworthy AI, requiring developers of powerful AI systems to share safety test results with the government, and instructing agencies to protect consumers and workers from algorithmic harms and discrimination across a variety of fields, including education, criminal justice, healthcare and housing. Crucially, the EO's holistic approach makes clear that government intervention should protect not only the privacy and civil rights of individuals, but also our wellbeing and liberty as workers, consumers, workers, entrepreneurs, and independent business owners.

Going forward, it is vital to approach all such regulation of specific risks posed by AI with great care. Such regulation is necessary to ensure that corporations and governments do not use the technology in unethical and harmful ways. But we must be alert to the risk that such regulation, if poorly designed, can be exploited by the biggest corporations to further entrench their dominance over both this suite of technologies and the rules that govern its use. The reason is simple. Government regulators of complex technologies often adopt complex and costly rules that can prove onerous for smaller and medium-sized businesses – thus deepening the advantage dominant corporations already enjoy thanks to their greater size and resources. This well documented fact may help to explain why, as discussed earlier, many of the dominant tech corporations have spoken out publicly in favor of AI regulation. Perhaps the best recent example of how such regulation can actually help or at least fail to rein in incumbents is the ongoing difficulty in enforcing the European Commission's General Data Protection Regulation (GDPR).[129]

More problematic yet are the voluntary initiatives introduced by the tech industry itself, ostensibly to ensure that AI is deployed responsibly and ethically. These initiatives include the AI ethics teams established by individual large companies, as well as alliances such as the Partnership on AI, a coalition founded by Amazon, Facebook, Google, DeepMind, Microsoft, and IBM in 2016 and which now counts a large number of non-profit actors among its membership. Recently, leading AI companies have sought to use self-regulation to deflect mounting concerns over the safety of their products. These include a set of vague voluntary commitments made by seven companies at the behest of the Biden administration,[130] and the launch of a "Frontier Model Forum" by Microsoft and Google, along with OpenAI and Anthropic.[131]

Serious questions about the intentions and effectiveness of such voluntary, industry-led initiatives are raised by the fact that many of these projects have already been watered down or entirely abandoned. Google's AI advisory board, established and shut down within the space of a fortnight, surely holds the record for most short-lived. And as seen earlier, that corporation subsequently forced out leading AI ethics researcher Timnit Gebru after she

HARM(S)	SOLUTION(S)
Discrimination and manipulation by dominant AI and cloud gatekeepers against customers.	Ban discrimination by powerful gatekeeper platforms providing essential services.
Leveraging of monopoly power in cloud to control AI; monopolistic conduct by dominant cloud providers.	Separate ownership and control of the cloud from gatekeeper platforms; regulate cloud platforms as utilities.
Concentration of data ownership; exploitation of this advantage to dominate AI.	Establish public-interest data regime to govern access to data collected by gatekeeper platforms.
Use without permission of creative property to train AI models and tools.	Aggressively enforce copyright laws to protect creative property; audit use of copyrighted material in AI systems.
Threat to resilience and national security from concentration of key technological capabilities.	Use government investment and procurement policies to break chokepoints; map the impact of gatekeeper corporations on national security.
Market concentration through by anti-competitive deals between gatekeepers and challengers/startups.	Block and reverse gatekeeper efforts to control AI through mergers, investments and partnerships.
Surveillance and exploitation of workers through AI and AI-augmented means.	Establish bright-line rules to limit digital exploitation of workers and contractors.
Privacy violations from illegal/unethical use of personal data to train AI models and tools.	Increase strategic collaboration between competition law enforcers and data protection regulators.

Figure 5: Overview of AI concentration harms and solutions

raised uncomfortable questions about the safety of its AI models. More recently, the race to dominate AI regardless of the consequences has led to large tech firms – including Microsoft, Meta, Amazon, Google, and Twitter – cutting, and in some cases entirely liquidating, teams working on ethical AI and trust and safety.[132]

USING COMPETITION POLICY TO KEEP AI SAFE, OPEN, AND ACCOUNTABLE

By failing to apply to today's digital gatekeepers the rules and measures historically used to rein in dominant corporations in other industries, policymakers now find themselves scrambling to address the many harms this unchecked dominance has inflicted on our democracies and economies – a task that AI makes both more urgent and more difficult.

Precisely because AI is so worrying in so many ways, it is vital that policymakers learn the lessons of the past and use competition policy to ensure this powerful new technology is designed and used in the public interest. Doing so will not only protect the public and enable it to take full advantage of AI's benefits, but will also make it easier to apply other forms of regulation – including privacy, consumer protection, and health and safety rules – to today's dominant corporations.

Above all, regulators should focus on studying and addressing AI's role in amplifying and accelerating existing monopoly harms, before moving onto emerging and hypothetical threats.

To maximize their chances of success, enforcers and policymakers should be guided by four core principles:

I. Establish a clear hierarchy of goals for regulatory action, to help prioritize the use of limited resources.

Given limited resources, and the scale of the challenge at hand, it is crucial that lawmakers and regulators establish a clear hierarchy of goals for regulatory action. The top priority should be tackling threats to individual liberty and democratic institutions, which are essential if we are to break and harness the power of the online gatekeeper corporations that now threaten us. This in turn implies a close and immediate focus on the many ways in which the *existing* power and *existing* behaviors of these immense, privately controlled gatekeepers threaten our ability to communicate and debate, gather and share news, and do business directly with one another. Questions of technological innovation should be of secondary importance compared to making these platforms safe for democracy. That said, given sufficient resources, law enforcers can *also* focus simultaneously on promoting an open and competitive political economy. Indeed, many actions that would protect our core political rights and interests would also begin to provide individuals and businesses with greater opportunity to promote innovation and to master AI and other new technologies in the public interest.

II. Make aggressive use of existing law, and invest in legislation and new regulatory institutions only where there's a clear need and reasonable chance of success.

Many governments already possess wide-ranging powers that can be deployed now to prevent today's monopolists from using AI to further cement their power and more effectively exploit and manipulate individual people and companies, as well as to unwind dangerous existing concentrations of capacity and control. These powers include competition law and policy, trade policy, consumer protection laws, privacy regulation, and copyright protection. This approach is especially important in the United States, where there is an extremely vast and robust collection of powerful laws and regulatory regimes to address such threats, built up and refined over the course of more than two centuries, and where longstanding gridlock in Congress makes it unlikely the institution will pass new competition laws soon.

III. Accelerate efforts to adapt existing competition law to address today's threats.

Law enforcers and lawmakers are engaged in the most fundamental rethinking of competition policy since the Chicago School revolution of the early 1980s and in some respects since the New Deal. In the United States, Europe, and elsewhere, enforcers are scrambling to restore traditional pre-Chicago School goals, principles, and analysis, as we see in the new draft merger guidelines published by the Department of Justice and Federal Trade Commission. Lawmakers and enforcers are also moving to adapt and update those regimes for the digital age, as we see in new European laws such as the Digital Markets Act and Digital Services Act and in the wide-ranging lawsuits by both the federal and state governments in the United States against Google, Amazon, and Facebook. This effort is still, however, in its early stages. It is vital to immediately extend this effort to cover how we treat such factors as control of data and computing capacity, including directly in relation to AI. It is also vital to move swiftly to integrate this effort with legal and regulatory regimes that intersect with antitrust, including communications, trade, privacy, copyright, and consumer protection, among others.

