Who Do AI Agents Work For?

Power and Control in the Next Internet

Sally Hubbard

June 2026

OPEN MARKETS INSTITUTE

Agent: /ā′jənt/

noun

1. a person who acts for or represents another

Cambridge Dictionary

Introduction

The 2022 release of ChatGPT signaled what may prove to be the biggest historical revolution in the structure and nature of the internet. Suddenly people could write their own code without having any engineering experience at all. They could receive one-on-one tutoring in any subject matter of their choice. They could instantly find answers to questions on the web without wading through Google search ad slop.

Of all the changes, perhaps the most radical has been the introduction of a new generation of vastly more powerful "agents" designed to autonomously use tools and make decisions on a person's behalf in furtherance of some specific practical aim — such as buying an airline ticket or vacuum cleaner or disputing a bill with the local utility.[1]

In doing so the agents are encapsulating many of the most dramatic advances of recent decades in online technologies. They are also changing in fundamental ways how people engage with the internet, by in essence adding an entirely new layer between the end user and the information she seeks. (In this paper, in addition to the word "people," I will also use the terms "users" and "citizens.")[2]

It is important not to understate the magnitude of the change we are living through. The first generation of the internet was structured as the world wide web, and users navigated from website to website. In the second generation, a few giant online applications like Google, Facebook, and Amazon became the primary portals through which people interacted with information and business online. Today we stand at the beginning of nothing less than a third paradigm, the "agentic web," in which people will no longer interact directly with apps but instead with AI agents who will learn users' needs and preferences and then interact with traditional apps, websites, and other AI agents to execute tasks on behalf of the user.[3]

This relationship makes the AI agent different from the AI chatbots that have captured so much attention the last few years, both in how it engages with the user and in what it can do or will soon be able to do. To be sure, AI assistants and chatbots have been around for many years —Apple rolled out the first generation of SIRI in 2011[4] and Amazon introduced Alexa in 2014.[5] But the advances in Generative AI over the last few years have expanded and extended the capabilities of these tools in revolutionary ways that are already beginning to remake the structure of power and commerce on the internet.

The speed at which people are embracing today's generation of AI agents is also stunning. In part, this is because the agents are already able to fill — or at least seem to fill — a variety of perceived needs. In addition to simple commercial tasks like shopping for groceries and buying concert tickets, this includes tasks that are more political in nature, such as gathering and fact-checking news. And it includes tasks that are much more personal, such as drafting legal documents like wills and making medical appointments.

This fast adoption is also due to the immense existing power of the corporations that control the main AI technologies. Most leading AI agents are embedded in the already dominant platforms that people are accustomed to using, and which have captured some degree of monopoly control over the foundational infrastructures of today's internet. Google, for instance, has embedded its Gemini technology in Google search, Gmail, Chrome, Android, Google Docs, and more.[6] Meta, meanwhile, has embedded agentic features in Instagram, WhatsApp, Facebook, and Messenger.[7] And Microsoft has embedded OpenAI's technology into Microsoft 365 Copilot, GitHub, Azure, and Bing.[8] Further, Microsoft, Google, IBM, and others are licensing their AI technology to other corporations to embed AI agents in their own online services, as well as licensing their technology to individuals.[9]

Recognizing the degree to which these already dominant corporations also dominate the design and rollout of the first generation of AI agents helps us focus on the ultimate essential question of this whole technology: who does the AI agent actually serve? Does it primarily represent the interests of the user? Or does it represent the interest of the corporation that provides and controls the agent? Or worse, a powerful corporation in service to an even more powerful state?[10]

Consider perhaps the simplest of examples, when people use an AI agent to buy a product such as an airline ticket, how do they know they are getting a fair price? A growing number of corporations, including airlines, already impose systems of *surveillance pricing* designed to charge individuals the maximum price that close study of that individual's actions and private data reveals they might be willing and able to pay.[11] Any AI agent routinely used by a specific person will have even more data about the user than an airline like Delta has. This will be vastly truer of any AI agent controlled by a corporation

like Google, which already dominates sprawling realms of internet commerce and communications and has assembled a vast portfolio of information on almost every user. In such a structure of power, is it not logical to expect the AI agent to charge even more money off the top for that airline ticket than the airline itself, without the user knowing? Or to expect the AI agent to choose the airline that pays it the biggest kickback, instead of the airline that offers the best deal to the user?

And when X users ask Grok, "Is this true?"— as they did 2.3 million times in just one week last June — most users will logically think that Grok is working for them.[12] But is Grok instead filtering the information it delivers to individuals in ways that promote the business and political interests of Elon Musk? Grok (which started as an AI assistant but now has agentic features) is of course an extreme example. It was trained on Elon Musk's tweets,[13] and, despite being billed as "your truth-seeking AI companion for unfiltered answers," it has repeatedly delivered extremely concerning information. In July 2025, for instance, Grok spouted antisemitic vitriol during what has been called a "Mecha-Hitler" meltdown,[14] while also censoring access to publications like Media Matters or *Rolling Stone* that Elon Musk had deemed to be too liberal.[15] Agents provided by Google and Microsoft pose many of the same threats, albeit behind a less controversial façade.

The list goes on and on. When a patient uses an AI agent to research a medical problem they have, how do they know the agent is providing the full range of solutions, including preventative or lifestyle modifications, and not just pushing pills and getting kickbacks from Big Pharma?

When people use an AI agent to challenge corporate overcharges or fraudulent fees, how do they know the AI agent is working in their best interests, and not delivering yet more private information to the corporation that is ripping them off?

When people allow an AI agent to learn about their emotional wellbeing, their financial status, their individual vulnerabilities, their spiritual crises, their career hopes and fears, who gets to control this information and to what end? What restrictions should be placed on how that information can be used and who gets to see it?

We don't know the answers to these questions. What we do know is that the AI agent can use what it already knows about the user to pick and choose what information the user sees, and the AI agent likely will have the ability to influence how the user engages with politics, family, community, even their own bodies and minds, to an even greater degree than today's tech platforms do.

We also know that it doesn't have to be this way. AI agents created by new innovators could help arm the citizen against harmful business models and empower citizens against the onslaught of manipulation and extraction.

Dazza Greenwood of Consumer Reports, part of an alliance of innovators called GliaNet discussed more fully below, puts forth a vision of the AI agent as a consumer advocate with a duty of loyalty to the consumer:

> "The implications of LLM agents for consumer empowerment are profound. If built with the right legal and technical safeguards, they could shift the balance of power, allowing individuals to navigate complex systems — whether financial, commercial, legal, or social — with an AI working solely in their interests. These agents could help consumers make informed choices, protect their privacy, and advocate for their needs in previously impossible ways."[16]

Policymakers can proactively foster the development of a deconcentrated agentic web that works for every individual citizen and for the public as a whole. The choice is up to us.

But if policymakers do nothing, the choice will be made for us all by default. Given the now familiar arc of the monopolist's playbook in the digital age, which has remained remarkably consistent since the 1990s, the default outcome is amplified exploitation and extraction. The only way to ensure that AI agents actually work for people — and do not simply amplify already dangerous forms of surveillance, addiction, manipulation, and extraction by today's dominant tech corporations — is to take decisive political action now.

The Purpose of this Paper

The purpose of this paper is to begin to ask the question: What can we do to ensure that the AI agent serves the user's interest, instead of the corporation's interests, or the interests of the corporation aligned with the state? And how can we do so through the framework of the legal regimes democratic society have traditionally used to regulate the power of corporations that provide good and services?

Throughout history, Americans developed many forms of regulatory policy to prevent the abuse of new technologies to concentrate dangerous levels of political power or dangerous forms of direct control over individual citizens and independent businesses. As new technologies have emerged that pose the risk of creating gatekeepers and chokepoints, this toolkit has repeatedly provided Americans with the ability to preserve both the free flow of information and dynamism in commerce. With each new wave of technology, American policymakers created policies designed to ensure that owners of crucial technologies did not privilege some people's speech while suppressing others.[17]

These policies aimed to prevent networks — whether the railroad, telegraph, telephone, or internet service provider — from discriminating in favor of, or against, any one person, party, or corporation.[18]

Unfortunately, these tools have largely been neglected in the digital age. For instance, the Telecommunications Act of 1996, a culmination of the anti-regulatory revolution of the 1980s and 1990s, de facto exempted Big Tech from most of the traditional forms of regulation that over the decades proved so critical to fundamental American freedoms.[19] This latest wave of technological advancement brought on by agentic AI increases the urgency of their revival.

A few clarifications: in raising the questions, "Who do AI agents work for?" and "How can we ensure that AI agents work for users?" this paper is not about the AI "alignment problem." That refers to the technical and ethical challenge of AI systems reliably doing what humans intend, instead of doing something slightly or entirely different, sometimes called "going rogue."[20] Nor does this paper address the range of serious concerns about AI safety, bias, and environmental impacts.

This paper also does not focus in any depth on enterprise AI agents. In the enterprise context, AI agents are designed to perform a wide variety of functions within a corporation. Again, the goal here is to focus on AI agents that regular people use to do things like find and make sense of information or to make purchases.[21]

This paper instead focuses largely on exploring fiduciary duty law, which is the body of law designed to ensure that real human agents owe fiduciary duties to their human customers and must act in their best interest in all real-life transactions. It explores whether AI agents could possibly uphold fiduciary duties to users when they are being deployed by corporations with business models that surveil, addict, manipulate and extract? (Hint: they can't). In doing so, the paper builds on the scholarship of former Federal Trade Commission chair Lina Khan and Columbia law professor David E. Pozen regarding tech platforms and fiduciary duty law and extends that analysis into the agentic web, drawing on Open Market's director Courtney C. Radsch's work on AI market concentration, cognitive liberty, and the structural conditions under which AI agents serve users or the corporations that deploy them.[22]

The paper will also emphasize the idea that stronger and more strategic enforcement of antimonopoly law and policy is necessary to eliminate the present chokehold on AI technologies and infrastructure by Google, Microsoft, and Amazon, including through regulation of the behavior of the monopoly platforms controlled by these corporations. Relatedly, the paper argues that policies such as interoperability are unlikely to succeed in reducing the power of the dominant players, until lawmakers and enforcers have more forcefully addressed the behavior, and structure, of these corporations.

The ultimate goal of this paper is to ensure either that the AI agent truly works on behalf of the user, or to ensure that users understand that the AI agent works for the corporation.

