

# FROM DISRUPTION TO REGULATION:

Towards Accountable Big Tech and  
AI in the Digital Age

**JANE S. HOFFMAN & IRUM J. MALIK**



HARVARD Kennedy School

**MOSSAVAR-RAHMANI CENTER**

for Business and Government

*CORPORATE RESPONSIBILITY INITIATIVE*

# **From Disruption to Regulation: Towards Accountable Big Tech and AI in the Digital Age**

**Jane S. Hoffman & Irum J. Malik**

## **Introduction**

Digital technology companies have significantly contributed to the common good while simultaneously disrupting many sectors of society. Big Tech comprised notably of the five most dominant information technology firms – Meta (Facebook), Apple, Amazon, Alphabet (Google), and Microsoft – make up the largest industry in the world with a current combined market capitalization of \$6.5 trillion (Laricchia, 2023). Their devices and services have made digital tech ubiquitous in global society, in which four billion people, roughly half the world’s population, own a smartphone (Business Wire, 2021) and 92% of Americans use the Internet (Petrosyan, 2023). In response to the outsized power and influence of Big Tech on consumers, democratic norms, industry competition, and the global economy, the European Union has been at the forefront of imposing regulations on the industry, namely the 2022 Digital Services Act and Digital Market Act (European Commission, 2023) and 2018 General Data Protection Regulation (GDPR; Burgess, 2020). In the United States, however, despite dozens of bills proposed in U.S. Congress over the past two-and-a-half decades, only one privacy law is currently in place in contrast to the sweeping laws directed at many aspects of the digital technology industry enacted by the EU. The United States government's 2023 Executive Order (EO) on AI released by the White House during the Biden-Harris administration represents a key step toward ensuring a safe, secure, and ethical development of AI technology. The EO directs federal agencies to focus on key areas, including managing dual-use AI models, implementing rigorous testing protocols

for high-risk systems, enforcing accountability, safeguarding civil rights, and promoting transparency throughout the AI lifecycle. (Brookings Institution, 2024)

In spite of this, concerns continue to persist about the EO's ability to address the monopolistic power of tech giants. The tech giants, who control much of the AI infrastructure, cannot be relied upon to self-regulate, as it has been observed that voluntary commitments from the end of tech giants are hard to achieve. In October 2024, building on the 2023 EO, the Biden-Harris administration issued a National Security Memorandum (NSM) titled "Advancing the United States' Leadership in Artificial Intelligence; Harnessing AI for National Security Objectives; and Ensuring the Safety, Security, and Trustworthiness of AI." This memorandum provides further guidance, including a timeline and clarity on the responsible federal agencies, outlining the next steps for appropriately integrating AI models and technologies into U.S. government operations, particularly within national security systems (NSS). It emphasizes the need to protect human rights, civil rights, civil liberties, privacy, and safety in AI-enabled national security activities. (The White House, 2024 – Article removed since Jan'25)

While the steps taken by the Biden-Harris administration mark a significant milestone in shaping U.S. AI policy, the future remains uncertain, especially with the unpredictability surrounding how these initiatives will evolve under the Trump administration. One of President Trump's first actions upon taking office in 2025 was to revoke a 2023 executive order signed by Former President Joe Biden, which aimed to mitigate the risks that artificial intelligence poses to consumers, workers, and national security citing reasons related to preventing any hindrances towards "AI innovation." (Reuters, 2025).

Another action undertaken recently has been the disbandment of the Consumer Financial Protection Bureau's (CFPB) technical team, and the mass layoffs represent a defining moment in

the regulation of new technologies in the financial sector. The future of the CFPB has come under intense scrutiny since the Trump administration announced plans in April 2025 to lay off nearly 1,500 of the agency's 1,700 employees – an 88% reduction in staff – signaling a dramatic retreat from regulatory enforcement. Soon after, a federal district court issued an injunction blocking the administration from proceeding, citing concerns that the move would render the agency unable to fulfill its statutory duties. As litigation advanced, a federal appeals panel began considering whether to pause the lower court's order, hinting at a possible compromise that might allow a scaled-back version of the CFPB to continue operating (Politico, 2025; The Hill, 2025). Most recently, the Trump administration filed an emergency petition with the U.S. Supreme Court, asking it to lift the injunction and permit the layoffs – arguing executive authority over agency staffing. The Supreme Court has asked the plaintiffs to respond by June 9, 2025, and its forthcoming decision is expected to significantly shape the CFPB's future structure and role (CBS News, 2025).

Established in response to the 2008 financial crisis, the CFPB took on the crucial responsibility of safeguarding consumers, especially as digital solutions became more integrated into financial products. However, the recent job cuts, including the elimination of the technical team, have raised concerns about the adequacy of consumer protection in the evolving digital age. This team was essential for addressing the complexities of artificial intelligence, algorithmic tools, and "dark patterns" – misleading design techniques intended to steer consumers toward decisions they would otherwise avoid. The removal of these experts has amplified worries about big tech firms and financial institutions operating with less oversight.

Specialists argue that without a regulatory body equipped to understand the intricate technologies behind modern financial products, consumers are at greater risk of being exploited.

As tech giants like Meta, Google, and Apple expand their reach into the financial services market, the need for rigorous regulation has never been more urgent. The CFPB had already taken significant steps, including launching investigations into Meta’s use of consumer data and issuing fines to firms such as Apple over unfair practices. Without the expertise of technologists to scrutinize the algorithms and user interfaces driving these products, there is an increased likelihood that consumers will be misled or harmed by automated decisions they don’t fully comprehend.

The lack of comprehensive privacy laws in the United States exacerbates this risk. In the absence of legislation that holds companies accountable, the exploitation of personal data is likely to continue, with long-term consequences for American consumers. As AI and algorithms increasingly shape financial decisions—ranging from mortgage approvals to student loan repayments—the need for regulatory frameworks that ensure ethical and transparent use becomes even more critical. Technological innovation should drive economic growth, but it must be balanced with regulations that protect consumers and maintain trust in the financial system. (Thomson Reuters Foundation, 2025)

There is significant uncertainty about the direction U.S. AI policy will take, leaving questions about how these competing visions will shape the future of AI development, regulation, and its broader societal impact.

The urgency for regulating these companies has intensified especially at a time when Big Tech surges toward expanding its AI product portfolio (Constantz, 2023; Robertson, 2023) that will increase its pervasive impact on users’ lives and deepen its monopoly position in the digital economy. This paper proposes that Big Tech’s enormously outsized societal and economic impact requires a more rigorous framework for addressing its activity than enacting laws alone. The proposed oversight model consists of a new federal agency, the Consumer Technology

Protection Agency, and presidential cabinet position, the Secretary of Technology, dedicated to technology-industry oversight and advisory capacity in the executive branch. Information technology firms' unprecedented reach into daily life and dominance in the market, which results in a wide-ranging spectrum of harms from the individual to democratic-system level, creates the need to equivalently recalibrate how they are regulated. In mid-2024, a major cybersecurity failure occurred when CrowdStrike, a prominent cybersecurity company, released a faulty security update. This flawed update triggered a widespread IT outage that began in Australia and rapidly spread worldwide due to CrowdStrike's integration with Microsoft's systems—widely used across both public and private sectors. The incident caused massive disruptions, including widespread “blue screens of death,” grounded flights, frozen banking systems, and halted medical operations. This event starkly revealed how deeply intertwined Big Tech companies are in critical infrastructure and everyday life, showing that a single technical glitch in a dominant platform can cascade into global chaos. (Alegre, 2024)

This paper will address Big Tech's benefits and the harms that call for a new approach to regulation, the role and status of corporate citizenship in the industry, suggested regulatory methods from various fields as well as other countries, and a framework for a model proposed for industry oversight.

### **The Deep Integration of Big Tech**

In today's world, Big Tech giants and their product ecosystems have become deeply embedded in nearly every aspect of our daily lives. The scale of this integration is staggering. For example, in 2024, Meta reported that 3.29 billion people used at least one of its core products daily—nearly half the world's population (Statista, 2024). Similarly, Apple has revealed that approximately one billion people actively use more than 1.8 billion Apple devices globally, with its brick-and-mortar stores welcoming over a million visitors daily (Warren, 2022). Amazon,

another major player, captures 92% of online shoppers worldwide (NPR/Marist Poll, 2018), while Google processes an astonishing 8.5 billion searches every day (seo.ai, n.d.). These figures highlight the pervasive influence of Big Tech giants across industries and geographies, shaping the daily lives of billions.