IV. Ensure that dominant corporations in control of essential platforms and services treat all users the same.

A core tenet of competition policy is the requirement that private corporations that control essential services do not discriminate in the delivery of these services, and provide equal access to all comers. As Senator John Sherman said in a speech in favor of the U.S. antitrust law that bears his name, such regulations lie "at the foundation of the equality of all rights and privileges." Today this principle is especially important when addressing the actions and business models of essential communications and commercial platforms, as well as all essential digital and AI infrastructure including cloud computing capacity and foundation models.

IMMEDIATE NEXT STEPS – EIGHT ACTIONS GOVERNMENTS CAN TAKE NOW

The rest of this section sets out what a few such policies could look like, in general terms, while focusing on eight strategic areas of action where law enforcers and lawmakers can swiftly begin to address the gravest dangers posed by AI.

1. Ban all discrimination by powerful gatekeeper platforms in the delivery of essential services to individuals and businesses.

Given the many actual and potential harms that the business models of the dominant gatekeepers already pose to citizens, workers, creators, independent businesses, and consumers – particularly through the automated and personalized discrimination in pricing and delivery of information and services outlined earlier in this report – it is paramount that competition authorities, consumer protection bodies, data protection agencies, and other regulators take swift action – both individually and in concert – to stamp out such practices.

In the United States, both the FCC and FTC have ample authority to establish rules to guide and control the broad behavior of the gatekeepers. At more specific levels – such as the divisions of these gatekeeper corporations that oversee transportation services or intersect with financial services – so do other departments and agencies including the Federal Reserve, Department of Commerce, Department of Treasury, and Department of Transportation, among others. Fortunately, President Biden recognized this broad need in July 2021, in calling for a whole-of-government approach to addressing the threats and harms posed by concentrated economic power and control. But given the proven ability of AI to accelerate and amplify existing monopoly threats and harms, it is vital to upgrade the ability of different agencies to more effectively coordinate in the enforcement of their existing authorities.

Gary Gensler, the chair of the U.S. Securities and Exchange Commission, recently made this point in an interview in which he warned that AI will almost definitely trigger a financial crisis within the next decade. The wide-ranging nature of the threat, Gensler said, poses "a cross-regulatory challenge."

In Europe, the EU has already demonstrated through a variety of recent enforcement actions and legislation – including the Digital Markets Act and the Digital Services Act – that it has a general understanding of the threats posed by the business models of the gatekeeper corporations. So too have the competition law enforcement agencies of some individual nations, especially Germany and the United Kingdom, which have both pursued ambitious antitrust cases against the gatekeepers and significantly expanded their own powers. Here as well however more coordination is needed, both between different European competition authorities and between competition authorities and their counterparts in other areas of regulation.

Encouragingly, competition, consumer protection and other agencies seem attuned to the risks of concentration in AI, and ready to move faster than in the past. In April 2023, four U.S. enforcement agencies issued a joint statement pledging to use their existing powers to crack down on the unlawful use of AI applications in different industries. And in October, the UK's Competition and Markets Authority published a detailed study on the risks of concentration in foundation models. Numerous competition authorities around the world have also undertaken detailed studies of concentration in the cloud and several are investigating anti-competitive conduct in the market for advanced semiconductors.

2. Recognize cloud computing as an essential infrastructure, separate ownership and control from the largest gatekeeper platforms, and regulate it as a utility.

As we have seen, much of the tech giants' emerging power in AI is rooted in their cloud computing dominance and unparalleled access to data. Given their systemic role across the economy and public sector, large cloud computing providers should be regulated as public utilities under common carrier principles, subject to strict obligations on non-discrimination, fair and equal treatment of all customers, and ensuring safety and reliability.

As multiple studies have shown, the cloud computing industry is extremely concentrated, with just three providers (Amazon, Microsoft, and Google) controlling roughly two-thirds of the global market.[133] This figure varies significantly by market, with the combined share of the top three approaching 80% in the UK.[134] As discussed earlier, this concentration creates a wide variety of threats.

This includes the financial threat to any individual business or government that depends on these cloud services, as this concentration of power and control puts the cloud giants in a position to lock in and exploit their customers through excessive switching costs, anti-competitive discounts, arbitrary restrictions on interoperability, and the usage without permission of the data and ideas of their customers.[135] It includes the major threat to economic and societal resilience posed by the reliance of our governments and key industries on a handful of geographically concentrated cloud providers, as illustrated by a number of critical failures in the past.

Despite these threats and the infrastructural, utility-like role played by the dominant cloud platforms, governments have so far failed to put in place the comprehensive regulatory regimes commensurate to this privileged status. While a number of recent initiatives, including the EU's Data Act, Digital Markets Act and Cybersecurity Act, impose a number of standalone responsibilities on cloud platforms, none of these are designed to provide the overall regulatory framework for the structure, management, and behaviors of the dominant cloud providers that is clearly necessary.

Law enforcers should move to immediately impose a non-discrimination regime on the entire cloud industry. Under such a regime, large cloud computing providers would be required by law to treat all customers fairly and equally while ensuring high standards of safety and reliability. This would include refraining from denying service arbitrarily; offering discounts or other benefits to favored customers (including its own vertically integrated business lines) or discriminating against others; and making it unnecessarily difficult to contract with alternative providers. These providers would also be required to uphold the highest standards when it comes to data privacy, cybersecurity, operational resilience and more.

Additional measures are needed to tackle the unavoidable conflicts of interest presented by the concentrated ownership of today's dominant cloud platforms. Even if the likes of Amazon and Microsoft are banned from self-preferencing their own services or discriminating against users, they are likely to continuously find new ways to leverage their dominance in the cloud to strengthen their positions in AI and other areas.

A lasting solution to the conflicts of interest inherent in owning both critical infrastructure and services that rely on that infrastructure would be to force Microsoft, Google, and Amazon to divest their cloud units, and to prevent cloud providers from being active in conflicting lines of business. This would eliminate any ability or incentive on their part to give their proprietary AI models – or those of close partners – special treatment. And it would make the utility-style regulation of cloud providers proposed above far more manageable.

Additionally, a general requirement of interoperability across the wider AI ecosystem would greatly help to prevent today's dominant corporations from using existing structural advantages to eliminate competition and lock in users and customers. In addition to making it easier to move from one cloud system to the next, such obligations could also aim to ensure that foundation model providers can train, host, and run their models across different cloud providers, and that AI developers and applications are able to run queries on different foundation models.[136]

A number of ongoing actions by competition authorities provide avenues for intervention. The CMA is currently undertaking an in-depth market investigation into the sector, which will give it the power to impose structural and behavioral remedies, while the FTC is in the early stages of its own investigation. France's competition authority, noting similar market failures in a recent study, is also considering the need for litigation.[137] Meanwhile the EU's recently passed Data Act contains provisions enabling switching between different cloud providers, while cloud providers are in the scope of its Digital Markets Act.

3. Recognize that any data collected by large platforms in their capacities as essential services is public in nature, and establish a public-interest regime to govern access.

Most of the data collected by the dominant technology platforms through the provision of essential commercial and communications services should be considered public in nature, and therefore governed as a common public resource.