1. What is an AI Agent?

Most people probably think of an AI agent much the way they think of human agents. This means, as defined by the Cambridge Dictionary, someone "who acts for or represents another." As the virtual version of a real-life agent, an AI agent is a software system, powered by generative AI, that autonomously uses tools and makes decisions on a person's behalf toward a goal.[23] For example, an AI agent could make shopping comparisons and purchasing decisions for you, plan your next vacation, or even analyze financial investments for you.

An example of a real-life agent with whom many people have interacted is the real estate agent. Anyone who has used an agent to help buy a home swiftly learns there is clear demarcation between an agent that works for the person who is selling a property and an agent who works for the person buying a property. People understand that if they are buying a house, the seller's agent does not work for them and is largely working for the interests of another person or party, and hence cannot be trusted.

Similarly, many people have hired a lawyer to serve as their agent, such as by representing their interests in court. In this experience, they have also learned that the opposing counsel represents the interests of their adversary. Much the same is true when people hire agents to help them invest in the stock market. They expect their broker to represent their interests, not the interests of a particular corporation, when facilitating the purchase of the corporation's stocks.

Given the wide variety of AI tools that are being introduced to the market at a rapid pace, there is no clearly agreed-upon public definition of an "AI agent." What can be said is that AI agents have traditionally been defined as being technically different from AI chatbots and assistants like earlier versions of ChatGPT or Grok, which are conversational interfaces that provide specific information or assistance.[24] Chatbots answer specific questions in a call and response format. AI assistants also help answer questions that empower users to complete a specific task.

AI agents go further than AI chatbots and assistants and can decide what to do next based on pre-set goals and can even create and execute workflows without human involvement in each step.[25] AI agents are able to "understand and respond to complex instructions, reason about different options, and use tools."[26] AI agents act at a higher level of autonomy as they work to achieve the user's goals, largely without human supervision along the way.

The definitional boundaries between these types of AI services, however, are breaking down as AI chatbots rapidly advance technologically and begin to perform more autonomously. Meta AI, for example, began as an AI assistant but now offers agentic features.[27] Instead of just responding to prompts, Meta's Llama 4 AI model can power AI agents that are capable of higher levels of reasoning and action.[28] Llama 4 is trained and tuned to break problems into subtasks, maintain a plan over many turns, and revise that plan as new information arrives.[29] Similarly, ChatGPT unveiled Agent Mode in July 2025, and xAI included agentic capabilities in Grok 4.1, both of which can do things like book appointments and handle complex tasks.[30]

Well-intentioned innovators are developing AI agents designed to faithfully work for the user, as discussed further below. Many of these innovators believe that technological disruption, paired with interoperability requirements, will open markets to new competition. Such a belief is appealing because innovating is easier than the hard work of challenging the entrenched power of Big Tech incumbents.

But history teaches otherwise. Specifically, that the already powerful corporations that dominate today's technologies and reap tremendous profits from them will use their power to ensure that these well-intentioned innovators don't stand a chance.

2. AI Agents As the Next Internet Middlemen

Big Tech platforms were the first internet middlemen, separating readers from publishers (Google and Facebook), buyers from sellers (Amazon), and fans from artists and content creators (YouTube and Spotify), and then intermediating those relationships. The result has been the destruction of journalism and the degradation of the entire political economy of information,[31] highly targeted manipulation of the citizenry and individuals,[32] increasingly sophisticated and effective extraction of wealth from individual people and small and mid-sized companies,[33] and ever more extreme concentration of economic and political power in the hands of a few.[34]

As the next level of middlemen, acting autonomously as a go-between for users and the web, or a go-between in agent-to-agent communications, AI agents have the capacity to amplify these harms, giving tech corporations even more intrusive access to our personal data, and even more power to manipulate us. Given that most leading AI tools are owned by or have ties to Big Tech, this looks to be the likely outcome if nothing is done to stop it.

A report published last year by venture capital firm Menlo Ventures showed that OpenAI (Microsoft has a 27% stake in OpenAI),[35] Google, Meta, Amazon, and Apple lead in terms of general AI assistant usage market share as of June 2025. It notes that "first-mover advantage and built-in distribution are currently driving market share."[36] Most AI consumers don't differentiate between AI technologies, says the report, whether voice assistants, LLMs, or algorithms, making their usage "fueled more by habit and convenience than concern for technology under the hood."[37]

In the consumer chatbot segment, the market leader as of April 2026 is OpenAI, with roughly a 60% market share, followed by Google's Gemini at 15% and Microsoft's Copilot at 13%.[38] Microsoft's Copilot is built directly into Bing, Microsoft Edge, Windows, and Office 365. Similarly, people encounter Gemini without having to affirmatively seek it out, due to integration with Search, Gmail, YouTube, and Android.[39] And Meta AI had nearly 1 billion monthly active users by Q1 2025, because it was integrated into existing platforms, Facebook, WhatsApp, and Instagram.[40]

Although market share information is difficult to pin down for AI agents, one recent report put Google Gemini (Agent Mode) in the lead with nearly 58% percent market share due to its integration with its dominant platforms.[41]

When it comes to AI agentic shopping, Perplexity Buy and ChatGPT Operator have led the transition, while Amazon, Google, Mastercard, and Shopify are all developing agentic shopping services at the time of writing. McKinsey predicts that by 2030 agentic commerce could reach $1 trillion in the U.S. alone, and $3 to $5 trillion globally.[42]

3. Big Tech Platforms – and Their AI Agents – Do Not Work for You

As internet middlemen, Big Tech platforms inserted themselves between the reader and the content creator and between the buyer and the seller. The effect of Big Tech's intermediation of those relationships over the last two decades has been a broad disempowerment and disenfranchisement of the citizen and user. Big Tech has not served the user as an agent working on their behalf. Rather Big Tech has surveilled and manipulated the citizen using invisible trackers and algorithms to promote the interests of the tech corporation, often in ways that have harmed the user, largely without the user's knowledge or consent. Tech corporations have earned many hundreds of billions of dollars in profits by exploiting these technologies, and the poor regulatory decisions of the last generation, to hyper-target individuals in order to persuade them to buy something, go somewhere, or to vote in a particular way — in exchange for payments from corporations, nation states, and people who seek to convince the user to buy a particular good, service, candidate, or idea.[43]

Unfortunately, for the last 20 years, most policymakers and law enforcement agencies have largely misunderstood how the last generation of technologies works, and/or how to use existing legal tools to reduce or eliminate the political, social, and personal harms that have resulted. And people have largely misunderstood whom technology in general, and AI tools, in particular, work for. Alexa works for Jeff Bezos, Meta AI works for Mark Zuckerberg, and Grok works for Elon Musk. These systems don't primarily serve the interests of regular people, even if they do provide benefits and value to users in some ways.

Amazon's Alexa, in standing in between the user and the sellers on the Amazon marketplace, weakened the user's ability to compare choices and quality, and steered the user toward the purchase of, for instance, Amazon Basics brand batteries instead of competitors' batteries, author Scott Galloway found.[44] (Note that the Federal Trade Commission and state attorneys general sued Amazon for self-preferencing its own products and for using Alexa to violate children's privacy laws[45]).

Facebook, too, has often portrayed its algorithms as tools for personalizing information in ways that serve the user by delivering content tailored to their interests, when in fact the information was personalized to serve the interests of Facebook's advertisers — hence ultimately serving the interests of Facebook's bottom line.[46]

Now Facebook is rocketing this problem to an entirely new orbit by integrating AI into its platforms without any new forms of protection. In a podcast interview, Mark Zuckerberg described as "super exciting" the ability to combine what Facebook learns about users from their interactions with the corporation's new integrated AI tools with what it learns about them from their feeds, all their existing profile information, and all their existing social graph information,[47] into what he called "a personalization loop." While personalization is a main value of AI agent technology, the question must be answered: Who does that personalization serve? What policy measures can ensure that personalization no longer is a means of control by the powerful, the oligarch, or the autocrat, but rather serves the citizen?

AI agents also risk amplifying the harms of the surveillance economy. The rise of surveillance pricing, a practice used by companies as wide-ranging as Delta, Uber, and Instacart,[48] only amplifies the potential harms of the next level of intermediation by AI agents. The AI agent can extract the maximum price for any purchase based on even greater amount of data about the user, with the corporation that created the agent pocketing the price differential. The AI agent could intimately know the limits of the user's attention, not to mention wallet, in any moment, and the maximum dollar amount that it can charge.

The dominant corporations that provide and control AI agents have introduced many tools to protect their corporate customers against surveillance. But when it comes to AI tools used by regular people, they have introduced essentially nothing to protect their interests.[49]

4. How AI Agents Can Make Existing Problems Worse

Absent action by government, today's new generation of AI agents will only increase the political, social, and economic harms caused by the business models of the last generation of dominant corporations. This is even more obviously true if Google, Amazon, Microsoft, and Facebook maintain their present control over the most advanced AI agents. These harms include the manipulation of public debate in ways that promote extreme political polarization, the degradation of trustworthy information and news, and a variety of social ills such as depression, various forms of addiction, and ever more extreme forms of financial exploitation.

These problems are not new. Dominant tech platforms like Facebook and Google, for instance, cut off essential traffic and revenue for journalism over the course of the second app-dominated era of the internet. But AI tools are already making these problems vastly more acute, such as by making it even harder for readers to connect directly to news publishers, while scraping their content and serving it up as answers to users. (See Appendix A for more detail on the digital age business model of these dominant corporations — sometimes referred to as surveillance, addiction, manipulation and extraction (SAME) — and how they serve the corporation's interests at the expense of the users' interests.)

Freedom of speech, of inquiry, and of thought requires a public sphere for the sharing of news and ideas, and for debate.[50] The dominant apps such as Google and Facebook have already dramatically limited the public's ability to engage in such protected actions, by individualizing feeds of content for specific people based on information learned about them through surveillance. The agentic web risks compounding this problem, as each person sees only the news or news-like content that is chosen for them or manufactured for them by their AI agent. Indeed, the agentic web is expected to be dominated by AI-generated content designed by machines for consumption by machines.[51]

Big Tech corporations over the years have provided many services that are of real value and benefits to users. But again, these corporations are not designed to serve the interests of either the individual user or the public as a whole and thus engage in business models that cause harm.

AI agents risk turbocharging these harms.

5. Could AI Agents Help Liberate People from Tech's Exploitative Business Models?

Let's envision a different world of possibilities, in which AI agents neutralize the exploitative business models of the digital age. AI agents could intermediate the relationships between people and tech companies with SAME business models or even disintermediate SAME corporations entirely by going straight to the seller, publisher, or content creator and cutting out the tech platform middlemen. If AI agents truly represented users' interests, AI agents could empower the people against exploitation.