The breadth of the offerings by these Big Tech players further amplifies this dominance. Meta's platforms, such as Facebook, Instagram, and WhatsApp, connect people, shape communication, and drive content consumption. Apple's ecosystem spans hardware like iPhones and MacBooks, software like iOS, and services like iCloud and Apple Pay, creating an integrated user experience. Amazon dominates e-commerce while expanding into cloud computing, streaming, and AI-driven solutions. Google extends its reach through search, advertising, Android, YouTube, and cloud technologies, while Microsoft's enterprise tools, including Microsoft 365 and AI solutions like Copilot, are rapidly becoming indispensable for businesses, with nearly 70% of Fortune 500 companies adopting them (Microsoft News, 2024)

While these innovations provide convenience and efficiency, such unparalleled integration also consolidates immense power in the hands of a few corporations. This concentration of influence poses significant risks to society, as the unchecked dominance of Big Tech can lead to monopolistic behavior, erosion of privacy, manipulation of information, and other harmful consequences. Through this paper, we aim to demonstrate that such unregulated power in the hands of a select few is not only a threat to competition but also to democratic values and societal well-being. The repercussions of this imbalance are already visible and could grow increasingly severe without proper checks and governance.

### **Big Tech's Advances and Societal Harms**

Big Tech has digitized the way individuals communicate, access information, make purchases, interact with medical providers, read books and news media, view films and

television, navigate travel, and efficiently use home utilities and appliances through the Internet of Things (IoT). Defining features of the COVID-19 era included online education and working from home, the latter resulting in a shift in which, by January 2023, 13% of full-time employees worked from home compared to 6% pre-pandemic and 28% worked in hybrid home/in-office situations (Barrero et al., 2023; Coate, 2021). On a larger scale, digital technology advances opportunities for underrepresented groups to utilize digital tools such as mobile banking and other Fintech services, thus expanding entrepreneurial activity that benefits economies. In the Middle East and North Africa (MENA) region, for example, where only 35% of women have bank accounts compared to 52% of men, Fintech is helping narrow the financial-industry-access gender gap (Gueguen et al., 2020). Also on the societal level, digital tech provides transparency about events in areas of the world where international media is minimal or banned, such as Iran, where real-time video of massive public protests in 2009 and 2022-23 (Agence France Presse, 2009; Burgess, 2022) exposed state security forces' fatal crackdowns on people exercising their human rights.

These valuable individual and societal contributions, in addition to benefits reported in Big Tech Corporate Responsibility (CR) programs and Environmental Social Governance (ESG) measurements, exist alongside the industry's detrimental impact on users and society. Trittin-Ulbrich et al. (2021) observed that a growing number of studies on the processes used by tech companies marks the industry as "inherently problematic" (p. 14). When the dominating industry in the world is assessed in this way, it is critical for regulation to catch up with its fast-paced advances rather than continue to fall behind and allow the companies to exacerbate their harms. Technology firms' negative effects involve issues of privacy (Hoffman, 2022; Shamsi and Khojaye, 2018; Greenwald, 2015; Stergiou, 2023; Zuboff, 2020), behavioral modification and lack of personal agency (Ienca & Vayena, 2018; Susser et al., 2019; Zuboff, 2019), mental health

(Boar et al., 2020; Elhai, 2017; Karim et al., 2020; Prinstein, 2023; Coyne et al., 2020), discrimination (Nahmias & Perel, 2021; Barocas & Selbst, 2016; Favaretto et al., 2019), and undermining democracy (Fukuyama et al., 2020; Haidt, 2022; Stoller, 2019; Zuboff, 2021). Each of these concerns is addressed in the following sections.

## **Privacy**

The advertising-based business model of most digital technology companies has aptly named the digital era the *attention economy*. This reflects the business model in which algorithms prioritize content that compels Internet users to stay online, thus exposed to advertising, as long as possible.

Tech companies sell advertising that offers targeted precision to potential customers based on millions of data points the companies harvest when users are online. For example, free services from Google and its acquired company YouTube and from Facebook and its companies Instagram and WhatsApp earn their revenue by mining personal data of their users through sophisticated tracking methods and selling that data to advertisers. The mining of user data at the core of this model produces never-before-encountered challenges to privacy rights. The fact that companies like Google, the largest online advertiser in the world (Konstantinovic, 2023), and other tech companies that combined dominate much of human interaction and the global economy run on raw data gathered freely from their users constitutes a privacy crisis. Gillmor and Stanley (2023) explained that privacy issues on cellphones/smartphones result from only two companies controlling the operating system software on which these “pocket computers” run:

The most common operating system, Android, is controlled by an advertising company (Google) and is notorious for leaking information about its users. Apple, which controls iOS . . . is also becoming increasingly interested in monetizing its customers' data and lacks adequate controls to prevent rogue apps from many forms of spying. The result is that a lot of the activity we engage in on our phones is tracked. (para. 2)

As the public becomes increasingly aware of these tracking processes, tech companies have been forced to address their concerns. In the wake of multiple lawsuits, tech companies' efforts to adhere to federal and state privacy laws have made it easier for users to opt out of some tracking processes, but critical concerns remain. In their privacy policies, companies admit to collecting a user's name, gender, birthday, phone number, email address, location, relationship status, work, income level, education, race/ethnicity, religious views, home address, political views, credit cards, phone calls, calendar events, search history, videos watched, uploaded photos, purchase history, fitness/health data, posted likes, voice and facial recognition data, Wi-fi and Bluetooth information, and more (Moscaritolo, 2022). No age group has been immune from this process. Big Tech's mining of children's data prompted the Children's Online Privacy Protection Act of 1998 (COPPA), which protects the privacy of children under the age of 13 by requesting parental consent.

The advent of LLMs and their associated chatbots poses new challenges for privacy. Many unanswered questions remain: Is our personal information part of a model's training data? Are our prompts being shared with law enforcement? Will chatbots connect diverse threads from our online lives and output them to anyone?

AI systems amplify privacy risks that have long existed in the internet era. The difference now is scale – AI's insatiable demand for data and lack of transparency make it even harder to

control what information is collected, how it is used, and whether it can be corrected or removed. Avoiding digital surveillance in daily life is nearly impossible, and AI threatens to exacerbate this problem. (Stanford University Institute for Human-Centered Artificial Intelligence, 2024)

Generative AI tools trained on scraped data may memorize personal and relational information, enabling targeted identity theft and fraud. Bad actors already use AI voice cloning for extortion. Data shared for one purpose – like a resume or photograph – is often repurposed to train AI systems without consent, raising civil rights concerns. Predictive AI tools used in hiring decisions have been biased, as seen in Amazon’s failed AI hiring tool, which discriminated against female candidates. (The Guardian, 2018).

Building AI so that it respects data privacy is complicated by how generative AI systems work. “Up until this point, tech companies have not done what they’re doing now with generative AI, which is to take everyone’s information and feed it into a product that can then contribute to people’s professional obsolescence and totally decimate their privacy in ways previously unimaginable,” said Ryan Clarkson, whose law firm has filed class action lawsuits against OpenAI, Microsoft, and Google. (Morrison, 2023)

In the U.S., the debate on data permissions for AI training has largely centered on copyright, as federal consumer privacy laws remain absent. Copyright law has been used by creators to demand removal of their data from training datasets, but this approach is flawed due to the lack of transparency from AI companies. In July 2023, the Federal Trade Commission (FTC) issued a civil investigative demand to OpenAI for details about its training data. The FTC has previously settled cases requiring companies to delete AI models and improperly acquired training data. Former FTC Chair Lina Khan emphasized that "exploitative collection or use of personal data" falls within the agency’s mandate to prevent unfair trade practices (The Washington Post, 2023)

The global expansion of AI is driving an insatiable demand for data, pressuring the existing data ecosystem to collect more consumer information while undermining data minimization principles. AI's dependence on data extends beyond the internet to physical spaces through embedded sensors, smart appliances, and biometric cameras. The primary question we raise is whether existing data protection principles are sufficient for tackling the privacy risks and harms posed by AI.

Privacy issues intersect with other harms wrought by digital technology companies. As the Electronic Privacy Information Center (2023) advocacy group stated, privacy is a fundamental right that requires “protection from abusive data practices like mass surveillance, browser tracking, demographic profiling, and data discrimination” and that protecting online privacy means “preserving our digital autonomy, individual freedom, and democratic values” (para. 4).

Privacy protection also carries the responsibility of addressing the mental health issues associated with the addictive nature and other psychological aspects of using digital technology.

### **Mental Health**

The attention economy's dependency on keeping users' eyes on their screens underlies the purposely addictive nature of online experiences. Tech addiction, or problematic use, is the result of neurological reward loops that, in the case of Facebook, former Facebook president Sean Parker said were conscientiously installed in its processes to keep users on the platform. Company inventors understood that the social validation loop produced by giving users “a little dopamine hit every once in a while, because someone liked or commented on a photo or a post or whatever” exploited users' psychological vulnerabilities, but “we did it anyway” (Pandey, 2017).

Mental health studies on information technology report that problematic use of digital tech leads to depression, anxiety, chronic stress and/or low self-esteem (Elhai et al., 2017). Problematic use of technology in children is particularly concerning because of its effects during critical periods of neural development. In testimony before the U.S. Senate Committee on the Judiciary, American Psychological Association President Mitch J. Prinstein (2023) explained that starting at the ages of 10 to 12 years old, regions in the brain “associated with our craving for ‘social rewards,’ such as visibility, attention, and positive feedback from peers” (p. 6) begin to develop. However, regions that enable individuals to resist temptations and inhibit behavior do not fully develop until 10 to 15 years later in early adulthood. This is why children are easily prone to addictive behavior and are vulnerable to the problems that social media promotes, for example, comparing themselves to others. This activity “is associated with lower self-image and distorted body perceptions” and “creates strong risk factors for eating disorders . . . and depression” (Prinstein, 2023, p. 14).