There are various ways this principle could be operationalized in practice. One option would be to require dominant technology firms to share aggregated and anonymized data with other actors, including competitors, startups, public bodies, and non-profit organizations. This would have a number of desirable consequences, from helping companies to develop rival offerings to the AI models and services dominated by these few corporations, to supporting socially beneficial research and innovation at universities and government agencies.[138]

An alternative option would be to task a distinct institution or trust with governing access to the data collected by these corporations whenever they are engaged in the provision of essential communications or commercial services. This entity could be a public body or a certified non-profit intermediary entrusted with data stewardship. It would be responsible for ensuring that the data it holds is stored and shared safely, responsibly, and in compliance with any relevant laws and regulations. The intermediary could also be given – or required to establish – principles and objectives that guide its decision-making in ensuring that the data is used to pursue beneficial rather than harmful ends.[139] This would include a clear system of rules limiting access to the data by law enforcement and other public officials.

Creating a workable public interest regime for data will also require balancing competing objectives and ethical priorities, such as protecting privacy while promoting innovation. A technology known as "federated learning," which allows models and algorithms to be trained on datasets hosted in different places without that data actually being moved or centralized, is one potential path forward.[140]

4. Aggressively enforce copyright laws to protect the properties of authors, creators, and other independent publishers from misappropriation and misuse by gatekeeper corporations, and establish a trustworthy and transparent system for auditing the use of copyrighted material in AI systems.

Given clear evidence of copyright violations by AI models and applications, enforcing existing copyright laws to protect the properties of authors, creators, and other independent publishers from misappropriation and misuse must be an urgent priority. To support this enforcement, corporations should be subject to audits of their use of such copyrighted material to train AI models and applications. Recent calls from across the creative industries in the U.S. and beyond for AI companies to treat their inputs as copyrighted work – and thus be required to obtain consent, provide compensation, and set transparent and fair parameters for use of the outputs generated – show there is strong support for this course of action.[141]

AI also greatly magnifies the longstanding need to rebalance power between publishers and digital monopolies. This time around, the media sector appears far more cognizant of the threat. The News Media Alliance, representing over 2,000 members across the globe, has already put forward principles to govern how generative AI systems use publisher content.[142] Similarly, media leaders from more than 24 countries recently proposed a framework for any country seeking to use regulation to force digital platforms to negotiate with publishers over fair use of their content.[143] And by way of the U.S. Journalism Competition and Preservation Privacy Act, legislators are pushing for publishers to have the right to negotiate compensation with companies using news content to train AI models,[144] mirroring similar initiatives already in force or being implemented in Australia, Canada, the EU, the UK, and other jurisdictions.

5. Clearly map how the structures, behaviors, and business models of the largest gatekeepers threaten national security, including by enabling foreign surveillance and interference. Use government investment and procurement policies to break chokepoints and promote security.

The disruption caused by the Covid-19 pandemic and war in Ukraine have highlighted like never before the dangerous levels of concentration in global supply chains for essential goods and materials, including semiconductors, medical equipment, food, and critical minerals. In response to these shocks, governments and multinationals are taking steps to make supply chains more resilient by promoting diversification of production, including using public funding and incentives to encourage companies

to manufacture more locally and regionally. Notable examples of such initiatives include the U.S. Inflation Reduction Act, the EU and U.S. Chips Acts, and the EU's Critical Raw Materials Act.

Building on this experience, there are steps governments can already take to ensure that our growing reliance on AI does not create new vulnerabilities. To start with, governments should clearly map how the structures, behaviors, and business models of the largest gatekeepers threaten national security, and identify practical means of addressing this. They should focus especially closely on the ways that various platforms and business models within Google, Meta, Amazon, Apple, Microsoft, and Twitter provide foreign states and non-state antagonists with the ability to disrupt commercial, communications, or political systems in the United States, Europe, and other nations.

Industrial policy, broadly defined, offers a variety of ways forward. The most obvious tactic is simply to build public capacity directly. Early examples of policies in this direction include the EU's recently announced plans to give startups access to its supercomputers,[145] the French government's funding of a supercomputer later used to train BigScience's BLOOM large-scale AI model, and recent investments by the UK government worth several billion pounds into supercomputers, quantum technologies, and advanced semiconductors.[146] Similarly, the French and other governments are exploring the potential to build publicly owned 'national cloud' systems.

Government can also use their massive procurement and investment budgets to help break dangerous chokepoints both in the ownership and the location of essential computing capacity and infrastructure, including cloud computing and semiconductor manufacture. Successful programs such as the U.S. Defence Advanced Research Projects Agency (DARPA) provide a potential template for such efforts.

6. Reverse gatekeeper efforts to control AI development through mergers, investments and partnerships and block similar deals in future.

Much if not most of the existing power of the digital gatekeepers is based directly on the hundreds of acquisitions these corporations have made over the last two decades. According to one study, Apple, Google, Microsoft, Meta, and Amazon have acquired at least 700 companies since the year 2000, none of which were stopped by regulators.[147] Many of these were takeovers of miniscule startups, which failed to generate much public attention or draw the scrutiny of regulators, making it difficult to know in each instance how important their technology and talent were to the giants' subsequent growth. But when it comes to a number of high-profile deals, including Facebook's $1 billion acquisition of Instagram in 2012 and Google's $3.1 billion purchase of DoubleClick in 2007, it is indisputable that these were significant in laying the ground for the platforms' future dominance.

As seen earlier, when it comes to today's leading AI startups, the tech giants have so far opted to provide substantial financial and logistical support over outright acquisition, partly out of a desire to avoid regulatory scrutiny. But this is likely to change soon, if the past is a useful guide. Putting aside the recent generative AI boom, there are many examples of the tech giants acquiring AI firms, including Google's purchase of DeepMind in 2014, Microsoft's purchase of speech recognition firm Nuance in 2022,[148] and Apple's acquisition of AI Music in the same year.[149] According to data from PitchBook, around a fifth of the combined acquisitions and investments of these corporations since 2019 have involved AI firms.[150] It does not require a great leap of the imagination to see Microsoft making an outright bid to acquire OpenAI, or Google or Amazon attempting to purchase Anthropic.

Preventing today's monopolies from dominating AI will therefore entail restricting their ability to acquire or co-opt

innovative startups and potential rivals, either to gain access to their technology or eliminate them from the market. Major investments and partnerships should not escape scrutiny, particularly where these enable the dominant firm to exert significant control over its partner or investee. In most jurisdictions, regulators already have the power to investigate cartels and anti-competitive mergers and investments; where this is not the case, these powers should be upgraded. Acquisitions, investments, and agreements that have already been completed – including Microsoft/OpenAI, Google/DeepMind and Amazon/Anthropic – must be urgently investigated and if necessary unwound.

7. Establish bright-line rules to limit digital exploitation of workers and contractors, including a complete ban on biometric surveillance and automated manipulation.

Law enforcers and lawmakers should also take immediate action to prevent AI from being used to further undermine the rights, autonomy, and privacy of workers and contractors.

Where workers are harmed by the application of AI to systems of management and control, the burden of proof in justifying such activity should lie with employers and developers rather than employees, given the obvious asymmetries in information and power.[151] Key regulatory initiatives intended to shield workers from AI surveillance and exploitation, including the EU's Platform Work Directive and the U.S.'s Stop Spying Bosses Act, should be adapted and updated where necessary to reflect the latest developments in generative AI.