This is not to say that AI agents are the best way to deal with the harms of the digital age or the modern economy. Laws, regulations, and law enforcement that protect the people against the abuses of concentrated corporate power, as well as government action to deconcentrate that power, would be the optimal course. Nonetheless, government action has fallen painfully short, and, meanwhile, AI agents are being deployed at a phenomenal pace.[52]

What would it take for the agentic web to develop in a way that is distributed and resilient, with each person and community having one agent — or a hive of specialized agents — that truly represent their interests? We could see a variety of benefits for the individual, some potentially dramatic in their effects.

Authentic AI agents could help consumers navigate the mazes, stumbling blocks, and hidden fees so prevalent in the modern economy, dubbed by *The Atlantic* as "The Annoyance Economy."[53] Authentic AI Agents could free people of their algorithmic news silos and hyper-targeting of content, directing users to news from sources across the political spectrum and helping users shield their data. And authentic AI agents could combat surveillance pricing, gathering information about prices being charged across the board, and negotiating the best price available.

We might also see an explosion of innovation and opportunities for entrepreneurs to start new businesses. And we might see some real de-concentration of economic opportunity, wealth, and power. Authentic AI agents could also promote government accountability, gathering data about the actions of a user's elected officials.

The possibilities are vast.

6. AI Agents and Fiduciary Duty Law

This paper lays out the challenges of ensuring that AI agents work for the people in ways designed to start the conversation without promising any ultimate answer. The intent is to ask the question of what types of policies should be explored to make AI agents work for the people and to prevent amplified exploitation by AI agents. Fiduciary duty law may prove to be an especially useful starting point for our analysis.

A. AI Agents and the Problem of Conflicting Fiduciary Duties

In the real world, human agents owe fiduciary duties to their human customers and clients and are required to always act in their customer's best interest. Any service that claims to act as an agent then should reasonably conform to fiduciary duty law.

However, an analysis of scholarly work raises a challenge: fiduciary duty principles cannot work when corporations have exploitative business models based on surveillance, addiction, manipulation and extraction, and existing fiduciary duties to shareholders to maximize profits. The AI agent's fiduciary duty to users will be in fundamental conflict with the SAME corporation's primary fiduciary duty to shareholders, hence its duty to maximize its use of surveillance, addiction, manipulation and extraction.

In 2014, Yale law professor Jack Balkin and Harvard law professor Jonathan Zittrain published a law review article proposing that Big Tech platforms should be treated as "information fiduciaries."[54] They defined a fiduciary as "one who has special obligations of loyalty and trustworthiness toward another person," explaining that "[t]he fiduciary must take care to act in the interests of the other person..."[55] "The client," they added, "puts their trust or confidence in the fiduciary, and the fiduciary has a duty not to betray that trust or confidence."[56]

Balkin and Zittrain argued the law should impose duties of care, confidentiality, and loyalty on tech companies like Google, Microsoft, Twitter (now X), and Uber to their end users, just as the law imposes such duties on doctors, lawyers, accountants, and estate managers. Each tech corporation should be deemed an "information fiduciary," defined as "a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship."

Zittrain later went on to present the information fiduciary duty framework as an alternative to "heavy-handed government intervention."[57] And at least one key founder of a platform monopoly — Mark Zuckerberg — embraced the idea, claiming that Facebook was already acting as a fiduciary to its users.[58]

In 2019, while working as a staffer in Congress, Lina Khan published an article with co-author David E. Pozen critiquing Balkin and Zittrain's information fiduciary proposal. Khan and Pozen pointed out that Facebook, Google, Twitter, and Uber were all Delaware corporations, and their officers and directors therefore owed fiduciary duties to the corporations and their shareholders. Khan and Pozen noted that Delaware fiduciary law does not allow traditional, for-profit corporations to consider other constituencies besides shareholders.[59] Balkin's proposed legal framework, therefore, would create an untenable position for corporate officers and directors. As Khan and Pozen put it, officers and directors cannot simultaneously honor their fiduciary duties to shareholders under Delaware law and their fiduciary duties to end users under the "information fiduciaries" regime. This in turn would mean that whenever shareholder and user interests diverged, the corporation's duties to their shareholders would win out.[60]

Using Facebook specifically as an example, Khan and Pozen pointed out how the interests of a social media corporation's stockholders and users would likely diverge. Facebook makes its money by selling targeted advertisements, which brought in $162.4 billion in 2024 alone.[61]

> "Like other corporations with comparable business models, Facebook therefore has a strong economic incentive to maximize the amount of time users spend on the site and to collect and commodify as much user data as possible.[62] By and large, addictive user behavior is good for business.[63] Divisive and inflammatory content is good for business.[64] Deterioration of privacy and confidentiality norms is good for business.[65] Reforms to make the site less addictive, to deemphasize sensationalistic material, and to enhance personal privacy would arguably be in the best interests of users. Yet each of these reforms would also pose a threat to Facebook's bottom line and therefore to the interests of shareholders.[66]"

While traditional fiduciaries like doctors and lawyers do sometimes experience tensions and misalignments with their

fiduciary obligations, and are ordinarily required to disclose them, the conflicts that tech platforms would experience go to the very core of their business models. And although fiduciary duties vary from context to context, one principle holds true: "the fiduciary always must act in the customer's best interest."[67] A fiduciary duty to users thus would not work with any existing business model based on surveillance, addiction, manipulation and extraction, like targeted behavioral advertising. By downplaying these differences between tech platforms and doctors and lawyers, Balkin's proposal hides the power imbalances that exist between ordinary people and tech platforms, Khan and Pozen concluded, describing them as "imbalances that stem both from the business model these firms employ and from the market dominance they enjoy."[68]

It follows then, that in order for AI agents to uphold fiduciary duties to users, they would need to employ business models that do *not* involve surveillance, addiction, manipulation, and extraction. And further, they must operate in competitive markets where users easily find similar services from a rival provider.

The business models and the market dominance of Big Tech make it impossible for them to promise to primarily serve the interests of the individual user/citizen/consumer. Fiduciary duties and business models must be aligned. With the imbalance of power between tech corporations and users stemming from both SAME business models and market dominance, both different business models and deconcentrated market structures are needed for AI agents to truly work on behalf of the people.

B. The "Net Fiduciary" Model

A growing class of innovators aims to authentically represent the interests of the individual user, not the corporation. In a paper published in 2024, Richard Whitt, founder of GliaNet and the GliaNet Alliance, proposed the "digital trustmediary" (DTM) in which intermediaries provide digital services to their clients, while voluntarily operating under heightened fiduciary duties of loyalty, care, and confidentiality. Whitt's vision "encompasses an individual creating and building a relationship with a digital trustmediary that actively promotes that individual's interests."[69] Whitt's proposal is different from Balkin and Zittrain's because he does not suggest that the Big Tech platforms with their SAME business models act as fiduciaries. Rather, Whitt proposes the creation of third-party authentic agents that mediate the interactions between users and the existing web or between users and other AI agents.

Whitt formed the GliaNet Alliance, a coalition of tech companies and other entities "committed to building a community of trustworthy Web intermediaries and edgetech capabilities."[70] The coalition's mission is "to develop open-source governance frameworks for a new sector of 'Net Fiduciaries' and AI agents, rooted in duties of care and loyalty."[71] The Alliance aims "to foster authentic trust-based digital markets that prioritize the best interests of individuals and communities," in a "self-regulating organization, with a formal certification and enforcement regime."[72]

Big Tech's business models monetize people's data in service of their own interests, says the Alliance. The coalition demonstrates the potential for agents that truly work for the people because many of its members have created new business models that focus on serving users. This alone makes it an important step in the right direction.

But Whitt's framework is voluntary and recommends the use of certified "trustmarks" to identify trustworthy intermediaries.[73] The GliaNet Alliance has not developed a way to guarantee the ability to protect people from being deceived and exploited by the AI tools of Google, Microsoft, and other corporations that rely on surveillance, addiction, manipulation and extraction business models.

As noted above, a few already dominant corporations control the means of distribution and are hence much more likely to reach, and be used by, regular people. These corporations have also demonstrated great ability to stop rivals from growing and expanding through a variety of different means.

Moreover, in the face of dominant tech platforms that act as the infrastructure of the internet,[74] innovators with better business models, such as those that protect privacy, have only gained limited traction in the digital age.[75] Business models based on surveillance, addiction, manipulation, and extraction are the prevailing business strategy used by tech companies no matter their size or their market power. However, those innovators who have sought to utilize different business models have often found they cannot get through dominant platforms' gatekeeping to reach users.[76] Strong antitrust enforcement and antimonopoly policies, discussed further below, must therefore prevent "Net Fiduciaries" from getting crushed by tech giants' "buy, bury, or kill" *modus operandi* toward competitive threats.[77]

In terms of policy measures, Whitt focuses primarily on interoperability and data portability to ensure that "Net Fiduciaries" can connect with the dominant players and their data silos. "[I]nteroperability is the bedrock for a competitive market where truly pro-consumer agents can thrive," echoes Dazza Greenwood of Consumer Reports.[78] With the promise of AI agents' innovation being tied closely to agent-to-agent communication, the agentic web requires interoperability to reach its innovative potential. Moreover, universal open standards have been developed to support this vision.[79]

Here again, however, the promise is highly circumscribed by the power of the corporations that already dominate communications and commerce on the internet, and most of the layers in the AI agent tech stack. The simple fact remains that new innovators will need access to Big Tech's walled gardens to neutralize SAME business models and realize the potential of the agentic web.

In fact, history demonstrates repeatedly that interoperability policies alone are not sufficient to promote and protect innovation or the ability to build a sustainable business in the face of the power of an entrenched incumbent. The U.S. Department of Justice lawsuit against Apple for monopolizing smart phone markets, for example, provided numerous examples of Apple outright blocking or creating friction with interoperability in order to preserve its monopoly power.[80] The same was true of long distance phone providers, who were legally required to integrate with competitive local exchange carriers (CLECs) by the Telecommunications Act of 1996, but have pulled endless tricks to make interconnection difficult.[81] As a legal tool, interoperability is necessary but not sufficient to achieve a competitive market that allows AI agents independent of corporations that rely on surveillance, addiction, manipulation, and extraction to loyally serve users.