In addition to physiological harms, digital technology is responsible for discriminatory actions impacting specific groups.

### **Discriminatory Processes**

The data that goes into algorithms to run digital systems can be sourced from biased information that in return produces biased results. An algorithm is “a formally specified sequence of logical operations that provides step-by-step instructions for computers to act on data and thus automate decisions” (Barocas et al., 2014). In artificial intelligence systems, algorithms are designed for machine learning, the ability to learn and evolve on their own. Algorithms are only as good as the data they are built upon, and digital services and software have been found to produce biased results regarding peoples’ race, gender, religion, age, income level, sexual orientation, national origin, and other characteristics. This biased information can

result in discriminatory action that unfairly disadvantages specific groups. Bias has been found in the photo editing app FaceApp, for example, which automatically “enhances” pictures of faces by lightening skin tones based on the predominance of White faces in the algorithm data. The algorithm established light skin as the standard of beauty (Lee, 2018). In medicine, algorithms in software designed to detect melanomas may not contain enough images of what skin disease looks like in darker skin, so it cannot detect melanoma in people of color with the accuracy it can detect disease in light skin (Adamson & Smith, 2018).

Policing tools that predict where certain types of crime are likely to occur have been found to be based on biased police officer data about “who to stop, search, and arrest” that results in overpolicing in low-income neighborhoods of color, even when certain crimes are more evenly spread across a city (Southerland, 2021, p. 502; Verma, 2022). This contributes to the overrepresentation of people of color in the criminal justice system. Relatedly, an investigation into a software frequently used to assess the probability of recidivism was “twice as likely to mistakenly flag black defendants as being at a higher risk of committing future crimes” and “twice as likely to incorrectly flag white defendants as low risk” (Crawford, 2016). These serious problems reveal how digital technology, meant to make institutional systems more efficient, further entrenches institutionalized racism.

Research has also documented gender bias in algorithmic processes (Vlasceanu & Amodio, 2022; Hutson, 2017; Buolamwini, 2019; Hadhazy, 2017), including a study of Google ads that revealed that male users were shown substantially more high-paying job ads than women (Spice, 2015). Two factors account for these biases: the lack of gender and racial diversity in digital tech workplaces and “the social norms and practices that prevail in a society” (Waelen & Wiczorek, 2022, p. 52). These norms of bias are reflected in the data that algorithms use.

Discriminatory actions based on the use of digital technology have also occurred in large-scale organizations. Government agencies throughout the world adapt automated programs to deliver their services more efficiently, but a lack of standard rules and human checks and balances put populations at risk. The most catastrophic example took place in the Netherlands, where in 2013 machine learning algorithms began creating risk profiles to uncover childcare benefits fraud. The algorithms gathered risk indicators in benefit applications such as “foreign sounding names” and “dual nationality,” resulting in algorithms adapting over time to create a “discriminatory loop with non-Dutch nationals flagged as potentially committing fraud more frequently than those with Dutch nationality” (Koning, 2021, para. 9; Felton, 2022). The AI system, run by the Dutch tax authorities for six years, wrongly accused thousands of parents of fraud and billed them for years of past benefit payments, resulting in bankruptcies, poverty, suicides, and 1,000 children moved into foster care (BBC News, 2021; Heikkilä, 2022). The actions of the unregulated AI system caused wide scale public distrust in the authorities, and the government resigned.

In April 2024, federal agencies, including the Equal Employment Opportunity Commission and Department of Labor issued a joint statement and emphasized the need to enforce civil rights and consumer protection laws in AI systems, warning of potential discrimination. In comparison, better efforts have been pulled off at the state and local level on this front. On a state level, new regulations like Illinois' AI Video Interview Act and Colorado's AI Consumer Protection Act aim to address bias in AI-driven employment decisions. Local laws like New York City's AEDT Law require bias audits and transparency from employers. Other states are also considering similar legislation to regulate AI's impact on employment and consumer rights (U.S. Department of Labor, 2024; Illinois General Assembly, 2024.; New York City Department of Consumer and Worker Protection, 2024)

As these examples show, the ability of AI to create group-based harms through popular mobile apps, free online services, and government organizations from policing to social benefits creates a societal problem that “is now so formidable that it cannot be ethically defensible to fail to address it” (Anderson et al., 2022, p. 6). While efforts at the state and local level are a step forward, much more remains to be done to ensure effective oversight and regulation, especially given the evolving scope and complexity of these technologies. Equally concerning is digital technology’s ability to manipulate behavior, resulting in the loss of personal autonomy.

### **Behavioral Modification**

In the attention economy, online advertising automatically delivered to digital tech users based on the raw data mined from them by multiple sources is the product of hidden algorithmic processes. Zuboff (2019) refers to the system in which this business model now dominates society and economies *surveillance capitalism*. Not only are online users unaware of the data being collected at any given second, but they are also incognizant of how the content they see is created specifically for them for the purpose of nudging their behavior. This process was exposed to the wider public in 2018 when the British political consulting firm Cambridge Analytica gathered Facebook user data without user consent to create psychological profiles sold to clients including the Donald J. Trump presidential campaign. Political ads could be precisely messaged, for example, to suppress the voting intentions of specific types of Democrat Facebook users: “A neurotic, extroverted and agreeable Democrat could be targeted with a radically different message than an emotionally stable, introverted, intellectual one” (Hern, 2018).

Prior to the Cambridge Analytical scandal, a scientific journal published a study conducted by Facebook and Cornell University that revealed the social media network’s ability “to make people happier or sadder on a massive scale and without their awareness—a phenomenon that was labeled ‘emotional contagion’” (Ienca & Vayena, 2018, para. 2). Susser et

al. (2019) defined this manipulative activity as “the use of information technology to covertly influence another person’s decision-making, by targeting and exploiting decision-making vulnerabilities” (p. 6). They also warned that “when information about us is used to influence our decision-making, it does more than diminish our interests—it threatens our autonomy” (p. 3). Zuboff (2019) described Big Tech’s covert influence as a “direct assault on human agency and individual sovereignty,” the consequence of “a global means of behavioral monitoring and modification in the service of [surveillance capitalism’s] commercial objectives” (para. 30).

This form of behavioral modification is not limited to politics or emotional manipulation – its logic now permeates digital consumer experiences, where generative AI and algorithmic systems increasingly optimize for persuasion, often at the cost of user autonomy. Generative AI has significantly enhanced marketing capabilities, allowing for hyper-targeted personalization at an unprecedented scale. However, this advancement has also brought ethical concerns, particularly regarding the amplification of dark patterns – manipulative tactics that exploit user behavior for corporate profit (Forbes, 2024). Research shows that many SaaS companies deploy dark patterns, such as hidden subscription renewals that are difficult for users to cancel. As AI becomes more sophisticated, it can replicate and magnify these manipulative tactics, further compromising consumer autonomy (Legal Dive, 2024).

By leveraging vast consumer data, AI systems can subtly steer user decisions, such as turning passive browsing into purchasing actions without the user’s full awareness. While platforms like Spotify use algorithms to enhance user experience with personalized playlists, similar technologies can also manipulate decision-making in ways that benefit companies more than consumers (Hermann & Puntoni, 2024; Banker & Khetani, 2019). These tactics undermine consumers' ability to make informed choices.

As AI transitions from analyzing single data types to integrating multimodal data (e.g., text, audio, images), it refines its marketing strategies even further (Cao et al., 2023; Fei et al., 2022). This vast increase in scale and personalization deepens the ethical challenges posed by AI. As Forbes (2024) highlights, generative AI has the potential to "supercharge dark patterns" by amplifying manipulative tactics, often unknowingly. While AI offers efficiencies and enhanced experiences, it also demands regulatory oversight to prevent exploitation and protect consumers.

The harms of this integral aspect of Big Tech, together with misinformation and other damaging content hosted by Facebook, YouTube, Twitter, and other platforms, lead to the wider harm of weakening democracy.

### **Undermining Democracy**

Changes in news access, the prevalence of behavioral modification in online experiences, and polarization due to social media use are significant areas in which Big Tech is negatively impacting democracy. The shift of the majority of newspaper advertising revenue that allowed the industry to flourish for hundreds of years to Big Tech companies is a far-reaching harm to society. The fundamental role of the press in a democracy is enshrined in the First Amendment and compelled the government to establish the Post Office Department one year after the founders introduced the Bill of Rights. The postal service was conceived as essentially "the distribution arm of American newspapers," according to media scholar Robert McChesney (Steiner, 2022). The government subsidized the proliferation of the media of the day to provide the public with the information they needed to participate in governance as informed citizens. The decline in newspapers since the conglomeration of media companies beginning in the 1980s (McChesney, 2015) and the loss of advertising revenue in the shift from print to digital media in

the 2000s made a stark impact. Weekday circulation of U.S. daily newspapers dropped from 55.8 million in 2000 to 24.2 million in 2020 (Grundy, 2022). Newspaper publishing revenue dropped by more than half between 2002 and 2020 (Grundy, 2022) while newspaper employment fell 70 percent (Abernathy, 2022).