The AI Now Institute has proposed a set of measures to protect workers from AI exploitation, including baseline protections from algorithmic management and workplace surveillance, clear bright line rules in relation to specific practices (such as automated hiring and firing) and technologies (such as emotion recognition), and ensuring workers have the right to engage in collective bargaining and action.[152]

8. Increase strategic collaboration between competition law enforcers and data protection and privacy regulators.

Privacy regulation, properly understood, is also a form of competition policy, in that it can be used to limit certain behaviors that corporations engage in order to concentrate power, control, and wealth. Similarly, competition law and regulation can be used to help achieve fundamental privacy and data protection goals. One obvious example would be the use of antimonopoly law to separate cloud infrastructure from the largest gatekeeper corporations. A less obvious example is common carrier law, which radically reduces the value of the data that platform monopolies gather, by eliminating most of the potential to use that data to manipulate the behaviors and decisions of customers.

Previous generations better understood these fundamental interconnections. One example is the U.S. Congress' decision to entrust the Federal Trade Commission with both competition and privacy powers. In recent decades, however, in large part thanks to Chicago School efforts to isolate antitrust authorities within hardened silos, this fundamental interlinkage has been largely ignored. As a result competition enforcers and privacy regulators have largely ignored one another's work.

This is beginning to change. The European Data Protection Supervisor's office, under the leadership of Giovanni Buttarelli, worked hard to bring these two realms back into close alignment. More recently, a landmark ruling by the European Court of Justice recognizing that privacy violations can be a form of monopolistic conduct has helped point the way to practical cooperation. Meanwhile, pioneering competition law enforcers such as Germany's Bundeskartellamt and the FTC have begun to actively explore and exploit the many intersections of these two legal regimes.

CONCLUSION

As with any technology, we cannot be sure what path AI will take, or how successful it will ultimately be. Will it become as ubiquitous as search and social media today, or are we in the midst of another overhyped bubble, in the same vein as crypto and the metaverse?

Either way, how AI is developed and the impact it has on our democracies and societies will depend on who is allowed to manage, develop, and deploy these technologies, and how exactly they put them to use. We have a choice to make: between allowing some of the most powerful corporations the world has ever seen to develop AI in their own narrow self-interest, or structuring markets in a way that ensures AI promotes the public interest, and is subject to democratic control by citizens, not corporations.

Competition policy is the single most powerful tool at our disposal when it comes to restructuring markets in this way. And we should fully understand that this does not simply mean antitrust law and regulation. The Biden White House has demonstrated this with its whole-of-government approach to addressing the many threats posed by the concentration of power and control in our political economy. This approach brings together powers held under privacy, consumer protection, corporate governance, copyright law, trade policy, labor law, and industrial policy regimes.

The more closely we integrate these regimes, in the United States and elsewhere, the more swiftly and effectively we will be able to ensure that AI truly serves the interest of the people as a whole, and not simply the interests of the very largest corporations.

ENDNOTES

1 David McCabe and Cecilia Kang, "Microsoft C.E.O. Testifies That Google's Power in Search Is Ubiquitous," *New York Times*, October 2, 2023, https://www.nytimes.com/2023/10/02/technology/microsoft-ceo-testifies-google-search.html

2 Barry Lynn, "The Big Tech Extortion Racket," *Harper's Magazine*, September 2020, https://harpers.org/archive/2020/09/the-big-tech-extortion-racket/

3 Shira Ovide, "Would you ask Facebook AI Snoop Dogg for frozen yogurt suggestions?," *Washington Post*, September 29, 2023, https://www.washingtonpost.com/technology/2023/09/29/ai-doesnt-work-alexa/

4 James Tapper, "Authors shocked to find AI ripoffs of their books being sold on Amazon," *The Guardian*, September 30, 2023, https://www.theguardian.com/technology/2023/sep/30/authors-shocked-to-find-ai-ripoffs-of-their-books-being-sold-on-amazon

5 "Tracking the US and China AI Arms Race," AI Now Institute, April 11, 2023, https://ainowinstitute.org/publication/tracking-the-us-and-china-ai-arms-race

6 Prarthana Prakash, "Former Google CEO Eric Schmidt doesn't support a 6-month A.I. pause 'because it will simply benefit China'," *Fortune*, April 7, 2023, https://fortune.com/2023/04/07/former-google-ceo-eric-schmidt-against-6-month-a-i-pause-elon-musk-benefit-china-chatgpt-openai/

7 "Public Cloud – Worldwide," Statista, accessed November 7, 2023, https://www.statista.com/outlook/tmo/public-cloud/worldwide

8 Jai Vipra and Sarah Myers West, "Computational Power and AI," accessed November 7 2023, https://ainowinstitute.org/wp-content/uploads/2023/09/AI-Now_Computational-Power-an-AI.pdf

9 Joe Lamming, "GPT-4: The Giant AI (LLaMA) Is Already Out Of The Bag," *Verdantix*, April 5, 2023, https://www.verdantix.com/insights/blogs/gpt-4-the-giant-ai-llama-is-already-out-of-the-bag

10 Will Knight, "OpenAI's CEO Says the Age of Giant AI Models Is Already Over," *Wired*, April 17, 2023, https://www.wired.com/story/openai-ceo-sam-altman-the-age-of-giant-ai-models-is-already-over/

11 Wallace Witkowski, "Nvidia 'should have at least 90%' of AI chip market with AMD on its heels," *MarketWatch*, July 11, 2023, https://www.marketwatch.com/story/nvidia-should-have-at-least-90-of-ai-chip-market-with-amd-on-its-heels-13d00bff

12 "Taiwan's dominance of the chip industry makes it more important, *The Economist*, March 6, 2023, https://www.economist.com/special-report/2023/03/06/taiwans-dominance-of-the-chip-industry-makes-it-more-important

13 Tim Bradshaw and Richard Waters, "How Nvidia created the chip powering the generative AI boom," *Financial Times*, May 26, 2023, https://www.ft.com/content/315d804a-6ce1-4fb7-a86a-1fa222b77266

14 Doug Black, "Google Launches AI Supercomputer Powered by Tens of Thousands of NVIDIA H100 GPUs," *InsideHPC*, May 11, 2023,

https://insidehpc.com/2023/05/googles-launches-ai-supercomputer-powered-by-tens-of-thousands-of-nvidia-h100-gpus/

15 Anissa Gardizzy, "Microsoft to Debut AI Chip Next Month That Could Cut Nvidia GPU Costs," *The Information,* October 6, 2023, https://www.theinformation.com/articles/microsoft-to-debut-ai-chip-next-month-that-could-cut-nvidia-gpu-costs

16 "Major websites block AI crawlers from scraping their content," *Dig Watch*, September 4, 2023, https://dig.watch/updates/major-websites-block-ai-crawlers-from-scraping-their-content

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

18 Danielle Balbi, "How Microsoft's $13 Billion Bet Made It a Force in AI Gift this article," *Bloomberg,* June 15,2023, https://www.bloomberg.com/news/newsletters/2023-06-15/how-chatgpt-openai-made-microsoft-an-ai-tech-giant-big-take

19 "OpenAI and Microsoft extend partnership," Open AI, January 23, 2023, https://openai.com/blog/openai-and-microsoft-extend-partnership

20 Aaron Mok, "ChatGPT could cost over $700,000 per day to operate. Microsoft is reportedly trying to make it cheaper," *Business Insider,* April 20, 2023, https://www.businessinsider.com/how-much-chatgpt-costs-openai-to-run-estimate-report-2023-4

21 "End of support for Cortana," Microsoft Support, accessed November 7, 2023, https://support.microsoft.com/en-gb/topic/end-of-support-for-cortana-in-windows-d025b39f-ee5b-4836-a954-0ab646ee1efa