It is therefore vital that policymakers prioritize addressing the present structure and behavior of the corporations that dominated the second generation of the internet and now appear ready to dominate the next agentic era. A common pattern in the digital age has been for corporations to introduce technology as open and fully interoperable and then move to closed models, usually once they have gained sufficient market power.[82] In fact, this is already happening with AI agents, as several of the big players have exploited existing market power in their legacy technologies to promote their own agents and to block the agents of others. On October 18, 2025, for instance, Meta announced it is changing its API policy to bar AI agents made by other companies from using its platform, closing off access to companies like OpenAI, Perplexity, Luzia, and Poke that had deployed WhatsApp-based agents.[83] The change made WhatsApp unavailable as a way to distribute AI agents, leaving Meta AI as the only agent available on the app.

Similarly, in November of 2025, Amazon sued Perplexity to stop its Comet AI agents from accessing its e-commerce marketplace.[84] Amazon alleges that Perplexity violates computer fraud and abuse statutes, puts consumer data at risk, and degrades the shopping experience.[85] Perplexity responded to threats from Amazon with a blog post entitled "Bullying is Not Innovation."[86] "Amazon wants to eliminate user rights so that it can sell more ads right now and partner with AI agents designed to take advantage of users later," reads the post. Amazon has its own AI assistant for shopping, called Rufus,[87] and it has indicated plans to partner with third-party agents. Perplexity's post continues, "Users want AI they can trust, and they want AI Assistants that work on their behalf and no one else's."[88] On March 10, 2026, a federal judge granted Amazon a temporary injunction against Perplexity, ruling that Amazon was likely to succeed on the merits of its case.[89] This is an unfortunate decision that helps Amazon fortify its walled garden and keep out competition. It also demonstrates the huge challenges ahead for anyone who claims they will be able to engineer and scale an agent that challenges the dominance of the corporations that control communications and commerce online, as well as the emerging AI tech stacks. At time of publication, Perplexity has been awarded a stay of the decision pending appeal.

7. Recommended Policy Priorities

Any proposal to regulate AI faces extreme headwinds now, due to President Trump's and policymakers' repeated efforts to bar AI regulation. But no matter the political challenges of the moment, allowing exploitation of the people by AI agents is not an option. If AI agents are legally permitted to betray users' interests with SAME business models, they will. Corporations are profit-maximizing by design. If laws can be broken and the only consequence is a monetary fine that amounts to a cost of doing business, tech corporations will continue to abuse users.

The digital age has been repeatedly marked by the failure of policymakers to impose traditional real-world laws — some of which have been in place for centuries — to the online world. This is perhaps the single biggest reason for today's concentration of power and lawlessness. It is illegal to read someone's mail, for example, yet email service providers scraped users' email accounts with impunity.[90] As AI agents replace offline roles, a continuation of this trend is a recipe for even more dangerous and widespread abuse and exploitation.

Already today, AI agents — and hence the corporations that control them — are giving investment and legal advice to individuals. In such instances, and in all reasonably analogous situations, the AI agent is serving a role traditionally held by humans bound by real-world fiduciary duties, yet they are doing so without having to abide by the same duties.

Based on such lessons of recent history, policymakers should prioritize the following four actions:

A. Apply Traditional Real-World Fiduciary Duties to AI Agents That Perform the Functions of Human Agents

Policymakers must immediately address the question of how to regulate AI agents acting as a real estate agent, a lawyer, investment broker, or any reasonably analogous role. An effective way to do so is to require any product labeled as an AI "agent" to be 100 percent responsible to the individual end user. This in turn means that no product labeled as an AI "agent" can be used for any SAME business model or practice, given that these actions violate an agent's duty to always act in the customer's best interest.

Policymakers should also consider how fiduciary duty rules could be imposed on AI agents and other AI tools that do not replace offline agentic roles but that users are led to believe are acting on their behalf and serving their interests.

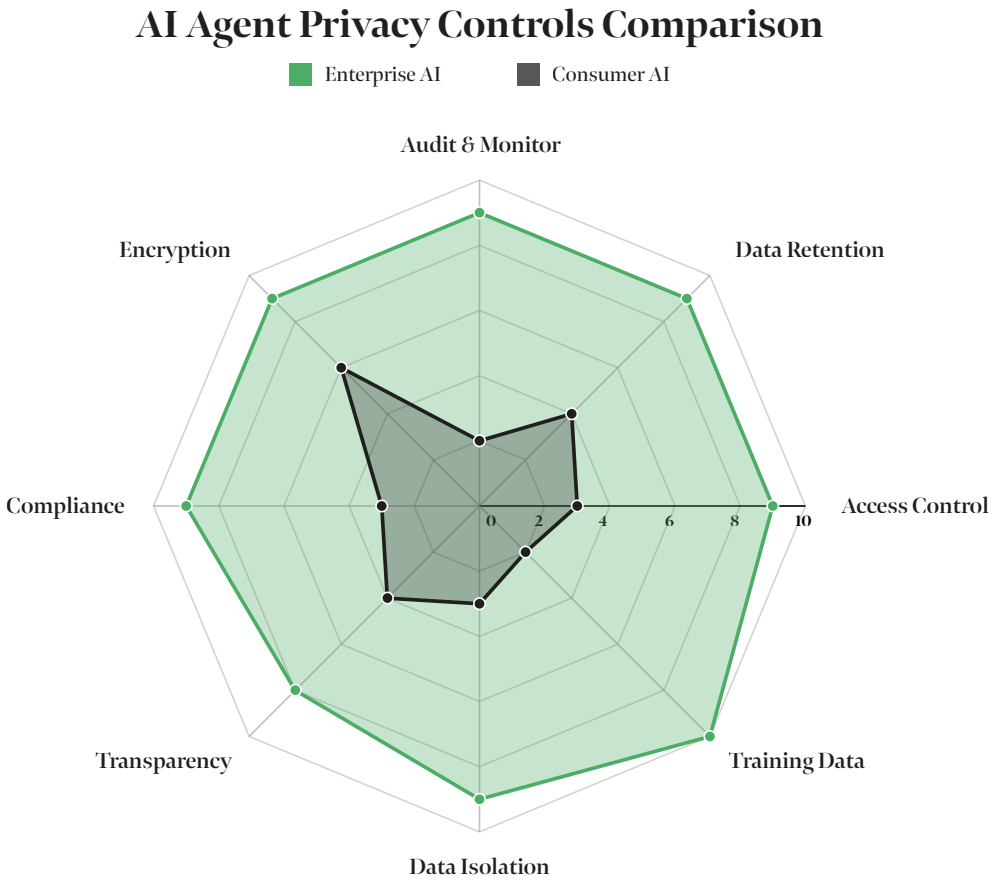
B. Develop Protections Against Surveillance

For AI agents to serve as legal fiduciaries to the people, they cannot simultaneously serve as surveillance machines that transmit every bit of information they learn about an individual into a data profile assembled for the purpose of manipulating that individual in any way. Without such protections, people using AI agents effectively have a spy in their mind that is acting as an agent of Google, or Meta, or OpenAI, or another AI corporation. To reinforce efforts to impose the actual responsibilities of real-world human agents on AI "agents," policymakers should develop data protections for any service that might be presented as an agent, or that seeks to exploit the trust of the individual user.

AI agents that serve corporate customers are closer to actual agents, as classically understood, proving that an alternative to the status quo exists. Thus, a starting point for data protection is the model that has been used for the enterprise AI customer, an example of a customer that does have AI agents serving its interests. Several protections to empower the user's control over their data have been deployed in the enterprise context but are virtually non-existent when it comes to AI agents used by regular people.[91]

The balance of power between a corporation paying an AI corporation for business agentic solutions is far different than the balance of power between a regular person and an AI company. Any employee who encounters an AI agent through their job, however, should assume that AI agent does not work for them as an employee, but rather for their employer.

The below charts, created using Perplexity AI, create a picture of the stark differences between enterprise AI and consumer-facing AI when it comes to privacy controls.[92] One can easily see what it looks like when AI works for the customer (the enterprise corporation) compared with what it looks like when AI doesn't (the consumer).



Examples of data protection controls that are standard practice for enterprise AI agents but are not available in the leading consumer-facing AI agents include:

- Model training off by default: AI agents are contractually prohibited from using customer prompts for model tuning.[93]
- Customer-managed keys: enterprise customers control their own keys for encryption and decryption, instead of the AI provider having the right to decrypt.[94]
- Zero-day data retention, or custom data retention periods. Data retention varies widely in consumer-facing AI, with Meta AI and Grok retaining a user's interactions indefinitely unless the user finds the opt-out setting.
- Compliance with stringent regulatory privacy frameworks.[95]
- Role-based access control (RBAC): enterprise customers assign unique identities to each AI agent, similar to how they manage human employees, enabling precise control over what data agents can access and which operations they can perform.

Policymakers must ask: Is it practicable to make similar data protections available to non-corporate users? If not, why not? What kinds of data practices would best protect regular people, without creating too many burdens on them to constantly monitor how their data is handled? Requiring that comparable data protections are available to all could be one significant way to move agents in the direction of working for users. What technical solutions and protocols could help foster a network of AI agents that serve users' interests rather than spying on users?

C. Enforce Laws Designed to Ensure Open Markets

Policymakers can help shape the AI agent market to develop openly and avoid powerful gatekeepers and chokepoints.

Competition policy is needed to promote and protect innovation in AI agents that serve the people, and to ensure that corporations that rely on surveillance, addiction, manipulation, and extraction business models don't squash authentic AI agents. With trillions of dollars at stake, it is unlikely already dominant corporations will stand by and allow innovators to disrupt existing business models designed to surveil, addict, manipulate, and extract by serving as loyal fiduciaries to the citizen, when they have both the incentive and ability to "buy, bury, or kill" them and thereby neutralize the threat they pose.

Rules of the road are needed to prevent dominant tech companies from leveraging their control over different parts of the AI technology stack as chokepoints — the hardware, cloud, models, and application layers — acting as gatekeepers over access to markets.[96]

Monopolization by corporations that rely on surveillance, addiction, manipulation, and extraction — and foreclosure of authentic AI agents that serve the people — is the familiar arc we will almost certainly see if policymakers do not take action to promote and protect innovation. Just as the monopolists' playbook has remained remarkably consistent over time, the set of solutions will be essentially the same for AI agents as it was for railroads, long-distance calling, and the tech platforms themselves.

A recent Open Market Institute report, *Stopping Big Tech from Becoming Big AI: A Roadmap for Using Competition Policy to Keep Artificial Intelligence Open for All*, by Max Von Thun and Daniel Hanley,[97] provides a good introduction to what such actions would look like. That report calls for policymakers to:

- *Block mergers and anticompetitive partnerships*: Prevent dominant firms from solidifying control over AI by halting mergers and breaking up existing exclusive agreements that limit market diversity.
- *Break up concentrations of power*: Target the concentration of power across the AI technology stack by applying structural separation and vertical integration restrictions.
- *Guarantee access to essential inputs*: Impose non-discrimination obligations on dominant firms to ensure fair access to computing power and other critical AI resources.
- *Enable consumer and business switching*: Empower consumers and businesses by enforcing data portability and interoperability.