Of special concern is the loss of local newspapers, which are vital to democratic engagement at the grassroots level. The resulting news desert leaves one-fifth of the U.S. population with no access to local news, a situation that corresponds with lower voter participation, increased government and business corruption, and higher taxes and local prices (Abernathy, 2022; Rubado & Jennings, 2019). Overall, the decreased ability for traditional newspapers to adequately fund investigative journalism and news has led some economists to urge lawmakers to look at competition issues in advertising from a “citizen welfare” position (Srinivasan, 2020, p. 65). Advertising revenue that formerly supported professional newsrooms “is now captured by Big Tech intermediaries, and some of that money now goes to dishonest, low-quality and fraudulent content” (Stoller, 2019, para. 3). Returning to the harm of psychological manipulation, Zuboff (2019) contended that the behavioral modification underlying the ad-based attention economy “erodes democracy from within because, without autonomy in action and in thought, we have little capacity for the moral judgment and critical thinking necessary for a democratic society” (para. 18).

While more than eight in ten Americans now access their news online, the majority of them turn to news websites or apps instead of social media news feeds (Shearer, 2021). The eleven percent of adults who prefer social media for news, however, are subject to the algorithmic process that presents content based on users’ emotional responses rather than news relevance or quality. As witnessed during the COVID-19 era and the attack on the U.S. Capitol on January 6, 2021, false and misleading online content undermines public trust in government

information and mainstream journalism and adversely affects democratic processes. “Social media manipulation campaigns have been carried out in 48 countries with a powerful effect to subvert elections and undermine trust in democratic institutions” (Coghlan et al., 2021, p. 6).

Polarization on political issues has also increased in the digital age. “Toxic polarization,” a declining “respect for counterarguments and associated aspects of the deliberative component of democracy,” is an element in the documented global trend in weakening democracies (Boese et al., 2022, p. 6). Further studies tying social media behavior to the state of democracies may bring us closer to establishing a causal relationship between the two. For example, researchers at New York University and Stanford University (Allcott et al., 2020) found that Facebook users who deactivated their Facebook accounts for four weeks became significantly less polarized on political issues.

During the COVID-19 pandemic, algorithmic-perpetuated misinformation had a deadly impact, according to medical researchers who referred to this “fake news” issue as the *COVID-19 infodemic*. “COVID-19 misinformation and disinformation on social media increases vaccine hesitancy, lowers vaccination rates, and causes preventable deaths, especially among certain demographic populations” (Gisoni et al., 2022, para. 4).

With trusted news sources in decline, online experiences shaped by manipulation, and polarization deepening by the day, democracy is already under immense strain. The rise of generative AI adds a new layer of complexity – one that doesn’t just accelerate the spread of misinformation but transforms it. These tools can produce persuasive, personalized, and entirely fabricated content at unprecedented speed and scale. As the 2024 election cycle made clear, we’re no longer just consuming information – we’re navigating an information environment that can be engineered to mislead.

Since 2022, more than 15 billion images have been created using text-to-image algorithms, and with the launch of OpenAI’s DALL-E 2—an AI system that can create realistic images and art from a description in natural language—people are generating an average of 34 million images per day (EveryPixel Journal, 2024). The 2024 election cycle was a great reflection of how generative AI has emerged as a potent tool for mass information generation, with far-reaching consequences for democratic governance. Misinformation and disinformation—already a major challenge in the digital era—were amplified by AI-generated content, making it increasingly difficult for voters, policymakers, and institutions to discern truth from fabrication. According to ABC News (2024), the World Economic Forum warned that “misinformation and disinformation is the most severe short-term risk the world faces” and that “AI is amplifying manipulated and distorted information that could destabilize societies.”

One of the most concerning developments was the rise of AI-generated deepfakes and fabricated narratives designed to manipulate voter perception. On Election Day, a viral AI-generated fake news post falsely claimed that shootings had occurred at polling places in Arizona and that election officials had rescheduled voting for November 6 (ABC News, 2024). Similarly, in January, an AI-generated robocall impersonating President Joe Biden urged New Hampshire Democrats not to vote in the primary—an incident so egregious that the Federal Communications Commission imposed a \$6 million fine on the political consultant responsible. (CNN, 2024)

In September, Taylor Swift had to take to Instagram to refute an AI-generated deepfake image falsely showing her endorsing Donald Trump, instead publicly declaring her support for Vice President Kamala Harris. Such instances illustrate a grim reality: AI-powered

misinformation is not just a theoretical risk – it is already shaping political narratives and influencing voter behavior. (NBC News, 2024)

Beyond individual cases, foreign adversaries have seized upon generative AI as a vehicle for disinformation. OpenAI revealed that it had shut down an Iranian operation attempting to manipulate U.S. voter opinion using its tools. The U.S. Justice Department has similarly reported that Russia is leveraging AI to spread political disinformation on social media platforms, exacerbating polarization and distorting public discourse. The effects of such interference are not confined to the United States. In Britain, deepfake audio clips of Prime Minister Keir Starmer spread widely before being debunked. In Slovakia, opposition leader Michal Šimečka was targeted by similar tactics. In Turkey, AI-generated explicit videos forced a presidential candidate to withdraw from the 2023 election. And in Argentina’s October 2023 presidential race, both leading candidates weaponized deepfakes to mock their opponents, escalating into what has been described as “AI memetic warfare.” (Carnegie, Europe, 2024)

While governments scramble to respond, Big Tech has thus far demonstrated an inability – or unwillingness – to curb the problem effectively. Generative AI models, including ChatGPT, Gemini, and Grok, have been found to replicate and even amplify harmful misinformation when prompted. A study by NewsGuard showed that these chatbots frequently fail to recognize disinformation sources and inadvertently reinforce Russian propaganda narratives. Without intervention, AI’s ability to mass-produce persuasive, misleading content will only strengthen the ability of authoritarian regimes and bad-faith actors to manipulate democratic societies. (NewsGuard, 2024)

AI’s threat to democracy extends beyond election interference. It also risks distorting the way policymakers understand their constituents’ concerns. Public opinion has long been a

critical input in democratic governance. As Robert Dahl argued in 1972, democracy requires “the continued responsiveness of the government to the preferences of its citizens.” For elected officials to be responsive, however, they must first accurately discern those preferences. Written correspondence, emails, and advocacy letters have traditionally served as crucial tools for citizens to communicate their concerns to their representatives.

Yet, in the era of generative AI, these signals can be manipulated at scale. A 2020 field experiment in the United States tested whether legislators could distinguish between AI-generated and human-written advocacy emails. Researchers sent 35,000 emails to 7,200 state legislators, covering six different policy issues. On three issues, response rates to AI-generated and human-written messages were statistically indistinguishable. On the remaining three, the AI-generated emails received only 2% fewer responses on average. These findings suggest that malicious actors could flood legislators with AI-generated messages that appear to reflect genuine constituent concerns – skewing perceptions of public opinion and potentially influencing policy decisions (Journal of Democracy, 2024)

Moreover, generative AI threatens to undermine the public-comment process, a cornerstone of democratic governance through which citizens provide input on regulatory decisions. Agencies responsible for crafting rules on issues ranging from environmental protections to financial regulations already struggle to process large volumes of public feedback. With AI, special interest groups can generate thousands of unique, well-articulated public comments tailored to favor their preferred outcomes, drowning out genuine civic engagement. This could tilt regulatory decisions in favor of corporate or partisan interests rather than reflecting the will of the broader public.

This overview of Big Tech’s prominent harms to individuals and society illustrates the industries’ failure to consider the well-being of digital technology users, the society in which they live, and the democratic system in which they participate. The tech companies that have become powerful forces in everyday life and the global economy due to their free access to user data now address several aspects of corporate citizenship, but these programs are voluntary and do not address fundamental issues of tech addiction, psychological and physiological impacts, monopolization, societal divisiveness and polarization, or dwindling access to local news and investigative journalism. Digital tech companies’ self-designed corporate citizenship efforts, described in the next section, are not adequate to resolving the range of the industry’s harms.

### **Assessing Big Tech Citizenship**

Expectations of corporate responsibility (CR), or corporate social responsibility (CSR), compel Big Tech companies to proactively contribute to the interests of a broad range of stakeholders to benefit society and the planet. Corporate responsibility defines how a company manages its core business activities and relationships, revealing how it is accountable as a sustainable business. Corporate responsibility has become integral to brand identity for employees, consumers, and investors who gauge a business’s sustainability on its carbon footprint, fair and equitable labor practices, philanthropy, and other CR approaches. Since assessing corporate responsibility involves qualitative information and CR programs are a complex mix that typically appear across multiple departments in a company, measuring CR impacts is difficult (O’Neill, 2022).