22 Tono Gil, "Watch out for AI cooperation agreements that are really mergers, Germany's Mundt warns," *Mlex,* September 21, 2023, https://mlexmarketinsight.com/news/insight/watch-out-for-ai-cooperation-agreements-that-are-really-mergers-germany-s-mundt-warns

23 Elon Musk (@elonmusk), "OpenAI was created as an open source (which is why I named it "Open" AI)," Twitter, February 17, 2023, https://twitter.com/elonmusk/status/1626516035863212034?lang=en

24 Kyle Wiggers, "Google consolidates AI research divisions into Google DeepMind," *Tech Crunch,* April 20, 2023, https://techcrunch.com/2023/04/20/google-consolidates-ai-research-divisions-into-google-deepmind/?guccounter=1

25 Krystal Hu, "Google agrees to invest up to $2 billion in OpenAI rival Anthropic," *Reuters,* October 28, 2023, https://www.reuters.com/technology/google-agrees-invest-up-2-bln-openai-rival-anthropic-wsj-2023-10-27/

26 Johan Moreno, "70% Of Generative AI Startups Rely On Google Cloud, AI Capabilities," *Forbes,* July 25, 2023, https://www.forbes.com/sites/johanmoreno/2023/07/25/70-of-generative-ai-startups-rely-on-google-cloud-ai-capabilities-says-alphabet-ceo-sundar-pichai/?sh=177061491243

27 "Hugging Face and AWS partner to make AI more accessible," Hugging Face press release, accessed November 11, 2023 https://huggingface.co/blog/aws-partnership

28 Frederic Lardinois, "Stability AI doubles down on AWS," *Tech Crunch,* November 30, 2022, https://

techcrunch.com/2022/11/30/stability-ai-doubles-down-on-aws/

29 "Amazon Bedrock," AWS Generative AI, accessed November 7, 2023, https://aws.amazon.com/bedrock/

30 "Amazon and Anthropic Announce Strategic Collaboration to Advance Generative AI," Amazon Press Center, accessed November 7, 2023, https://press.aboutamazon.com/2023/9/amazon-and-anthropic-announce-strategic-collaboration-to-advance-generative-ai

31 James Vincent, "Meta's powerful AI language model has leaked online — what happens now?," *The Verge*, March 8, 2023, https://www.theverge.com/2023/3/8/23629362/meta-ai-language-model-Llama-leak-online-misuse

32 "Meta and Microsoft Introduce the Next Generation of Llama," Meta, last updated July 18, 2023, https://about.fb.com/news/2023/07/Llama-2/

33 Madhumita Murgia and Patrick McGee, "Apple seeks to bolster expertise in generative AI on mobile devices", *Financial Times*, August 5, 2023, https://www.ft.com/content/d74477b6-8355-42a9-ae37-7c835880ef9e

34 Dylan Patel and Afzal Ahmad, "Google 'We Have No Moat, And Neither Does OpenAI,'" *SemiAnalysis*, ay 4, 2023, https://www.semianalysis.com/p/google-we-have-no-moat-and-neither

35 Will Douglas Heaven, "The open-source AI boom is built on Big Tech's handouts. How long will it last?," *MIT Technology Review*, May 12,2023, https://www.technologyreview.com/2023/05/12/1072950/open-source-ai-google-openai-eleuther-meta/

36 David Gray Widder, Sarah West, and Meredith Whittaker, "Open (For Business): Big Tech, Concentrated Power, and the Political Economy of Open AI," SSRN, August 18, 2023, https://papers.ssrn.com/sol3/papers.cfm?abntract_id=4543807

37 Stefano Mafulli, "Meta's LLaMa 2 license is not Open Source," *Voices of Open Source*, July 20, 2023, https://blog.opensource.org/metas-Llama-2-license-is-not-open-source/

38 Will Douglas Heaven, "The open-source AI boom is built on Big Tech's handouts. How long will it last?" *MIT Technology Review*, May 12, 2023, https://www.technologyreview.com/2023/05/12/1072950/open-source-ai-google-openai-eleuther-meta/

39 "GPT-4 Technical Report," Open AI, March 27, 2023, https://cdn.openai.com/papers/gpt-4.pdf

40 David Gray Widder, Sarah West, and Meredith Whittaker, "Open (For Business): Big Tech, Concentrated Power, and the Political Economy of Open AI," August 18, 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4543807

41 "Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine," European Commission Press Release, July 18, 2023, https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581

42 Steven J. Vaughan-Nichols, "Bing vs. Google: the new AI-driven search wars are on," *Computer World*, February 13, 2023, https://www.computerworld.com/article/3687988/bing-vs-google-the-new-ai-driven-search-wars-are-on.html

43 Ruchir Sharma, "What's wrong with tech giants riding the AI wave," *Financial Times*, July 30, 2023

https://www.ft.com/content/31dc322a-b2a1-4ef3-9a9d-d7268d58fac5

44 "Meta and Microsoft Introduce the Next Generation of Llama," Meta, July 18, 2023, https://about.fb.com/news/2023/07/llama-2/

45 Ariel Ezrachi, "Competition Overdose: How Free Market Mythology Transformed Us from Citizen Kings to Market Servants," University of Oxford Law, accessed November 7, 2023, https://www.law.ox.ac.uk/content/ariel-ezrachi

46 Sheen S. Levine and Dinkar Jain, "How Network Effects Make AI Smarter," *Harvard Business Review,* March 14, 2023, https://hbr.org/2023/03/how-network-effects-make-ai-smarter

47 "FTC Sues Amazon for Illegally Maintaining Monopoly Power," Federal Trade Commission, September 26, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-sues-amazon-illegally-maintaining-monopoly-power

48 Ben Brody, "Tech lobbies more the bigger it gets. A new paper explains why," *Protocol,* August 25, 2021, https://www.protocol.com/policy/tech-concentration-lobbying

49 Emilia David, "The rise of AI will only make Big Tech more powerful, researchers warn," *Business Insider,* Paril 25, 2023, https://www.businessinsider.com/ai-will-make-big-tech-even-more-powerful-2023-4

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

51 James Vincent, "OpenAI says it could 'cease operating' in the EU if it can't comply with future regulation," *The Verge,* May 25, 2023, https://www.theverge.com/2023/5/25/23737116/openai-ai-regulation-eu-ai-act-cease-operating

52 Billy Perrigo, "Exclusive: OpenAI Lobbied the E.U. to Water Down AI Regulation," *Time,* June 20, 2023, https://time.com/6288245/openai-eu-lobbying-ai-act/

53 Brendan Bordelon, "How a billionaire-backed network of AI advisers took over Washington," *Politico,* October 13, 2023, https://www.politico.com/news/2023/10/13/open-philanthropy-funding-ai-policy-00121362

54 Center for Journalism & Liberty, "Democracy, Journalism, and Monopoly," The Open Markets Institute, November 2023, https://www.journalismliberty.org/publications/report-how-to-fund-independent-news-media-in-the-21st-century

55 Nushin Rashidian, et al., "Friend and Foe: The Platform Press at the Heart of Journalism," Columbia Journalism Review, June 14, 2018, https://www.cjr.org/tow_center_reports/the-platform-press-at-the-heart-of-journalism.php

56 Courtney Radsch, "The Value of News Content to Google is Way More Than You Think," *Tech Policy Press,* August , 2023, https://techpolicy.press/the-value-of-news-content-to-google-is-way-more-than-you-think/

57 Eric Cortellessa and Phillip Longman, "A Free Market Won't Self-Correct the Disinformation Problem," *Washington Monthly, February 27, 2021,* https://washingtonmonthly.com/2021/02/27/a-free-market-wont-self-correct-the-disinformation-problem/