This antimonopoly toolkit is an important starting point for promoting competition in the AI agent market.

D. Require Transparency and Easy Audits

Enterprise AI agents offer granular auditing capabilities for corporate users. Policymakers must ask: Why not require these same capabilities be provided to everyone? Further, policymakers must do so in a way that does not place the burden on users to audit AI agents, in order to hunt down instances where the agent betrayed their interests. The great majority of people simply do not have enough time, resources, or training to do such auditing. Policymakers must therefore immediately begin to define the types of transparency measures that would actually protect users, without imposing unrealistic demands on them. Experts worldwide are working on AI transparency issues, which have critically important implications for AI safety beyond the AI agent context.[98] But functional policy also demands that policymakers establish some sort of market structure for businesses or other actors to provide mass auditing on behalf of users.

8. Key Questions For Policymakers

As they approach this next great challenge in regulation of the digital information system, policymakers must ensure they are guided every day by the following four questions:

- How do we ensure that the AI "agent" is in fact working for the user, instead of a tool of the corporation to manipulate the user, or a tool of the state in alliance with the corporation, with unprecedented access to personal information and unprecedented means of user control?
- Given our collective experience with Big Tech middlemen, and the profound effects of their intermediation on journalism, wealth inequality, and democracy, in what ways could AI agents, as the next level of middlemen, amplify these harms?
- Could AI agents intermediating today's dominant digital platforms provide an opportunity to build a new deconcentrated and democratically resilient agentic web that serves humanity?
- What policy actions can be taken now to foster the development of a deconcentrated agentic web that serves the people?

Without asking these questions as a society now, the present extreme exploitation of individual users will not merely continue but grow rapidly and dramatically worse. So too will all the related threats, to democracy, innovation, human creativity, human spiritual freedom, and the basic functioning of society. We must ensure that markets develop in a manner where AI agents work for the user, people are not surveilled by AI agents, and authentic AI agents are not squashed by dominant tech corporations with exploitative business models.

9. Conclusion

Before us is the opportunity for a deconcentrated political economy of information, a more resilient democracy, a less extractive economy, and a less polarized America that is free of manipulative algorithms. Such a goal may seem unrealistic, because it is so different from our lived experiences of the digital age. But it is not merely possible, it is eminently achievable given sufficient political will.

To achieve these possibilities of the agentic web, and to usher in AI agents that empower the citizen user, corporations that subject users to surveillance, addiction, manipulation, and extraction business models cannot be recognized as trusted AI agents. Nor can market dominance be allowed to thwart innovators that do work for the people.

Many questions remain unanswered. Yet the North Star of all policymaking should ask: Who does the AI agent work for? How can we promote the development of a deconcentrated network of AI agents that serves the people?

Appendix A

The harms of Big Tech's business models based on surveillance, addiction, manipulation, and extraction have been documented extensively.[99] Here is a quick summary of how they work.

Surveillance

Tech giants have an all-encompassing view of what you read, think, do, believe, buy, watch, where you go, who you're with, even how many credit lines you have and what you invest in. The companies track you across millions of websites, devices, tech wearables, and offline, and combine the data they collect on you with data from other companies, like data brokers, or your smart TV maker. Google and Meta have repeatedly been found to violate privacy laws.[100] A 2024 study by Consumer Reports found that each Facebook user's data came from an average of 2,230 companies, including data brokers, retailers, credit reporting agencies, and payment processors.[101]

Most tracking by tech giants is designed to target us with ads and sell us stuff, which may seem harmless. Although the now common practice of *surveillance pricing* certainly is not.[102] And whatever data Big Tech collects, the government can get.[103] Digital surveillance is a modern development, but surveillance itself has a long dark history of being used by the powerful to control and persecute innocent people. Whether the Stasi in East Germany, McCarthyism's spying on Americans, China's citizen's scores based on surveilled obedience, or ICE's screening of social media accounts for political protest,[104] surveillance does not serve the people.

Addiction

The more time people spend on social media and other digital platforms, the more data the platforms collect, the more ads they show, and the more money they make. Taking Meta as an example, in 2024, it made more than $3 billion *per week* by collecting data and then targeting ads at individuals based on that data. Meta reports to investors how much of users' time and attention it can hoard because that's what fuels its targeted advertising business model.[105] According to lawsuits filed by 42 state attorneys general in October 2023, Meta knowingly designed and deployed harmful features that purposefully addict children and teens.[106]

Manipulation

When it comes to harmful and deceptive content, most people think social media platforms like Facebook's and YouTube's main problem is they can't take millions of posts down quickly enough. But these platforms actually *boost* hate and disinformation. Their algorithms prioritize "engagement" (that is, clicks, likes, comments, and shares) to keep users on their platform longer because content that provokes fear and anger — the most incendiary content — "engages" humans the most.[107] Meta's and YouTube's algorithms take fear-mongering to the extreme by targeting content at individuals based on all the bits of data the platforms have collected about them.[108] Because of surveillance, the algorithms know what content is likely to make each individual react and know how to target each person based on their particular vulnerability. Indeed, Facebook's algorithms were responsible for recruiting the majority of QAnon members, according to the company's own internal research.[109]

Just as social media giants enable advertisers to influence people's purchasing decisions, they enable propagandists to influence people's political decisions. These platforms make propagandists' work easy by spying on us, by programming their algorithms to amplify incendiary content, and by developing micro-targeting that allows propagandists to individually target voters based on highly granular data it has gathered about them.

Extraction

At the same time that they amplified disinformation, the tech platforms siphoned off the ad dollars that used to support trustworthy journalism, using publishers' work product as fodder for their platforms and taking the financial gains for themselves. Once dominant tech platforms control the infrastructure of the internet and act as gatekeepers, they act as trolls collecting tolls from everyone who must cross their bridge, be it the consumer, the entrepreneur, the innovator, or the business. All market participants have little choice but to deal with the dominant platform on its terms. The result has been rampant extraction of the fruits of the labor of artists, merchants, publishers, businesses, and workers, intensifying economic inequality and imperiling the American Dream.[110]

Another way that most people have served the interests of Big Tech, rather than the other way around, is by helping to train Big Tech's algorithms, doing "digital labor" without compensation. As entrepreneur Joe Toscano explained in his 2019 TEDx Talk, "Want to Work for Google? You Already Do," Google Maps is only as good as it is because billions of us effectively work for Google, taking pictures of meals, adding

ratings and reviews, and pinning locations. "Companies have turned billions of us into unpaid machine trainers," said Toscano, creating "a multi-trillion-dollar stream of unpaid untaxable labor."[111]

Google has also rolled out Google AI Studio, which enables people to make their own AI agents and applications, a practice commonly referred to as "vibe coding." But is it just another way for Google to get free digital labor, in the form of both data and great ideas? The Gemini terms of service as of December 2025 read:

> "Some of our Services allow you to generate original content. Google won't claim ownership over that content. You acknowledge that Google may generate the same or similar content for others and that we reserve all rights to do so.... When you use Unpaid Services, including, for example, Google AI Studio and the unpaid quota on Gemini API, Google uses the content you submit to the Services and any generated responses to provide, improve, and develop Google products and services and machine learning technologies, including Google's enterprise features, products, and services..." [112]

It turns out that data created by our digital labor is a scarce resource that is desperately needed for AI development. As Dr. Courtney C. Radsch, director of Center for Journalism and Liberty at Open Markets Institute, wrote in an article entitled, *AI Needs Us More Than We Need It*, to "make bots smart you need to feed them high-quality data created by humans." Yet "we are running low on such data and will run out all the faster if AI puts more human content creators out of business."[113] Despite appearances, Big Tech has never worked for you, and, if anything, you have worked for it.

Acknowledgements

Deep thanks to reviewers Dr. Courtney C. Radsch, Tara Pincock, Stephanie Nguyen, and Katie Van Dyck for your feedback and insights.

Endnotes

1 The Knight First Amendment Institute at Columbia University, in a recent paper, defines an AI agent as "compound software systems, inclusive of one or more AI models, that operate within an environment and take actions with it."(https://knightcolumbia.org/content/levels-of-autonomy-for-ai-agents-1) The paper defines the user as "an entity, human or AI, who issues an initial request for the agent's services." Another definition comes from Dazza Greenwood, Protocol Lead at Consumer Reports Digital Lab: "An AI agent is a digital assistant powered by advanced AI technologies, particularly Large Language Models (LLMs), which enable them to understand and respond to complex instructions, reason about different options, and use tools." (https://innovation.consumerreports.org/engineering-loyalty-by-design-in-agentic-systems/)

2 I will reluctantly usually use the term "users," though "citizens" or "people" would be preferable and avoid de-humanizing those who use this technology. I will, however, sometimes use the word "citizen" when I want to emphasize the political nature of the interaction between the AI corporation and the individual. When I do so, my intention is to include all people, whether they are citizens or not, and to draw attention to the aspect of humanity that possesses certain unalienable political rights.

3 https://dev.to/esdanielgomez/lets-talk-about-agentic-web-or-web-40-4m88; https://arxiv.org/pdf/2507.21206

4 Allen, Jennifer. 2021. "10 Years of Siri: The History of Apple's Voice Assistant." TechRadar. October 4, 2021. https://www.techradar.com/news/siri-10-year-anniversary.

5 Etherington, Darrell. 2014. "Amazon Echo Is a $199 Connected Speaker Packing an Always-on Siri-Style Assistant." TechCrunch. TechCrunch. November 6, 2014. https://techcrunch.com/2014/11/06/amazon-echo/.

6 "Gemini Agent - AI Automation for Daily Tasks & Multi-Step Work." 2025. Gemini. https://gemini.google/overview/agent/; Lanz, Jose Antonio. 2026. "Google Brings Agentic Browsing to Chrome—and It's Not Playing Nice with Competitors." Yahoo Tech. January 29, 2026. https://tech.yahoo.com/ai/gemini/articles/google-brings-agentic-browsing-chrome-215333659.html;

"AI in Chrome | Meet the next Generation of AI in Chrome | Chrome." Google.com. https://www.google.com/chrome/ai-innovations/.; Elias, Jennifer. "Google Is Unleashing Gemini AI Features on Gmail. Users Will Have to Opt Out." CNBC, 8 Jan. 2026, www.cnbc.com/2026/01/08/google-adds-gemini-features-to-gmail-message-summaries-proofreading-.html.