Environmental, Social, and Governance (ESG) performance indicators provide quantitative measurement that allows investors and other stakeholders to assess a company’s achievements in these areas. Environmental data can include carbon emissions, pollution, and energy efficiency; social factors, which will reflect company CR policies, may address diversity, health and safety, and supply chain labor standards; and the integrity of governance can be

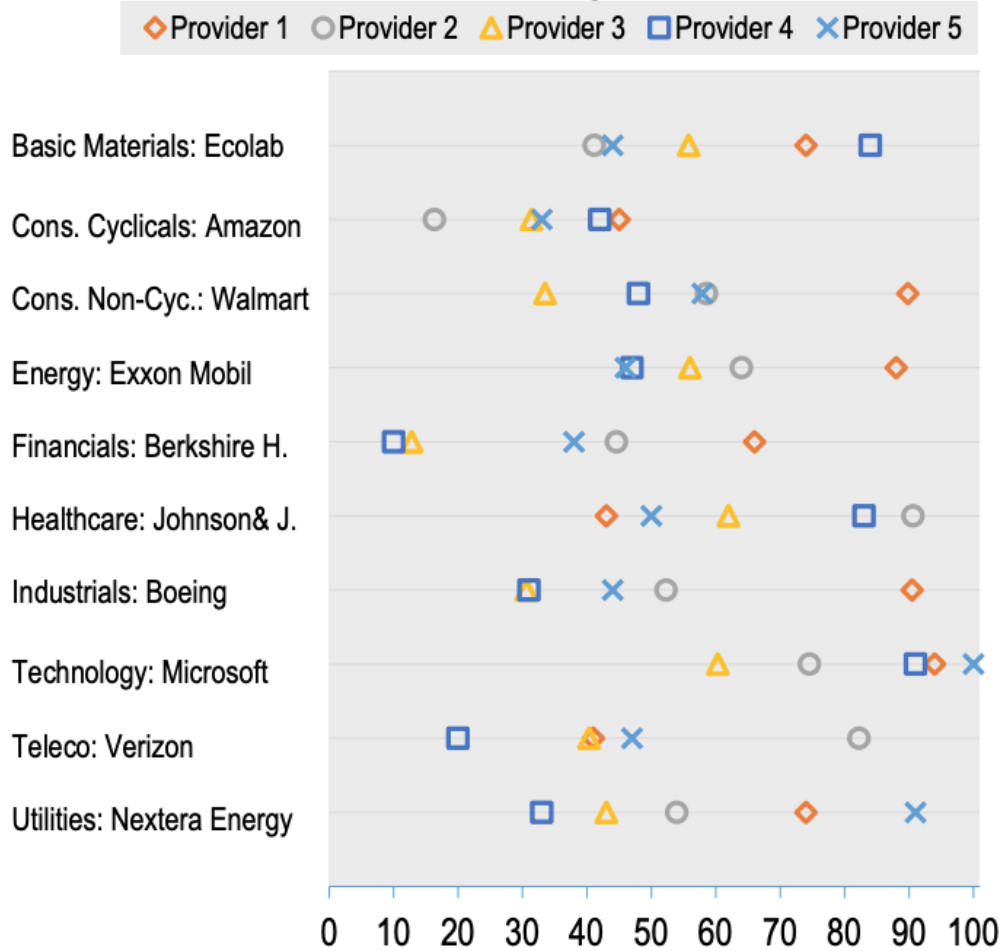
measured by financial and compliance practices, executive compensation, and board diversity. Impressive ESG scores show that companies are mitigating risks, creating shared value, and building shared trust. They attract investment and signal the depth of a company’s commitment to positively impacting the world. Okafor et al. (2021) reported that strong CR achievements are profitable for tech companies. Analyzing data from 100 tech firms, they reported that those “that spend more on CSR experience a corresponding increase in revenue and profitability” (p. 1).

Environmental, Social, and Governance ratings are not a perfect science at this stage, as shown by the wide variance of scores for 10 companies—including Amazon and Microsoft—in Figure 1. The figure reveals that five providers (ESG raters or investment portfolio managers) often calculated widely dissimilar ratings for the same company. The importance of ESG scores has brought the rating process under scrutiny by the U.S. Securities and Exchange Commission and other organizations. A report from the International Organization of Securities Commissions (2021) stated that “there is little clarity and alignment on definitions, including on what ratings or data products intend to measure” and “a lack of transparency about the methodologies underpinning these ratings” (p. 1).

Figure 1

*ESG Ratings of Companies with Largest Market Capitalization in 10 Industries*

## ESG Rating



*Note:* Adapted from “ESG Investing: Practices, Progress and Challenges,” by R. Boffo and R. Patalano, 2020, OECD Paris, p. 29, [www.oecd.org/finance/ESG-Investing-Practices-Progress-Challenges.pdf](http://www.oecd.org/finance/ESG-Investing-Practices-Progress-Challenges.pdf). Copyright 2020 by the The Organisation for Economic Co-operation and Development (OECD). Used with permission.

In an effort to “[go] beyond existing ESG scores” and understand the most common metrics companies use to present their CS programs, the Rustandy Center for Social Sector Innovation at the University of Chicago Booth School of Business gathered social and environmental metrics from S&P 500 companies’ 2017 CSR reports (Li et al., 2021, p. 3). Given the confusing host of variables in CR reports across industries, the results of this study deserve a brief look. The most commonly used social metrics across 327 Fortune 500 firms were for

diversity, safety, community engagement, and suppliers, and each category in the study went one level deeper to list the top five most-used metrics. The number one most-used metric for diversity was “women employees”; for safety: “total recordable incident rate”; for community engagement: “volunteer hours,” with “donations” a close second; and for suppliers: “total spending on diverse suppliers.” Data for environmental metrics revealed that the most-used metrics were for greenhouse gas (number one most-reported: “Gross scope 1 GHG emissions”), energy, water, waste, and accidents and fines (p. 5).

Big Tech reports on the same basic categories outlined in the above study. On social responsibility, Amazon, Apple, Google, Meta, and Microsoft each report on their increases in gender and racial diversity, progress of their community engagement programs, and updates to their detailed privacy policies. They also develop multi-faceted environmental programs and announce climate change goals: Google, Apple, and Meta announced they would be carbon-neutral (removing the equal amount of CO<sub>2</sub> from the atmosphere that they emit) by 2030, Amazon by 2040, and Microsoft said it would be carbon negative (capturing more CO<sub>2</sub> than it emits) by 2030. Facebook launched a “Climate Science Center” in 2020 to counter misinformation about climate change (Facebook, 2023). The positive effects of these significant corporate commitments extend to company financial performance (Wang et al., 2015). A study conducted by the Infosys (2022) consulting firm reported that increasing ESG spending by 10 percentage points correlates with a 1 percentage point increase in profit growth. One issue around CR/ESG reporting important to consumers, particularly around facts about environmental programs, concerns messaging that can be misleading. For example, reading the statement printed in bold text—“100% renewable energy sourced for all Apple facilities” (Apple, 2022, p. 14)—a customer may believe the company is 100 percent “green,” when in fact “facilities” refers to corporate buildings, not the manufacturing and transportation supply chain. Elsewhere in the

report, the consumer will find graphics and tables informing that the company had a carbon footprint of 23,200,000 metric tons of gross carbon emissions (p. 15, 78).

Traditional CR/ESG frameworks often fall short in capturing the full complexity of Big Tech's societal impact. To address this, it may be more effective to focus on alternative metrics that better reflect the true influence of Big Tech on society. Some of these alternative metrics could be:

- **Data Privacy and User Control:** Evaluating how well companies protect user data, ensure transparency, and give users control over their personal information.
- **Algorithmic Fairness and Bias Mitigation:** Assessing the fairness of algorithms and the effectiveness of strategies to reduce bias.
- **Platform Responsibility in Combating Misinformation and Hate Speech:** Measuring how platforms address and mitigate harmful content, including misinformation and hate speech.
- **Impact on Local Journalism:** Analyzing how Big Tech influences the sustainability of local journalism and broader media ecosystems.

Corporate responsibility and ESG assessment, measurement, and profitability have motivated Big Tech to make positive impacts on society and the environment, yet those impacts exist alongside the spectrum of disruptions they have also produced.

The rapid growth of AI, driven by significant investments from Big Tech companies like Google, Microsoft, and Meta, has amplified both environmental and social costs. With projections that these companies will invest \$320 billion in AI infrastructure by 2025, the demand for energy is soaring. This surge, much of it fueled by fossil fuels, compromises efforts toward clean energy goals. Data centers, responsible for much of this energy use, are expected to

account for 9% of U.S. electricity consumption by 2030, significantly heightening the industry's environmental impact (ESGDive, 2025).

The effects of Big Tech's dominance in AI are increasingly evident. Research from UC Riverside and Caltech highlights that pollution from data centers run by these companies has already cost the U.S. over \$5 billion in healthcare expenses, disproportionately affecting lower-income communities. Actions like a single ChatGPT query consume nearly ten times the energy of a standard Google search, underscoring the rising costs of AI growth (Sustainability Magazine, 2025).