58 Johnny Ryan, "Unfair & Deceitful Commercial Surveillance," ICCL and The Open Markets Institute,

November 2022, https://www.iccl.ie/wp-content/uploads/2022/11/ICCL-Open-Markets-TACD-comment-on-FTC-call-commercial-surveilance-rulemaking.pdf

59 Billy Perrigo, "Why We Should All Be Worried About 'Chokepoint Capitalism'," *Time*, October 4, 2022, https://time.com/6219423/chokepoint-capitalism-doctorow-giblin/

60 Kim Lyons, "Timnit Gebru's actual paper may explain why Google ejected her," *The Verge*, December 5, 2020, https://www.theverge.com/2020/12/5/22155985/paper-timnit-gebru-fired-google-large-language-models-search-ai

61 Davey Alba and Julia Love, "Google's Rush to Win in AI Led to Ethical Lapses, Employees Say," *Bloomberg*, April 19, 2023, https://www.bloomberg.com/news/features/2023-04-19/google-bard-ai-chatbot-raises-ethical-concerns-from-employees?leadSource=uverify%20wall&sref=ZvMMMOkz

62 Tom Dotan and Deepa Seetharaman, "The Awkward Partnership Leading the AI Boom," *The Wall Street Journal*, June 13, 2023, https://www.wsj.com/articles/microsoft-and-openai-forge-awkward-partnership-as-techs-new-power-couple-3092de51

63 Kevin Schaul, Szu Yu Chen and Nitasha Tiku, "Inside the secret list of websites that make AI like ChatGPT sound smart," *The Washington Post*, April 19, 2023, https://www.washingtonpost.com/technology/interactive/2023/ai-chatbot-learning/

64 Tiffany Hsu and Stuart A. Thompson, "Disinformation Researchers Raise Alarms About A.I. Chatbots," *The New York Times*, June 20, 2023, https://www.nytimes.com/2023/02/08/technology/ai-chatbots-disinformation.html

65 Amber Middleton, "A Twitch streamer was caught watching deepfake porn of women gamers. Sexual images made without consent can be traumatic and abusive, experts say — and women are the biggest victims," *Insider*, February 10, 2023, https://www.insider.com/atrioc-caught-qtcinderella-ai-picture-twitch-deepfake-controversy-streamer-trauma-2023-2

66 Philip Marcelo, "FACT FOCUS: Fake image of Pentagon explosion briefly sends jitters through stock market," https://apnews.com/article/pentagon-explosion-misinformation-stock-market-ai-96f534c790872fde67012ee81b5ed6a4

67 Lucia Moses, "News Corp and other media companies are gearing for battle with Google and Microsoft over AI chatbots using their content, and litigation is likely if not inevitable," Insider, March 8, 2023, https://www.businessinsider.com/big-media-battle-google-microsoft-over-ai-chatbots-2023-3

68 Elizabeth Reid, "Supercharging Search with generative AI," Google Blog, May 10, 2023, https://blog.google/products/search/generative-ai-search/

69 "Major websites block AI crawlers from scraping their content," *Digwatch*, September 4, 2023, https://dig.watch/updates/major-websites-block-ai-crawlers-from-scraping-their-content

70 Karina Montoya, "The New Gold Rush in Advertising Is Your Shopping List," *Washington Monthly*, June 12, 2023, https://washingtonmonthly.com/2023/06/12/the-new-gold-rush-in-advertising-is-your-shopping-list/

71 Matthew Crain, *Profit over Privacy* (Minneapolis: University of Minnesota Press, 2021), https://www.upress.umn.edu/book-division/books/profit-over-privacy

72 Gerrit De Vynck, "ChatGPT maker OpenAI faces a lawsuit over how it used people's data," *The Washington Post,* June 28, 2023, https://www.washingtonpost.com/technology/2023/06/28/openai-chatgpt-lawsuit-class-action/

73 Cat Zakrzewski, "FTC investigates OpenAI over data leak and ChatGPT's inaccuracy," *The Washington Post,* July 13, 2023, https://www.washingtonpost.com/technology/2023/07/13/ftc-openai-chatgpt-sam-altman-lina-khan/

74 "The hidden dangers of generative advertising," *VentureBeat*, April 8, 2023, https://venturebeat.com/ai/the-hidden-dangers-of-generative-advertising/

75 "How Generative AI Enables and Promotes Harmful Eating Disorder Content," Center for Countering Digital Hate, August 7, 2023, https://counterhate.com/research/ai-tools-and-eating-disorders/

76 David Greenfield and Shivan Bhavnani, "Social media: generative AI could harm mental health," May 23, 2023, https://www.nature.com/articles/d41586-023-01693-8

77 "Introducing the AI Sandbox for advertisers and expanding our Meta Advantage suite," Meta Announcements, May 11, 2023, https://www.facebook.com/business/news/introducing-ai-sandbox-and-expanding-meta-advantage-suite;
Jerry Dischler, "Introducing a new era of AI-powered ads with Google," Google ADS, https://blog.google/products/ads-commerce/ai-powered-ads-google-marketing-live/

78 Jonathan Vanian, "How the generative A.I. boom could forever change online advertising," *CNBC,* July 12, 2023, https://www.cnbc.com/2023/07/08/how-the-generative-ai-boom-could-forever-change-online-advertising.html

79 Patience Haggin, "Google Violated Its Standards in Ad Deals, Research Finds," *The Wall Street Journal,* June, 27, 2023, https://www.wsj.com/articles/google-violated-its-standards-in-ad-deals-research-finds-3e24e041

80 Jeff Horwitz, "Facebook Accused in Amended Lawsuit of Knowing Ad Audiences Were Inflated," *The Wall Street Journal,* March 20, 2023, https://www.wsj.com/articles/facebook-accused-in-amended-lawsuit-of-knowing-ad-audiences-were-inflated-11584745492

81 Josh Taylor, "Meta slammed over scam ads on Facebook featuring Australian TV personalities," *The Guardian,* March 23, 2023, https://www.theguardian.com/technology/2023/mar/28/australian-tv-networks-criticise-meta-over-inadequate-response-time-to-damaging-scam-ads

82 Arielle Garcia, "An Industry In Conflict: It's Time For Tough Questions And Hard Decisions," *adExchanger,* September 18, 2023, https://www.adexchanger.com/marketers/an-industry-in-conflict-its-time-for-tough-questions-and-hard-decisions/

83 Naomi Nix and Elizabeth Dwoskin, "Justice Department and Meta settle landmark housing discrimination case," *The Washington Post*, June 21, 2023, https://www.washingtonpost.com/technology/2022/06/21/facebook-doj-discriminatory-housing-ads/

84 Nicolas Kayser-Bril, "Automated discrimination: Facebook uses gross stereotypes to optimize ad delivery," *Algorithm Watch,* accessed November 9 2023, https://algorithmwatch.org/en/automated-discrimination-facebook-google/

85 David Shepardson, "US FCC chair to seek

reinstating net neutrality rules rescinded under Trump," *Reuters,* September 26, 2023, https://www.reuters.com/world/us/us-telecom-chair-seek-reinstating-net-neutrality-rules-rescinded-under-trump-2023-09-26/

86 Alessandro Acquisti and Hal R. Varian, "Conditioning Prices on Purchase History," Marketing Science 24, no. 3 (November 2005): 367–81, https://www.jstor.org/stable/40056968