7 Pazur, Barbara. "What Is Meta AI? Everything to Know about the Tech Giant's AI Tools." CNET, July 10, 2025, www.cnet.com/tech/services-and-software/what-is-meta-ai-everything-to-know-about-the-tech-giants-ai-tools/.

8 "Microsoft and OpenAI Extend Partnership." Microsoft Blog, January 23, 2023. https://blogs.microsoft.com/blog/2023/01/23/microsoftandopenaiextendpartnership/.

9 "AI Agents Are Changing the Way We Work." Microsoft 365. https://www.microsoft.com/en-us/microsoft-365-copilot/agents. "Gemini Enterprise." Google Cloud. https://cloud.google.com/gemini-enterprise.; "Unlock the Future of AI Agent Orchestration with IBM Agent Connect." IBM. https://www.ibm.com/new/announcements/unlock-the-future-of-ai-agent-orchestration-with-ibm-agent-connect.

10 Radsch, Courtney C. "The Battle for Cognitive Liberty in the Age of Corporate AI." Tech Policy Press, January 6, 2026. https://www.techpolicy.press/the-battle-for-cognitive-liberty-in-the-age-of-corporate-ai/

11 "The Big Tech Extortion Racket: How Google, Amazon, and Facebook Control Our Lives," Barry C. Lynn, Harper's Magazine, September 2020; "AI and Surveillance Pricing May Squeeze Wallets More." Marketplace, July 25, 2025. https://www.marketplace.org/story/2025/07/25/ai-and-surveillance-pricing-may-squeeze-wallets-more; Wells, Katie J. and Owen, Lindsay, Groundwork Collaborative, Hang, Angel and Smith, Alan, Consumer Reports, "Same Cart, Different Price: Instacart's Price Experiments Cost Families at Checkout," December 9, 2025, https://groundwork-collaborative.org/work/instacart/.

12 Christopher, Nilesh and Pepe, Velerio. "As Millions Adopt Grok to Fact Check, Misinformation Abounds." Al Jazeera, July 11, 2025. https://www.aljazeera.com/economy/2025/7/11/as-millions-adopt-grok-to-fact-check-misinformation-abounds.

13 Zeff, Maxwell. "Grok 4 Seems to Consult Elon Musk to Answer Controversial Questions." TechCrunch, July 10, 2025. https://techcrunch.com/2025/07/10/grok-4-seems-to-consult-elon-musk-to-answer-controversial-questions/.

14 Klee, Miles. "Elon Musk's Grok Chatbot and Antisemitic Posts." Rolling Stone. July 8, 2025. https://www.rollingstone.com/culture/culture-news/elon-musk-grok-chatbot-antisemitic-posts-1235381165/; Jones, Dylon. "Hitler AI." Politico, July 10, 2025. https://www.politico.com/news/magazine/2025/07/10/musk-grok-hitler-ai-00447055.

15 X employees also coded Grok to be "maximally based," a slang phrase adopted by the far right to go against "woke" narratives. Id.

16 "Empowering Consumers with Personal AI Agents: Legal Foundations and Design Considerations." Consumer Reports. https://innovation.consumerreports.org/empowering-consumers-with-personal-ai-agents-legal-foundations-and-design-considerations/.

17 One of the first such efforts was New York State's Telegraph Act of 1848. Its goal was to check what one journalist at the time called the "stupendous power" of telegraph monopolies over the flow and content of news by making it easier for new competitors to join the market. The law did so by prohibiting telegraph operators from discriminating in favor of any one person's or company's messages, which it did by mandating that the operator carry messages on a first- come, first-served basis, and that it charge all senders the same price and terms. Similar rules were implemented over telecommunications systems and internet service providers. See Richard John, Network Nation: Inventing American Telecommunications (Cambridge, Massachusetts: The Belknap Press of Harvard University Press, 2010), 91, 124-125, 138.

18 Lynn, Barry C., "The Antitrust Revolution: Liberal Democracy's Last Stand Against Big Tech," Harper's Magazine, Oct. 2024, https://harpers.org/archive/2024/10/the-antitrust-revolution-big-tech-barry-c-lynn/

19 See e.g. Hanley, Daniel, "The Case for Rethinging Section 230 and Bloated Tech Monopolies," The Reboot, March 29, 2021, https://web.archive.org/web/20210419051607/https://thereboot.com/reassessing-section-230-and-bloated-tech-monopolies/; Hubbard, Sally, "Forget Bias, the Real Danger is Big Tech's Overwhelming Control Over Speech," CNN, Nov. 17, 2020, https://www.cnn.com/2020/10/28/perspectives/section-230-hearing-big-tech/index.html.

20 "AI Agents and Their Impact on Society." IBM. https://www.ibm.com/think/topics/ai-alignment.

21 "Introducing ChatGPT Enterprise." OpenAI. https://openai.com/index/introducing-chatgpt-enterprise/. "What is the Enterprise Plan." Claude. https://support.claude.com/en/articles/9797531-what-is-the-enterprise-plan; "Amazon Bedrock Security and Privacy." Amazon. https://aws.amazon.com/bedrock/security-compliance/; "Enterprise dat Protection in Microsoft 365, Copilot and Microsoft 365 Copilot Chat." Microsoft. https://learn.microsoft.com/en-us/copilot/microsoft-365/enterprise-data-protection

22 Khan, Lina M., and David Pozen. "A Skeptical View of Information Fiduciaries." Yale Law Journal 129 (2020); Radsch, Courtney C. "The Battle for Cognitive Liberty in the Age of Corporate AI." Tech Policy Press, January 6, 2026. https://www.techpolicy.press/the-battle-for-cognitive-liberty-in-the-age-of-corporate-ai/

23 The Knight First Amendment Institute at Columbia University, in a recent paper, defines an AI agent as "compound software systems, inclusive of one or more AI models, that operate within an environment and take actions with it." "Levels of Autonomy for AI Agents." Knight First Amendment Institute at Columbia University. https://knightcolumbia.org/content/levels-of-autonomy-for-ai-agents-1.The paper defines the user as "an entity, human or AI, who issues an initial request for the agent's services."

24 "AI Agent vs. AI Chatbot." DigitalOcean. https://www.digitalocean.com/resources/articles/ai-agent-vs-ai-chatbot.

25 "AI Agents vs. AI Assistants." Quisitive. https://quisitive.com/ai-agents-vs-ai-assistants/.

26 Greenwood, Dazza. "Engineering Loyalty by Design in Agentic Systems." Consumer Reports Digital Lab. https://innovation.consumerreports.org/engineering-loyalty-by-design-in-agentic-systems/. ("An AI agent is a digital assistant powered by advanced AI technologies, particularly Large Language Models (LLMs), which enable them to understand and respond to complex instructions, reason about different options, and use tools.")

27 "Meta is Targeting Hundreds of Millions of Businesses for Agentic AI." CNBC. https://www.cnbc.com/2025/03/06/meta-is-targeting-hundreds-of-millions-of-businesses-for-agentic-ai.html.

28 Id.

29 Kolekar, Rahul. "Llama 4 Agentic Capabilities Review: How to Measure Real Autonomy," January 3, 2026, https://rahulkolekar.com/llama-4-agentic-capabilities-review/.

30 "Introducing ChatGPT Agent." OpenAI. https://openai.com/index/introducing-chatgpt-agent/; "Grok 4.1 Fast and Agent Tools API." xAI. Nov. 19, 2025. https://x.ai/news/grok-4-1-fast.

31 See, e.g., "How Big Tech Killed Local Media & Over 250,000 Jobs Across the U.S." The Tech Oversight Project. Sep. 2022. https://techoversight.org/wp-content/uploads/2022/09/Big-Tech-Kills-Local-Journalism.pdf; Perotti, Elena, "Paying for News: Google and Meta Owe US Publishers $11.9-13.9 Billion Each Year," World Association of News Publishers, https://wan-ifra.org/2023/11/paying-for-news-google-and-meta-owe-us-publishers-11-9-13-9-billion-each-year/; Jim VandeHei, "Behind the Curtain: How Google Got Media Companies Addicted," Axios, May 8, 2018. https://www.axios.com/google-media-companies-facebook-tech-industry-a10898ee-e0b7-46ef-bcfc- d2561a2e0630.html; United Kingdom. Parliament. House of Commons. Disinformation and Fake News: Final Report. 2019; Radsch, Courtney. "The Value of News Content to Google Is Way More Than You Think." Tech Policy Press, August 8, 2023. https://techpolicy.press/the-value-of-news-content-to-google-is-way-more-than-you-think/

32 See, e.g., Tobias Rose-Stockwell, "This Is How Your Fear and Outrage Are Being Sold for Profit," Quartz, July 28, 2017, https://qz.com/1039910/how-facebooks-news-feed-algorithm-sells-our-fear-and-outrage-for-profit/; Marcia Stepanek, "The Algorithms of Fear," Stanford Social Innovation Review, June 14, 2016, https://ssir.org/articles/entry/the_algorithms_of_fear; House of Commons Digital, Culture, Media and Sport Committee, UK Parliament, "Disinformation and 'Fake News': Final Report," Feb. 14, 2019, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf; Olivia Solon, "Ex-Facebook President Sean Parker: Site Made to Exploit Human 'Vulnerability,'" Guardian, Nov. 9, 2017, https://www.theguardian.com/technology/2017/nov/09/facebook-sean-parker-vulnerability-brain-psychology.

33 See, e.g., Ron Knox, "The Copyright Killer," Global Competition Review, Jan. 11, 2019, https://globalcompetitionreview.com/insight/gcr-q1-2019/1179029/the-copyright-killer; Sergei Klebnikov, "Jeff Bezos Gets $6.4 Billion Richer as Amazon Stock Hits a New Record High," Forbes, April 14, 2020, https://www.forbes.com/sites/sergeiklebnikov/2020/04/14/jeff-bezos-gets-63-billion-richer-as-amazon-stock-hits-a-new-record-high/#4fc4bb6e53b0; Verne Kopytoff, "How Amazon Crushed the Union Movement," Time, Jan. 16, 2014, https://time.com/956/how-amazon-crushed-the-union-movement/; Chris Stokel-Walker, Karen Weise, "Prime Power: How Amazon Squeezes the Businesses Behind Its Store," New York Times, Dec. 19, 2019, https://www.nytimes.com/2019/12/19/technology/amazon-sellers.html. "'Success' on YouTube Still Means a Life of Poverty," Bloomberg, Feb. 26, 2018, https://www.bloomberg.com/news/articles/2018-02-27/-success-on-youtube-still-means-a-life-of-poverty.