As the scale of AI investment continues to grow, so do its associated costs. The industry therefore requires, now, more than ever, oversight through a regulatory framework that addresses tech companies' relationships with and responsibilities toward consumers and the digital information and commerce environments. The model presented here addresses those components.

### **A Model of Big Tech Oversight**

Historically, innovations that have sparked periods of massive technological change are followed by movements to rein in the socially disruptive elements the technology imposes. Economists such as Caetano Penna (2022), who calls for a new era of governance that addresses Big Tech's disruptions to business models and other established norms, recognize the impact of the industry's ever-growing reach and harms. Their prediction that a phase of social self-protection will inevitably follow is based on Karl Polanyi's (1957/2001) conception of the capitalist "double movement"—periods of new technology that launch free market expansion are separated by periods of protective intervention.

To date, the United States Congress has been unable to provide the protective intervention necessary to address the harms wrought by Big Tech other than one law, the

Children’s Online Privacy Protection Act of 1998 (COPPA), which “prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet” (Federal Trade Commission, 1999, p. 22751). In 2022, Amazon, Apple, Google, Meta, and Microsoft spent nearly \$69 million (Cohen, 2023) lobbying the federal government in efforts to prevent passage of laws that would curb their anti-competitive behavior such as The American Innovation and Choice Online Act and The Open Apps Market App, both of which have bipartisan support.

However, movement on Big Tech regulation in the U.S. is beginning to take place at the state level. California, Colorado, Connecticut, Utah, and Virginia have enacted comprehensive data privacy laws. Common provisions among these laws include the right to opt-out of the sale of personal information—an action that targets the main driver of the attention economy business model (National Conference of State Legislators, 2022). These laws can provide protection to users throughout the country: California’s 2020 privacy law “became a de facto US standard because tech companies realized it would be easier to follow its rules universally rather than weed out California users” (Olson, 2022).

The past 15 years of Big Tech expansion into the framework of society is a critical shift that requires the same protective action the federal government provided when industries developed dominant economic power and/or impact. New economic realities required specialized oversight. Former FCC Commissioner Tom Wheeler (2021) cited examples such as the Interstate Commerce Commission (the nation’s first regulatory agency) launched in 1887 to counteract the railroad companies’ “abusive exercise of their economic power”; the Securities and Exchange Commission (SEC) in 1934 to oversee markets following the stock market crash of 1929 that led to the Great Depression; and the Consumer Financial Protection Bureau (CFPB) in 2010 in the wake of the stock market crash of 2008 and ensuing Great Recession. These

specialized agencies were created to bring the critical expertise and concentration of focus required to adequately oversee industries that have outsized societal and economic impact. In some cases, new agencies branched off from larger ones, and in others, such as the formation of the CFPB as part of the Dodd-Frank Wall Street Reform and Consumer Protection Act., originated on their own.

The lack of tech policy from Congress leaves the court system responsible for consequential decisions about the behavior of Big Tech. The largest of the federal and state antitrust cases, *U.S. v. Google*, filed by the Department of Justice and 11 state attorneys general in October 2020, accuses the company of monopolizing the internet search and advertising markets. The Justice Department’s rationale for the case is a fit summary of the scope of Big Tech disruptions that block the innovations that could make the industry fairer and more competitive:

As one of the wealthiest companies on the planet with a market value of \$1 trillion, Google is the monopoly gatekeeper to the internet for billions of users and countless advertisers worldwide. For years, Google has accounted for almost 90 percent of all search queries in the United States and has used anti-competitive tactics to maintain and extend its monopolies in search and search advertising. Competition in this industry is vitally important, which is why today’s challenge against Google—the gatekeeper of the Internet—for violating antitrust laws is a monumental case both for the Department of Justice and for the American people. (U.S. Department of Justice, 2020, para. 4)

Regarding oversight for Big Tech’s societal harms, to-date the industry has not been liable for harms resulting from content on its platforms due to protections granted by Section 230 of the Communications Decency Act. In early 2023 the Supreme Court heard arguments about two cases challenging this protection. The first of two cases argued in February and March 2023,

*Gonzales v. Google*, was brought by a family who allege their daughter was killed in a 2015 ISIS terrorist attack in Paris due to ISIS recruitment videos on YouTube. The case alleges that not only did YouTube's algorithms proliferate radicalism that recruited ISIS members, but that the company materially benefited by earning revenue from the ads inserted into the ISIS videos. Both the Anti-Terrorism Act (ATC) and the Justice Against Sponsors of Terrorism Act (JASTA) come into play in the second case, *Twitter Inc. V. Taamneh*. Similar to the *Gonzalez* case, the *Taamneh* complaint alleges that ISIS content on Twitter was responsible for the death of Nawras Alassaf during an ISIS attack on a nightclub in Turkey. The platform allegedly aided and abetted the attack by providing the infrastructure for ISIS to carry out its activities (Broukhim et al., 2023).

Both cases shed light on the algorithms that spin out recommendations designed to keep users online and exposed to ads. This manipulation at the heart of the tech business model defines the greatest harms allegedly caused by the industry: the loss of human life. As the Supreme Court cases and the online-induced organization of the attack on the U.S. Capitol on January 6, 2021, attest, the "recommendations" issue is key to tech harms. Facebook recommendation algorithms alone are responsible for 64% of all extremist group recruitment (Minevich, 2021). Resolving the issue requires new rules regarding these automated recommendations, a highly technical area in an industry that Supreme Court Justice Elena Kagan admitted challenged the Court's expertise, stating during Gonzalez arguments, "We're a court, we really don't know about these things. These are not like the nine greatest experts on the internet" (Gerstein & Kern, 2023, para. 5).

If the Court's rulings permit tech companies to continue to be shielded from liability about content via Section 230, advocates for tech regulation will likely call for Congress to take up an urgent agenda on the issue. The tech culture that is continuously on the defensive to fend

off policy changes would benefit from partnering “with the public sector on projects that in the short term might be financially costly and limit flexibility but will yield longer-term benefits,” advised Columbia Business School professor and investment expert Jonathan Knee (Beard, 2022, para. 9). Matt Schruers, president of the tech-promoting group the Computer & Communications Industry Association, suggested that Congress should focus on pieces of oversight such as “ensuring consumers have baseline federal privacy protections” while the courts engage in Section 230 and First Amendment issues (Fried, 2023, para. 9).

Facebook whistleblower Frances Haugen (2021) testified that revisions in Section 230, if so ordered by the Court, would not be adequate to regulating the industry because it would not have enough of an impact on the fundamental business model. Facebook, she stated, will not change their business model on their own because “they have put their immense profits before people. . . . Facebook chooses profit over safety every day” (pp. 1, 4). She maintained that the “severity of this crisis demands that we break out of previous regulatory frames” (p. 2) because “a company with control over our deepest thoughts, feelings and behaviors needs real oversight” (p. 3).

Big Tech has shown, through years of government hearings such as the one in which Haugen (2021) testified as well as its business behaviors, that its priorities are expanding market growth and profits, even though these priorities create the harms described in this paper. This justifies a call for rigorous oversight. Wheeler (2021) advised that the complexity of digital tech demands a stand-alone agency. Penna (2020) claimed that digital tech’s disruptions of established structures call for “a new governance system” (para. 20) comprised of “a new institutional architecture that addresses the negative consequences of technologies and the socioeconomic inequalities at the global level” (para. 24). Other tech experts submit that “multiple overlapping tools and specialist oversight are needed to identify and mitigate

significant risks and prevent systemic problems” (Simpson & Conner, 2021) and “the fundamental data and AI algorithms need to change” (Minevich, 2021).

The proposed regulatory framework presented here is designed in part to reflect the consumer-protection mission of the Consumer Financial Protection Bureau (CFPB), an agency launched in the wake of the 2008 financial crisis to remedy the harms of the inadequately regulated finance industry.

### **Lessons from AI Regulation Efforts Worldwide**

The EU’s 2024 AI Act sets a strong precedent with its comprehensive approach to regulating AI, focusing on high-risk applications and ensuring transparency. It bans social scoring, restricts criminal profiling, and mandates labels on AI-generated content. These provisions highlight the importance of safeguarding fundamental rights while promoting innovation (European Union, 2024)

In contrast, the U.S. continues to lack a unified AI regulatory framework. The few states who have been trying to work towards AI regulation have faced strong pushback from tech companies. Similarly, Canada’s proposed AI regulations have met criticism from firms like Amazon and Meta, who argue that the laws are too vague and burdensome (The Canadian Press, 2024). Globally, countries like Chile and South Korea are adopting similar risk-based approaches to AI regulation, while others, such as Japan and Taiwan, are prioritizing to foster innovation

### How AI policy differs across the US, EU and China

|                                       | UNITED STATES   | EUROPEAN UNION  | CHINA  |
|---------------------------------------|---|---|--|
| <b>Core AI regulation approach</b>    | Market-driven   | Rights-driven   | State-driven   |
| <b>Governing institutions</b>         | Representative democracy  | Multinational representative democracy  | Single-party autocracy   |
| <b>User rights and privacy policy</b> | Limited regulation, history of both public and private sector user-data collection and surveillance | Increasingly regulated (GDPR, Digital Markets Act, etc.), limits on public and private surveillance | Systematic data aggregation and surveillance, limited user access to international internet activity               |
| <b>Response to AI risks</b>           | Democracy/rights promotion, open internet   | Democracy/rights promotion, open internet   | Strengthen party control   |
| <b>Policy action to date</b>          | AI Bill of Rights, NIST AI Risk Management Framework, CHIPS and Science Act, Executive Order on AI  | AI Act, GDPR, DMA, DSA  | Regulations on recommendation algorithms, deep synthesis, and generative AI; party oversight of publicly held LLMs |

Abbreviations: CHIPS, Creating Helpful Incentives to Produce Semiconductors; DMA, Digital Markets Act; DSA, Digital Services Act; GDPR, General Data Protection Regulation; LLM, large language model; NIST, National Institute of Standards and Technology.