87 "FTC Sues Amazon for Illegally Maintaining Monopoly Power," Federal Trade Commission (press release), September 26, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-sues-amazon-illegally-maintaining-monopoly-power

88 Barry Lynn, "The Big Tech Extortion Racket," *Harper's Magazine*, September 2020, https://harpers.org/archive/2020/09/the-big-tech-extortion-racket/

89 Brian Callaci and Sandeep Vaheesan, "How an Old U.S. Antitrust Law Could Foster a Fairer Retail Sector" *Harvard Business Review*, February 09, 2022, https://hbr.org/2022/02/how-an-old-u-s-antitrust-law-could-foster-a-fairer-retail-sector

90 Hannah Ellis-Petersen, "Amazon and publisher Hachette end dispute over online book sales," *The Guardian*, November 13, 2014, https://www.theguardian.com/books/2014/nov/13/amazon-hachette-end-dispute-ebooks

91 Adrianne Jeffries, Leon Yin and Surya Mattu, "Swinging the Vote," *The Markup*, February 26, 2020, https://themarkup.org/google-the-giant/2020/02/26/wheres-my-email

92 Nick Thompson, Fred Vogelstein, "15 Months of Fresh Hell Inside Facebook," *Wired*, April 16, 2019, https://www.wired.com/story/facebook-mark-zuckerberg-15-months-of-fresh-hell/

93 "Changes to News Availability on Our Platforms in Canada," Meta, June 1, 2023, https://about.fb.com/news/2023/06/changes-to-news-availability-on-our-platforms-in-canada/

94 Jason Abbruzzese, Kevin Collier and Phil Helsel, "Twitter suspends journalists who have been covering Elon Musk and the company," *NBC News*, December 15, 2022, https://www.nbcnews.com/tech/social-media/twitter-suspends-journalists-covering-elon-musk-company-rcna62032

95 Nick Thompson, Fred Vogelstein, "Inside the Two Years That Shook Facebook—and the World," *Wired*, February 12, 2018, https://www.wired.com/story/inside-facebook-mark-zuckerberg-2-years-of-hell/

96 Victor Luckerson, "'Crush Them': An Oral History of the Lawsuit That Upended Silicon Valley," *The Ringer,* May 18, 2018, https://www.theringer.com/tech/2018/5/18/17362452/microsoft-antitrust-lawsuit-netscape-internet-explorer-20-years

97 "Justice Department Sues Google for Monopolizing Digital Advertising Technologies," Office of Public Affairs at U.S. Department of Justice, January 14, 2023, https://www.justice.gov/opa/pr/justice-department-sues-google-monopolizing-digital-advertising-technologies

98 "Antitrust: Commission accepts commitments by Amazon barring it from using marketplace seller data, and ensuring equal access to Buy Box and Prime," (press release) European Commission, December 20, 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7777

99 "Introducing the new Bing," Microsoft, https://www.bing.com/new?form=MY028Z&OCID=MY028Z

100 Zoubin Ghahramani, "Introducing PaLM 2," Google's The Keyword Blog, May 10, 2023, https://blog.google/technology/ai/google-palm-2-ai-large-language-model/

101 Nilutpal Timsina and Juby Babu, "Microsoft threatens to restrict data from rival AI search tools-Bloomberg News," *Reuters*, March 26, 2023, https://www.reuters.com/technology/microsoft-threatens-restrict-data-rival-ai-search-tools-bloomberg-news-2023-03-25/

102 "Cloud services market study. Interim Report," Ofcom, May 17, 2023, https://www.ofcom.org.uk/__data/assets/pdf_file/0029/256457/cloud-services-market-study-interim-report.pdf

103 Sara Fischer, "IAC warns regulators generative AI could wreck the web," *Axios*, November 1, 2023, https://www.axios.com/2023/11/02/iac-generative-ai-wreck-web?stream=top1

104 "Summary of the 2023 WGA MBA," Writers Guild of America, https://www.wgacontract2023.org/the-campaign/summary-of-the-2023-wga-mba

105 "Open Markets Submits Public Comment on Artificial Intelligence & Copyright," Open Markets Institute, October 31, 2023, https://www.openmarketsinstitute.org/publications/open-markets-submits-public-comment-on-artificial-intelligence-copyright

106 Kevin Schaul, Szu Yu Chen and Nitasha Tiku, "Inside the secret list of websites that make AI like ChatGPT sound smart," *The Washington Post*, April 19, 2023, https://www.washingtonpost.com/technology/interactive/2023/ai-chatbot-learning/

107 James Tapper, "Authors shocked to find AI ripoffs of their books being sold on Amazon," *The Guardian*, September 30, 2023, https://www.theguardian.com/technology/2023/sep/30/authors-shocked-to-find-ai-ripoffs-of-their-books-being-sold-on-amazon

108 Ibid.

109 Igor Bonifacic, "AI-generated Drake and The Weeknd song pulled from streaming platforms," *Engadget*, April 19, 2023, https://www.engadget.com/copyright-in-spotlight-after-streaming-platforms-pull-ai-generated-drake-song-183513972.html

110 Amanda Hoover, "Spotify Has an AI Music Problem—but Bots Love It," *Wired*, May 11, 2023, https://www.wired.com/story/spotify-ai-music-robot-listeners/

111 Daron Acemoglu and Pascual Restrepo "Tasks, Automation, and The Rise In U.S. Wage Inequality," *Econometrica*, Vol. 90, No. 5 (September, 2022), https://economics.mit.edu/sites/default/files/2022-10/Tasks%20Automation%20and%20the%20Rise%20in%20US%20Wage%20Inequality.pdf

112 John Bluedorn, Weicheng Lian, Natalija Novta, Yannick Timmer, "Widening Gaps: Regional Inequality within Advanced Economies," *IMF Blog*, October 9, 2019, https://www.imf.org/en/Blogs/Articles/2019/10/09/widening-gaps-regional-inequality-within-advanced-economies

113 Julian Jacobs, "Automation and the radicalization of America," Brookings Institution, November 22, 2021, https://www.brookings.edu/articles/automation-and-the-radicalization-of-america/

114 Niamh McIntyre, Rosie Bradbury, "The eyes of Amazon: a hidden workforce driving a vast surveillance system," *The Bureau of Investigative Journalism*, November 21, 2022, https://www.thebureauinvestigates.

com/stories/2022-11-21/the-eyes-of-amazon-a-hidden-workforce-driving-a-vast-surveillance-system

115 Sarah Krouse, "How Google Spies on Its Employees," *The Information*, September, 23, 2021, https://www.theinformation.com/articles/how-google-spies-on-its-employees?rc=qudiig

116 Liam Tung, "Microsoft 365's Productivity Score: It's a full-blown workplace surveillance tool, says critic," *ZDNET.com*, November 27, 2020, https://www.zdnet.com/article/microsoft-365s-productivity-score-its-a-full-blown-workplace-surveillance-tool-says-critic/

117 Megan Cerullo, "How companies get inside gig workers' heads with 'algorithmic wage discrimination'," *CBS News*, April 18, 2023, https://www.cbsnews.com/news/algorithmic-wage-discrimination-artificial-intelligence/

118 Veena Dubal, "On Algorithmic Wage Discrimination," UC San Francisco, Research Paper No. Forthcoming, January 19, 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4331080

119 Samrhitha A and Chavi Mehta, "Amazon cloud services back up after big outage hits thousands of users," *Reuters*, June 14 2023, https://www.reuters.com/technology/amazon-says-multiple-cloud-services-down-users-2023-06-13