34 See, e.g. Chung, Jane "Big Tech, Big Cash: Washington's New Power Players," Public Citizen, March 2021, https://www.citizen.org/article/big-tech-lobbying-update/; David Dayan, "The Android Administration, Intercept, April 22, 2016, https://theintercept.com/2016/04/22/googles-remarkably-close-relationship-with-the-obama-white-house-in-two-charts/; Katelyn Newman, "San Francisco Is Home to the Highest Density of Billionaires," U.S. News & World Report, May 10, 2019, https://www.usnews.com/news/cities/articles/2019-05-10/san-francisco-is-home-to-the-worlds-most-billionaires-per-capita, and Kevin Fagan, "Bay Area Homelessness: 89 Answers to Your Questions," San Francisco Chronicle, July 28, 2019, https://projects.sfchronicle.com/sf-homeless/homeless-questions/

35 "Microsoft and OpenAI Sign New AI Deal Paving Way for More Investments." PCMag. https://www.pcmag.com/news/microsoft-openai-sign-new-ai-deal-paving-way-for-more-investments.

36 "2025: The State of Consumer AI." Menlo VC. https://menlovc.com/perspective/2025-the-state-of-consumer-ai/.

37 Id.

38 "Top Generative AI Chatbots." First Page Sage. https://firstpagesage.com/reports/top-generative-ai-chatbots/.

39 Note that a federal court declared Google Search and illegal monopoly in 2024; laughably the court did not impose a breakup due to AI competition. United States, et al. v. Google, LLC, No. 20-cv-3010 (APM) (D.D.C. Aug. 5, 2024), Dkt. No. 1033.

40 Vanian, Jonathan. "Mark Zuckerberg says Meta AI has 1 billion monthly active users." CNBC, May 28, 2025. https://www.cnbc.com/2025/05/28/zuckerberg-meta-ai-one-billion-monthly-users.html.

41 "AI Agents by Market Share." First Page Sage. https://firstpagesage.com/seo-blog/the-top-ai-agents-by-market-share/.

42 "Agentic Commerce Opportunity: How AI Agents Are Ushering in a New Era for Consumers and Merchants." McKinsey & Company. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-agentic-commerce-opportunity-how-ai-agents-are-ushering-in-a-new-era-for-consumers-and-merchants.

43 For a more in-depth discussion of Big Tech's SAME business models, see Appendix A.

44 Galloway, Scott. "Alexa: How Can We Kill Brands?" Prof Galloway. https://www.profgalloway.com/alexa-how-can-we-kill-brands/.

45 "FTC Sues Amazon for Illegally Maintaining Monopoly Power." Federal Trade Commission. September 2023. https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-sues-amazon-illegally-maintaining-monopoly-power; "FTC and DOJ Charge Amazon with Violating Children's Privacy Law." Federal Trade Commission. May 2023. https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever.

46 Mark Zuckerberg, Facebook Post, January 11, 2018: "I'm changing the goal I give our produce teams from focusing on helping you find relevant content to helping you have more meaningful social interactions." https://www.facebook.com/zuck/posts/10104413015393571

47 Mark Zuckerberg. "The Future of AI Agents." Dwarkesh. https://www.dwarkesh.com/p/mark-zuckerberg-2.

48 "AI and Surveillance Pricing May Squeeze Wallets More." Marketplace, July 25, 2025. https://www.marketplace.org/story/2025/07/25/ai-and-surveillance-pricing-may-squeeze-wallets-more. Wells, Katie J. and Owen, Lindsay, Groundwork Collaborative, Hang, Angel and Smith, Alan, Conumer Reports, "Same Cart, Different Price: Instacart's Price Experiments Cost Families at Checkout," December 9, 2025, https://groundwork-collaborative.org/work/instacart/. "Personalized Pricing." The New York Times, July 26, 2025, https://www.nytimes.com/2025/07/26/business/dealbook/personalized-pricing.html; Kloczko, Justin. "Consumer Alert Details Uber Example of Surveillance Pricing." Consumer Watchdog. Dec. 19, 2025. https://consumerwatchdog.org/privacy/consumer-alert-details-uber-example-of-surveillance-pricing/

49 See, e.g. "How Private Are Popular AI Assistants?" Northbound Advisory. https://www.northboundadvisory.com/blog/how-private-are-popular-ai-assistants; "Anthropic's Claude AI: Updated Terms Explained." AMST Legal. https://amstlegal.com/anthropics-claude-ai-updated-terms-explained/. https://libguides.marian.edu/c.php?g=1321167&p=10738998 "Safeguarding the Enterprise AI Evolution: Best Practices for Agentic AI Workflows." ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2025/safeguarding-the-enterprise-ai-evolution-best-practices-for-agentic-ai-workflows.;"AI Agents: RBAC and VertexAI." Sakura Sky. https://www.sakurasky.com/blog/ai-agents-rbac-vertexai/; "Access Control in the Era of AI Agents." Auth0. https://auth0.com/blog/access-control-in-the-era-of-ai-agents/.

50 An important principle of First Amendment law is the counterspeech doctrine. Supreme Court justice Louis D. Brandeis established the doctrine in the 1927 case Whitney v. California, saying, "If there be time to expose through discussion, the falsehoods and fallacies, to avert the evil by the process of education, the remedy to be applied is more speech, not enforced silence." Brandeis's solution to deceptive or harmful speech is to counter it with speech that sets the record straight or conveys an opposite message, rather than censoring it. But with targeted social media feeds, users don't see counterspeech. Having no public sphere of debate, individualized algorithms programmed to push individuals' buttons, and a fear-mongering business model ready to be weaponized by wagers of culture war all exacerbate political division and destroy democracy.

51 "Agentic AI Report." Artificiality Institute. https://artificialityinstitute.org/agentic-ai-report/. Until now, websites and applications have been optimized for human consumption, in what is known as user-centered design or UX. Today, designers are also optimizing websites and applications for AI agent consumption, in a shift to agent-centered design or AX. "From UX to AX: Designing for AI Agents." Pragmatic Coders. https://www.pragmaticcoders.com/blog/from-ux-to-ax-designing-for-ai-agents ; Gomez, Daniel. "Let's Talk About Agentic Web or Web 4.0." DEV Community. https://dev.to/esdanielgomez/lets-talk-about-agentic-web-or-web-40-4m88.; "Understanding the Agentic Web." arXiv. https://arxiv.org/pdf/2507.21206.

52 Commentators, using a broad definition of AI agents, estimate that AI agents are on the verge of outnumbering humans. See e.g., "The Future of AI Agents," Your Everyday AI Podcast, https://www.youreverydayai.com/ep-666-the-future-of-ai-agents-will-there-be-more-agents-than-humans/

53 "The American Economy and Consumer Confidence." The Atlantic, October 2023, https://www.theatlantic.com/ideas/archive/2023/10/american-economy-consumer-confidence/675687/.

54 Balkin, Jack M. "The First Amendment in the Second Gilded Age." *UC Davis Law Review* 49, no. 4 (2016): 1205. https://lawreview.sf.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/49-4_Balkin.pdf.

55 Id.

56 Id.

57 Zittrain, Jonathan. "How to Exercise the Power You Didn't Ask For." Harvard Business Review, September 19, 2018.

58 Constine, Josh. "Highlights & Transcript from Zuckerberg's 20K-Word Ethics Talk." TechCrunch, February 20, 2019. https://techcrunch.com/2019/02/20/zuckerberg-harvard-zittrain/.

59 Miller, Robert T., Delaware Law Requires Directors to Manage the Corporation for the Benefit of its Stockholders and the Absurdity of Denying It (October 27, 2023). 48 Journal of Corporation Law, 32, 2023, U Iowa Legal Studies Research Paper No. 2023-39, Available at SSRN: https://ssrn.com/abstract=4615410.

60 Khan, Lina M., and David Pozen. "A Skeptical View of Information Fiduciaries." Yale Law Journal 129 (2020), at 504.

61 "How Does Meta Make Money?" Visual Capitalist. https://www.visualcapitalist.com/charted-how-does-meta-make-money/.

62 Khan and Pozen at 505, FN 35.

63 Id. at 505, FN 36

64 Id. at 505, FN 37

65 Id. at 505, FN 38

66 Id. at 505, FN 39

67 Khan and Pozen at 510.

68 Balkin published a response to Khan and Pozen, saying that the information fiduciary duties concept intended to require tech platforms to change their business models to the extent they don't serve users. However, he stated: We are still in the early stages of figuring out how digital advertisements actually work and the harms they actually cause. The more we earn about digital advertising, the more we may discover that some practices that initially seemed troublesome are mostly harmless, and those that seemed benign do real damage to end users and to the society in which they live." I find it unpersuasive in addressing the concerns Khan and Pozen raise. See Balking, Jack M. The Fiduciary Model of Privacy, Balkin, 134 Harvard Law review F. 11 at 29. (2021).

69 Whitt, Richard S., OLD SCHOOL GOES ONLINE: EXPLORING FIDUCIARY OBLIGATIONS OF LOYALTY AND CARE IN THE DIGITAL PLATFORMS ERA, 36 Santa Clara High Tech. L.J. 75 (2020), at 106 Available at: https://digitalcommons.law.scu.edu/chtlj/vol36/iss1/3 .

70 GliaNet Alliance Comments Responding to the UK Department for Science, Innovation & Technology: Shaping Policy for Data Intermediaries. May 12, 2025. https://www.glianetalliance.org/news/UKcallforevidenceondataintermediaries.

71 Id.

72 Id.

73 Id.

74 See Radsch, Dr. Courtney C., "Dismantling AI Data Monopolies Before it's Too Late," Tech Policy.Press, October 9, 2024, available at https://www.techpolicy.press/dismantling-ai-data-monopolies-before-its-too-late/

75 See e.g. DuckDuckGo, ProtonMail; Brave Browser. "Mobile Search Engine Market Share United States of America Dec 2024-Dec 2025" Global Stats. (showing Google's search engine market share at 93.19% with DuckDuckGo's market share at 2.07%; Note that Google's payments to Apple to be the default search engine were found to me illegal monopolization in court) https://gs.statcounter.com/search-engine-market-share/mobile/united-states-of-america

76 See, e.g., Huang, Roger. "Andy Yen, CEO of Proton, on the Tech Giants That Dominate the Internet, the Web's Future, and Bitcoin." Forbes, December 27, 2022. https://www.forbes.com/sites/rogerhuang/2022/12/27/andy-yen-ceo-of-proton-on-the-tech-giants-that-dominate-the-internet-the-webs-future-and-bitcoin/.