SOURCE: ADAPTED FROM A. STANGER ET AL / AR POLITICAL SCIENCE 2024

KNOWABLE MAGAZINE

with lighter regulations. In these cases, the emphasis is on balancing regulation with business growth and investment (du Plessis, McQue, Martins, & Bhattacharya, 2025)

Widespread lobbying efforts from tech giants is clearly one of the biggest challenges to regulation in this sector. These companies consistently push to shape laws in ways that favor their business interests. The U.S. will face the same pressures, and the key lesson from

other countries is the need for a regulatory framework that is both flexible and robust enough to address the risks posed by AI without stifling innovation.

As the U.S. develops its approach, it could learn from these global efforts - combining risk-based regulation with a focus on transparency, fairness, and accountability. A balanced framework can foster innovation while ensuring that the public interest and human rights are protected.

However, even as regulatory frameworks emerge, enforcement remains a significant challenge. Many governments struggle to ensure compliance, as rapid AI advancements often outpace legal mechanisms. Without strong enforcement strategies, even the most well-designed regulations risk being ineffective.

### The Enforcement Gap: Challenges in Regulating AI

Despite the EU's extensive regulatory efforts, compliance remains a significant challenge for Big Tech. The enormous societal and economic impact of Big Tech requires a more rigorous framework beyond merely enacting laws. The EU AI Act, one of the first comprehensive laws towards AI, exemplifies the regulatory push, but its implementation timeline and complexity pose difficulties for organizations striving to comply.

A recent panel of AI experts assembled by MIT Sloan Management Review and Boston Consulting Group reveals divided opinions on organizational readiness for the EU AI Act. Nearly half (47%) of experts doubt that organizations will meet the Act's requirements within the next 12 months, while only 20% express confidence. Compliance will be phased in, but the timeline remains aggressive. The first phase, covering prohibited AI systems, takes effect in six months, followed by generative AI requirements in 12 months and broader high-risk system regulations within two years. Many organizations will struggle to meet these deadlines, with experts suggesting that even two years may be insufficient for full compliance. (Sloan Review, 2024)

Large corporations with extensive AI deployments face hurdles such as achieving transparency across multiple AI use cases, interpreting ambiguous requirements, and establishing oversight mechanisms. Medium and small-sized businesses, on the other hand, may find the compliance process overly complex and resource-intensive. One of the biggest challenges is the interpretation of the Act's requirements, as many of its provisions introduce novel concepts that require translation into actionable engineering solutions. Experts argue that the ambiguity surrounding legal definitions, risk classifications, and penalties could delay compliance efforts.

AI expertise is critical for ensuring compliance, but there is a shortage of qualified professionals to navigate the regulatory landscape. Compliance with the EU AI Act requires not

just legal and ethical expertise but also the ability to integrate these considerations into AI systems. Organizations with strong governance structures in place – particularly those in highly regulated industries – may fare better. However, companies already lagging in their AI governance efforts will likely find compliance daunting.

Beyond organizational readiness, enforcement remains a key concern. The EU AI Act categorizes AI models based on risk levels – ranging from minimal to unacceptable risk. While banning high-risk AI models outright may be straightforward, regulating them effectively poses significant challenges. The EU plans to establish an AI Office to oversee implementation, but ensuring consistent enforcement across member states remains uncertain, as seen with previous laws like GDPR. Questions also persist about the AI Office’s funding, staffing, and overall capacity to oversee general-purpose AI systems (TechTarget, 2024; Regulatory Review, 2024)

Businesses operating within or affecting the EU must proactively plan for compliance. High-risk AI applications, such as those used in hiring or border security, will face stringent requirements, while minimal-risk AI models will be encouraged to adhere to voluntary codes of conduct. Organizations must inventory their AI systems, develop classification frameworks, and assess risks.

Once the EU AI Act is officially adopted, it will take effect in phases—within six months for unacceptable-risk AI, 24 months for general-purpose AI, and 36 months for high-risk AI. Noncompliance will result in financial penalties. Despite its challenges, the Act’s risk-based regulatory approach ensures relevance even as AI technology evolves. However, the effectiveness of the EU AI Act will ultimately depend on enforcement mechanisms, corporate preparedness, and the broader ability to translate legal mandates into actionable AI governance practices

## **The Consumer Technology Protection Agency**

Creating a robust regulatory framework for Big Tech is not out of reach. Just as the CFPB was established to protect individuals from predatory financial practices, a dedicated Consumer Technology Protection Agency could safeguard users in the digital realm. While the CFPB itself currently faces headwinds – including funding cuts, layoffs, and political resistance – its existence proves that bold regulatory action is possible. Strengthening and adapting such oversight models is essential to holding powerful tech companies accountable and protecting the public interest. The CFPB, which was already handling Big Tech cases, oversees a wide range of areas that reflect the complexity of the financial services industry. The bureau consolidated oversight that had been scattered throughout seven other agencies, and its current director has hired 25 technologists to work on Big Tech issues (Lapowsky, 2022).

In 2021 the CFPB addressed Big Tech-enabled fraud by filing a lawsuit in federal court against BrightSpeed Solutions, Inc., “for knowingly processing payments for companies engaged in internet-based technical-support fraud” (Consumer Financial Protection Bureau, 2021a, para. 1). The same year, the CFPB began an inquiry into the payment services operated by Amazon, Apple, Facebook, Google, PayPal and Square “to provide information about their business practices, including their data collection and use, their policies for removing individuals or businesses from their platforms, and their policies and practices for adhering to key consumer protections like addressing disputes and errors” (Consumer Financial Protection Bureau, 2022, para. 1). The CFPB inquiry targets the companies’ use of personal data, which puts consumers at risk through “behavioral targeting,” a practice that “may not align with consumers’ expectations” (Consumer Financial Protection Bureau, 2021b, para. 7). Their concerns were heightened by the fact that Big Tech aspired to expand these payment programs.

Modeling a Big Tech regulatory agency after the CFPB and naming it the Consumer Technology Protection Agency would assure the public that the government recognizes and is committed to remedying the severity of Big Tech harms. The new agency would be tasked with making the digital eco-space work for consumers and the economy as a whole, echoing the CFPB's purpose to "protect consumers from unfair, deceptive, or abusive practices and take action against companies that break the law" (Consumer Financial Protection Bureau, 2023, para. 1). Applied to the tech industry, this would bring a new arm of federal scrutiny to Big Tech impacts on privacy, mental health, discrimination, behavioral modification, monopolization, and other facets of society and democracy.

While the CFPB is funded by the Federal Reserve, which derives the funding from bank fees, the Consumer Technology Protection Agency could be funded through Congressional appropriations that are in turn funded by the billion's tech companies pay in penalty fees to the U.S. Treasury. Since 2015, more than \$30 billion in antitrust fines have been levied against Google, Apple, Meta, Amazon, and AI company Qualcomm (Fitri, 2022). This amount would potentially operate the new tech protection agency for five decades, based on the \$640 million the CFPB received for the 2022 fiscal year (Gresko, 2023). The technical expertise the CFPB brought on board to address tech abuses is another model for the proposed Consumer Technology Protection Agency, which would be staffed by data scientists and individuals with industry engineering experience. This workforce would have the capacity to investigate solutions to the algorithmic processes and other highly technical factors exclusive to the industry.

We also propose a cabinet post devoted to industry to ensure a strong relationship with the presidency. The status of Big Tech in the economy and its role in society requires a Secretary of Technology to advise the president on the complex issues of digital technology. This position

could also be inserted in a related office as the Assistant Secretary of Technology in the Commerce Department.

The creation of The Consumer Technology Protection Agency and Secretary of Technology cabinet position would provide the level of oversight sufficient for the dominating influence digital technology companies have on the nation and the global economy.

The call for stronger oversight becomes even more critical in light of the unprecedented surge of generative AI technologies. Fueled by the same tech giants that dominate today’s digital landscape, this new wave of AI innovation brings both transformative potential and complex risks – from misinformation and bias to data privacy and market concentration. Understanding this rapidly evolving frontier highlights why a dedicated Consumer Technology Protection Agency is essential to safeguard the public interest in an increasingly AI-driven world.