120 Isabelle Bousquette, "Goldman Sachs CIO Tests Generative AI," *Wall Street Journal*, May 2, 2023, https://www.wsj.com/articles/goldman-sachs-cio-tests-generative-ai-886b5a4b

121 Hugh Son, "JPMorgan is developing a ChatGPT-like A.I. service that gives investment advice," *CNBC*, May 25, 2023, https://www.cnbc.com/2023/05/25/jpmorgan-develops-ai-investment-advisor.html

122 Jonathan Spencer Jones, "How generative AI is coming to the energy sector," *Smart Energy International*, April 11, 2023, https://www.smart-energy.com/features-analysis/how-generative-ai-is-coming-to-the-energy-sector/

123 Katrina Manson, "The US Military Is Taking Generative AI Out for a Spin," *Bloomberg*, July 5, 2023, https://www.bloomberg.com/news/newsletters/2023-07-05/the-us-military-is-taking-generative-ai-out-for-a-spin?sref=ZvMMMOkz

124 Sascha Dieh and Andrea Ketzer, "Harnessing the Power of Generative AI for Automotive Technologies on AWS," AWS Blog, June 5, 2023, https://aws.amazon.com/blogs/industries/harnessing-the-power-of-generative-ai-for-automotive-technologies-on-aws/

125 Stefania Palma and Patrick Jenkins, "Gary Gensler urges regulators to tame AI risks to financial stability," *Financial Times*, October 15, 2023, https://www.ft.com/content/8227636f-e819-443a-aeba-c8237f0ec1ac

126 Gary Gensler and Lily Bailey, "Deep Learning and Financial Stability," Massachusetts Institute of Technology, November 12, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3723132

127 Tejas Narechania and Ganesh Sitaraman, "An Antimonopoly Approach to Governing Artificial Intelligence," Vanderbilt Policy Accelerator For Political Economy & Regulation, October 2023, https://cdn.vanderbilt.edu/vu-URL/wp-content/uploads/sites/412/2023/10/06212048/Narechania-Sitaraman-Antimonopoly-AI-2023.10.6.pdf.pdf

128 "AI Act: a step closer to the first rules on Artificial Intelligence," European Parliament (press release), May 11, 2023, https://www.europarl.europa.eu/

news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence

129 Mark Scott, Laurens Cerulus, and Steven Overly, "How Silicon Valley gamed Europe's privacy rules," *Politico*, May 22, 2019, https://www.politico.eu/article/europe-data-protection-gdpr-general-data-protection-regulation-facebook-google/

130 "Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI," The White House Press Release, July 21, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/

131 "Frontier Model Forum: Advancing Safe AI Development," Frontier Model Forum, Accessed November 11, 2023, https://www.frontiermodelforum.org/

132 Cristina Criddle and Madhumita Murgia, "Big tech companies cut AI ethics staff, raising safety concerns," *Financial Times*, March 29, 2023, https://www.ft.com/content/26372287-6fb3-457b-9e9c-f722027f36b3

133 "Q1 Cloud Spending Grows by Over $10 Billion from 2022; the Big Three Account for 65% of the Total," Synergy Research Group, April 27, 2023, https://www.srgresearch.com/articles/q1-cloud-spending-grows-by-over-10-billion-from-2022-the-big-three-account-for-65-of-the-total

134 "Cloud services market study Interim Report," Ofcom, May 17, 2023, https://www.ofcom.org.uk/__data/assets/pdf_file/0029/256457/cloud-services-market-study-interim-report.pdf

135 Sonya Mann, "Startups Beware: If You Use AWS, Amazon May Have You in Its Crosshairs," *Inc.com*, April 24, 2017, https://www.inc.com/sonya-mann/aws-startups-conflict.html

136 Tejas Narechania and Ganesh Sitaraman, "An Antimonopoly Approach to Governing Artificial Intelligence," Vanderbilt Policy Accelerator For Political Economy & Regulation, October 2023, https://cdn.vanderbilt.edu/vu-URL/wp-content/uploads/sites/412/2023/10/06212048/Narechania-Sitaraman-Antimonopoly-AI-2023.10.6.pdf

137 "Cloud computing: the Autorité de la concurrence issues its market study on competition in the cloud sector," Autorité de la Concurrence, June 29, 2023, https://www.autoritedelaconcurrence.fr/en/press-release/cloud-computing-autorite-de-la-concurrence-issues-its-market-study-competition-cloud

138 There are many precedents for data access mandates, including the UK's Open Banking regulatory regime requiring dominant banks to share data with competitors, provisions in the EU Digital Services Act granting researchers access to certain data from large tech companies, and France's Law for a Digital Republic which among other things requires private entities involved in public sector activities to share data.

139 "Unlocking the value of data: Exploring the role of data intermediaries," Centre for Data Ethics and Innovation, accessed November 10, 2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004925/Data_intermediaries_-_accessible_version.pdf

140 Katharina Koerner and Brandon Lalonde, Federated learning: Supporting data minimization in AI, *iapp*, February 28, 2023, https://iapp.org/news/a/federated-learning-supporting-data-minimization-in-ai/

141 Winston Cho, "SAG-AFTRA Leader: Actors Should Get Same AI Protections As Studios," October 4, 2023, https://www.hollywoodreporter.com/business/business-news/ftc-hearing-ai-sagaftra-wga-1235609247/

142 "News/Media Alliance AI Principles," News Media Alliance, April 20, 2023, https://www.newsmediaalliance.org/ai-principles/

143 "Big Tech and Journalism - Principles for Fair Compensation," Gordon Institute of Business Science, https://www.gibs.co.za/news-events/news/pages/big-tech-and-journalism-principles.aspx

144 Ray Schultz, "News/Media Alliance Issues Principles Covering Generative AI Use Of Publisher Content," *MediaPost*, April 20, 2023, https://www.mediapost.com/publications/article/384574/newsmedia-alliance-issues-principles-covering-gen.html

145 Zosia Wanat, "EU will allow European AI startups to use supercomputers to train its models," *Sifted*, September, 13, 2023, https://sifted.eu/articles/eu-will-allow-european-ai-startups-to-use-supercomputers-to-train-its-models

146 Jai Vipra and Sarah Myers West, "Computational Power and AI," accessed November 7, 2023, https://ainowinstitute.org/wp-content/uploads/2023/09/AI-Now_Computational-Power-an-AI.pdf

147 "Mergers and Acquisitions in Digital Markets, Congressional Research Services," March 30, 2021, https://crsreports.congress.gov/product/pdf/R/R46739

148 "Microsoft completes acquisition of Nuance, ushering in new era of outcomes-based AI," Microsoft News Center, last updated March 4, 2022, https://news.microsoft.com/2022/03/04/microsoft-completes-acquisition-of-nuance-ushering-in-new-era-of-outcomes-based-ai/

149 Mark Gurman, "Apple Buys Startup That Makes Music With Artificial Intelligence," *Bloomberg*, February 7, 2023, https://www.bloomberg.com/news/articles/2022-02-07/apple-buys-startup-that-makes-music-with-artificial-intelligence?sref=ZvMMMOkz

150 "Big tech and the pursuit of AI dominance," *The Economist*, March 26, 2023, https://www.economist.com/business/2023/03/26/big-tech-and-the-pursuit-of-ai-dominance

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

152 Ibid.

OPEN MARKETS INSTITUTE