77 "FTC Alleges Facebook Resorted to Illegal 'Buy or Bury' Scheme to Crush Competition After String of Failed Acquisitions." Federal Trade Commission. August 2021. https://www.ftc.gov/news-events/news/press-releases/2021/08/ftc-alleges-facebook-resorted-illegal-buy-or-bury-scheme-crush-competition-after-string-failed.

78 Greenwood, Dazza. "Agents Talking to Agents: A2A Reshaping the Marketplace and Your Power." https://www.dazzagreenwood.com/i/164827056/agents-talking-to-agents-a2a-reshaping-the-marketplace-and-your-power.

79 The Model Context Protocol (MCP), developed by Anthropic and now controlled by the Agentic AI Foundation, is a universal open standard for connecting AI applications to external systems. "Donating the Model Context Protocol and Establishing of the Agentic AI Foundation." Anthropic. https://www.anthropic.com/news/donating-the-model-context-protocol-and-establishing-of-the-agentic-ai-foundation.

80 "Justice Department Sues Apple for Monopolizing Smartphone Markets." U.S. Department of Justice. https://www.justice.gov/archives/opa/pr/justice-department-sues-apple-monopolizing-smartphone-markets.

81 Cendan, Felipe. "The Future of AI and the Law." *New York University Law Review* 78, no. 5 (2018): 1234-1256. https://nyulawreview.org/wp-content/uploads/2018/08/NYULawReview-78-5-Cendan.pdf.

82 For example, Android was initially developed as an open source operating system, but Google has over time restricted access to Android source code and limited the functionality of the Android Open Source Project (AOSP). See, e.g., Holwerda, Thom. "Google further guts the Android Open Source Project by deprecating the dialer and messaging apps." June 13, 2023. https://www.osnews.com/story/136235/google-further-guts-the-android-open-source-project-by-deprecating-the-dialer-and-messaging-apps/.

83 "WhatsApp Changes Its Terms to Bar General-Purpose Chatbots from Its Platform." TechCrunch. https://techcrunch.com/2025/10/18/whatsapp-changes-its-terms-to-bar-general-purpose-chatbots-from-its-platform/.

84 "Amazon Sues Perplexity AI Shopping Agents." Retail Dive. https://www.retaildive.com/news/amazon-sues-perplexity-ai-shopping-agents/804871/.

85 Id.

86 "Bullying Is Not Innovation." Perplexity AI. https://www.perplexity.ai/hub/blog/bullying-is-not-innovation.

87 "Technology Behind Amazon's GenAI-Powered Shopping Assistant Rufus." Amazon Science. https://www.amazon.science/blog/the-technology-behind-amazons-genai-powered-shopping-assistant-rufus.

88 Id.

89 Palmer, Annie. "Amazon Wins Court Order to Block Perplexity's AI Shopping Agent." CNBC, March 10, 2026. https://www.cnbc.com/2026/03/10/amazon-wins-court-order-to-block-perplexitys-ai-shopping-agent.html

90 Kulp, Patrick. "Google promises to stop digging through your email inbox to target ads (which it was totally doing)" Mashable. Jne 23, 2017.

91 See, e.g. "How Private Are Popular AI Assistants?" Northbound Advisory. https://www.northboundadvisory.com/blog/how-private-are-popular-ai-assistants; "Anthropic's Claude AI: Updated Terms Explained." AMST Legal. https://amstlegal.com/anthropics-claude-ai-updated-terms-explained/. https://libguides.marian.edu/c.php?g=1321167&p=10738998 "Safeguarding the Enterprise AI Evolution: Best Practices for Agentic AI Workflows." ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2025/safeguarding-the-enterprise-ai-evolution-best-practices-for-agentic-ai-workflows;"AI Agents: RBAC and VertexAI." Sakura Sky. https://www.sakurasky.com/blog/ai-agents-rbac-vertexai/; "Access Control in the Era of AI Agents." Auth0. https://auth0.com/blog/access-control-in-the-era-of-ai-agents/.

92 Because these charts were creating using AI, they are not presented here as hard facts but rather to graphically paint a picture of the differences between surveillance of regular people who use AI tools and of corporate AI clients.

93 "Introducing ChatGPT Enterprise." OpenAI. https://openai.com/index/introducing-chatgpt-enterprise/. "What is the Enterprise Plan." Claude. https://support.claude.com/en/articles/9797531-what-is-the-enterprise-plan; "Amazon Bedrock Security and Privacy." Amazon. https://aws.amazon.com/bedrock/security-compliance/; "Enterprise dat Protection in Microsoft 365, Copilot and Microsoft 365 Copilot Chat." Microsoft. https://learn.microsoft.com/en-us/copilot/microsoft-365/enterprise-data-protection.

94 Id.

95 Frameworks include GDPR, HIPAA, SOC 2, and PCI DSS.

96 Stopping Big Tech from Becoming Big AI: A Roadmap for Using Competition Policy to Keep Artificial Intelligence Open for All, by Max Von Thun and Daniel Hanley, Open Markets Institute. https://www.openmarketsinstitute.org/publications/report-stopping-big-tech-big-ai-roadmap.

97 Id.

98 For example, GliaNet Alliance is developing open and auditable governance and technology for trusted intermediaries. GliaNet Alliance Comments Responding to the UK Department for Science, Innovation & Technology: Shaping Policy for Data Intermediaries. May 12, 2025. At 13. https://www.glianetalliance.org/news/UKcallforevidenceondataintermediaries

99 For a more detailed discussion, see Hubbard, Sally. Monopolies Suck: 7 Ways Big Corporations Rule Your Life and How to Take Back Control. Simon & Schuster. 2020; Lynn, Barry. Liberty From All Masters: The New American Autocracy vs. The Will of the People. St. Martin's Press. 2020.

100 See., e.g., "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook." July 24, 2019, https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook; "1.2 Billion Euro Fine for Facebook." European Data Protection Board. May 22, 2023. https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en; "Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law," FTC. September 2019. https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law.

101 "Each Facebook User is Monitored by Thousands of Companies." Consumer Reports.https://www.consumerreports.org/electronics/privacy/each-facebook-user-is-monitored-by-thousands-of-companies-a5824207467/.

102 See FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individual Consumer Prices, January 17, 2025. https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.

103 See, e.g., "Google's Transparency Report" (showing 127,000 FISA request for user data in the first six months of 2024 alone). https://transparencyreport.google.com/user-data/us-national-security

104 Bragg, Julianna. "Unions Sue Trump over Surveillance and Allege First Amendment Breach." Axios. Oct. 16, 2025, www.axios.com/2025/10/16/trump-surveillance-first-amendment-union-lawsuit.

105 On Facebook's first quarter 2016 earnings call, CEO Mark Zuckerberg announced that users spend on average more than fifty minutes a day using Facebook, Instagram, and Messenger, up ten minutes from the number reported in 2014. James B. Stewart. "Facebook Has 50 Minutes of Your Time Each Day. It Wants More." New York Times. May 5, 2016. https://www.nytimes.com/2016/05/06/business/facebook-bends-the-rules-of-audience-engagement-to-its-advantage.html.

106 Kern, Rebecca, Josh Sisco, and Alfred Ng. "Dozens of States Sue Meta over Addictive Features Harming Kids." POLITICO, 24 Oct. 2023, www.politico.com/news/2023/10/24/states-sue-meta-addictive-features-kids-00123217.

107 Chakradhar, Shraddha. "More Internal Documents Show How Facebook's Algorithm Prioritized Anger and Posts that Triggered It." Washington Post. October 26, 2021. https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/

108 Tobias Rose-Stockwell, "This Is How Your Fear and Outrage Are Being Sold for Profit," Quartz, July 28, 2017, https://qz.com/1039910/how-facebooks-news-feed-algorithm-sells-our-fear-and-outrage-for-profit/, and Marcia Stepanek, "The Algorithms of Fear," Stanford Social Innovation Review, June 14, 2016, https://ssir.org/articles/entry/the_algorithms_of_fear.

109 "Facebook Knows it Encourages Division." Wall Street Journal. https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499.

110 See, e.g., Ron Knox, "The Copyright Killer," Global Competition Review, Jan. 11, 2019, https://globalcompetitionreview.com/insight/gcr-q1-2019/1179029/the-copyright-killer; "How Big Tech Killed Local Media & Over 250,000 Jobs Across the U.S." The Tech Oversight Project. Sep. 2022. https://techoversight.org/wp-content/uploads/2022/09/Big-Tech-Kills-Local-Journalism.pdf; Perotti, Elena, "Paying for News: Google and Meta Owe US Publishers $11.9-13.9 Billion Each Year," World Association of News Publishers, https://wan-ifra.org/2023/11/paying-for-news-google-and-meta-owe-us-publishers-11-9-13-9-billion-each-year/; Jim VandeHei, "Behind the Curtain: How Google Got Media Companies Addicted," Axios, May 8, 2018. https://www.axios.com/google-media-companies-facebook-tech-industry-a10898ee-e0b7-46ef-bcfc- d2561a2e0630.html; Sergei Klebnikov, "Jeff Bezos Gets $6.4 Billion Richer as Amazon Stock Hits a New Record High," Forbes, April 14, 2020, https://www.forbes.com/sites/sergeiklebnikov/2020/04/14/jeff-bezos-gets-63-billion-richer-as-amazon-stock-hits-a-new-record-high/#4fc4bb6e53b0; Verne Kopytoff, "How Amazon Crushed the Union Movement," Time, Jan. 16, 2014, https://time.com/956/how-amazon-crushed-the-union-movement/; Chris Stokel-Walker, Karen Weise, "Prime Power: How Amazon Squeezes the Businesses Behind Its Store," New York Times, Dec. 19, 2019. https://www.nytimes.com/2019/12/19/technology/amazon-sellers.html. "'Success' on YouTube Still Means a Life of Poverty," Bloomberg, Feb. 26, 2018, https://www.bloomberg.com/news/articles/2018-02-27/-success-on-youtube-still-means-a-life-of-poverty.

111 "Joe Toscano," Tedx Lincoln, https://www.tedxlincoln.com/speakers/2019/joe-toscano.html.

112 Gemini API Additional Terms of Service" Last Accessed December 2025. https://ai.google.dev/gemini-api/terms

113 Radsch, Courtney C. "AI Needs Us More Than We Need It." Washington Monthly. October 29, 2024. https://washingtonmonthly.com/2024/10/29/ai-needs-us-more-than-we-need-it/.

OPEN MARKETS INSTITUTE