### **The 2023 Artificial Intelligence Boom**

The 2023 artificial intelligence (AI) boom, marked by the launch of chat-based search products from Microsoft and Google, has heightened concerns about the concentration of power among tech giants—Meta (Facebook), Apple, Amazon, Alphabet (Google), and Microsoft. These companies now dominate the world’s most profitable and far-reaching industry.

The current AI boom revolves around generative AI technology and large language models (LLMs). Trained on vast datasets, these LLMs can predict words, generate coherent text, translate languages, and answer complex questions in a human-like manner (Ihnatchyck, 2023) Some prominent models in the market include OpenAI’s ChatGPT-4, Meta’s Llama 3.1, Google’s Gemini, and Anthropic’s Claude 3.5.

The rapid growth of these technologies has been striking—OpenAI’s ChatGPT became the first application in history to reach 1 million users in just five days after launch and currently has an

active user base of over 400 million weekly users (Reuters, 2023; CNBC, 2025). Microsoft, notably, owns approximately 49% of OpenAI's equity, further entrenching its influence. The partnership between Microsoft and OpenAI highlights the unchecked power wielded by Big Tech. In 2023, OpenAI secured a substantial investment from Microsoft, entering into an exclusive agreement for computing power. Over time, OpenAI sought to renegotiate the deal to secure more resources and reduce costs. This highlights the consolidation of power within Big Tech: even a major AI player like OpenAI is dependent on tech giants for funding and cloud infrastructure essential for AI development. This raises a critical question about the future for smaller AI startups, whose survival could be at the mercy of these monopolistic forces (Duhigg, 2023)

In such a short span of time, this new technology too has been at the forefront of several controversies largely on the front of misinformation, bias and data privacy. A key risk associated with this technology is its tendency to hallucinate which happens when a generative AI model produces inaccurate or completely fabricated information, essentially "making things up" and presenting them as factual, even though they don't exist.

In 2023, U.S. talk radio host Mark Walters sued OpenAI after ChatGPT falsely claimed he was sued by the Second Amendment Foundation (SAF) for embezzlement. Walters, unaffiliated with SAF, was misidentified due to a statistical correlation in the model's training data (Ballard Spahr, 2024)

Earlier in 2024, an AI chatbot on New York City's official website falsely claimed that employers could legally fire workers for complaining about sexual harassment, failing to disclose a pregnancy, or refusing to cut their dreadlocks (Associated Press, 2024)

In another recent instance, controversy arose when users attempted to generate images of historical figures using Google's Gemini. The tool produced historically inaccurate results, such as

ethnically diverse depictions of the U.S. Founding Fathers and a multiracial portrayal of Nazis (The Guardian, 2024)

### **Conclusion**

Controversy around the trustworthiness of this new technology has been fueled by expectations that (a) big tech will more deeply infiltrate daily life and society, and (b) development of AI as the next generation of innovation will remain in the hands of the few companies that have the resources to develop it.

Big tech companies are just that—entities created to make a profit. Their influence on society puts that fundamental goal at odds with their stakeholders, from individuals to the global environment, regardless of their ESG initiatives, because short-term-profit motives overtake investment in the most well-intentioned programs.

The unchecked power of Big Tech has prompted growing calls for stronger AI legislation to ensure ethical oversight. While Biden’s executive order on AI marked a step forward, several proposed bills aim to establish necessary guardrails. The Algorithmic Accountability Act would require companies to assess and mitigate the impact of automated systems to prevent biased or discriminatory outcomes. The Deepfakes Accountability Act seeks to regulate the use of AI in creating misleading or harmful content. The Future of Artificial Intelligence Innovation Act focuses on studying AI’s long-term impact on the economy, workforce, and national security. The challenge now lies in transforming these proposals into enforceable laws. In an era marked by diminished corporate responsibility, Big Tech stands as a prime example. Without comprehensive regulation, the harmful effects of these companies will not only persist but likely intensify. Thoughtfully crafted regulation can do more than just curb the damage – it can foster a healthier, more accountable tech industry, one that continues to innovate while upholding ethical standards and protecting the public interest.

Polanyi (1944/2001) asserted that no society could withstand the damages inflicted by a market economy “unless its human and natural substance as well as its business organization was protected against the ravages of this satanic mill” (77). His language is not extreme when considering the threat to democratic principles and institutions, mental health costs of tech addiction, deadly consequences of behavioral manipulation and online misinformation, and lack of moral consciousness regarding these facts that appears to drive Big Tech’s rejection of any and all oversight. The digital era requires protection with the substance to match the most powerful and influential industry in the world.

## References

- Abernathy, P. (2022, June 29). The state of local news: The 2022 report. Northwestern University Local News Initiative.  
<https://localnewsinitiative.northwestern.edu/research/state-of-local-news/report/>
- ABC News. (2024, February 20). *AI deepfakes top concern for election officials as voting gets underway*. ABC News. <https://abcnews.go.com/Politics/ai-deepfakes-top-concern-election-officials-voting-underway/story?id=114202574>
- Adamson, A. S., & Smith, A. (2018). Machine learning and health care disparities in dermatology. *Journal of the American Medical Association Dermatology*, 154(11), 1247–1248. <https://doi.org/10.1001/jamadermatol.2018.2348>
- Agence France Press. (2009, June 14). Mobile phones, Facebook, YouTube cut in Iran. Phys.org. <https://phys.org/news/2009-06-mobile-facebook-youtube-iran.html>
- Alegre, S. (2024). The CrowdStrike outage shows how vulnerable we have become. Centre for International Governance Innovation. <https://www.cigionline.org/articles/the-crowdstrike-outage-shows-how-vulnerable-we-have-become/>
- Alizada, N., Boese, V. A., Lundstedt, M., Morrison, K., Natsika, N., Sato, Y., Tai, H., & Lindberg S. I. (2022). *Democracy report 2022: Autocratization changing nature?* Varieties of Democracy. [https://v-dem.net/media/publications/dr\\_2022.pdf](https://v-dem.net/media/publications/dr_2022.pdf)
- Allcott, H, Braghieri, L., Eichmeyer, S., & Gentzkow, M. (2020). The welfare effects of social media. *American Economic Review*, 110(3), 629–676. <https://doi.org/10.1257/aer.20190658>
- Anderson, J. A., McCradden, M. D., & Stephenson, E. A. (2022). Response to open peer commentaries: On social harms, big tech, and institutional accountability. *American Journal of bioethics*, 22(10), W6–W8. <https://doi.org/10.1080/15265161.2022.2075977>

- Apple. (2022). Environmental Social Governance Report 2022.  
[https://s2.q4cdn.com/470004039/files/doc\\_downloads/2022/08/2022\\_Apple\\_ESG\\_Report.pdf](https://s2.q4cdn.com/470004039/files/doc_downloads/2022/08/2022_Apple_ESG_Report.pdf)
- Associated Press. (2024, January 28). New York City chatbot misinformation lawsuit allowed to proceed. AP News. <https://apnews.com/article/new-york-city-chatbot-misinformation-6ebc71db5b770b9969c906a7ee4fae21>
- Ballard Spahr LLP. (2024, January 23). Judge denies motion to dismiss AI defamation suit. Ballard Spahr. <https://www.ballardspahr.com/insights/alerts-and-articles/2024/01/judge-denies-motion-to-dismiss-ai-defamation-suit>
- Banker, S., & Khetani, S. (2019). Algorithm overdependence: How the use of algorithmic recommendation systems can increase risks to consumer well-being. *Journal of Public Policy & Marketing*, 38(4), 500–515. <https://doi.org/10.1177/0743915619860429>
- Barrero, J. M., Bloom, N., & Davis, S. J. (2021). *Why working from home will stick*. National Bureau of Economic Research Working Paper 28731. [https://wfhresearch.com/wp-content/uploads/2023/02/WFHResearch\\_updates\\_February2023.pdf](https://wfhresearch.com/wp-content/uploads/2023/02/WFHResearch_updates_February2023.pdf)
- BBC News. (2021, January 15). *Dutch Rutte government resigns over child welfare fraud scandal*. <https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/>
- Beard, A. (2022). Can big tech be disrupted? *Harvard Business Review*.  
<https://hbr.org/2022/01/can-big-tech-be-disrupted>
- Berryman, K. (2024, December 19). *Responsible enforcement will be critical to AI Act's impact*. The Regulatory Review. <https://www.theregreview.org/2024/12/19/berryman-responsible-enforcement-will-be-critical-to-ai-acts-impact/>

Boer, M., van den Eijnden, R. J. J. M., Bonie-Nissim, M., Wong, S., Inchley, J. C., Badura, P., Craig, W. M., Gobina, I., Kleszczewska, D., Klanšček, H., J., & Stevens, G. W. J. M. (2020). Adolescents' intense and problematic social media use and their well-being in 29 countries. *Journal of Adolescent Health* 66(6), S89–S99.

Boffo, R., & Patalano, R. (2020). *ESG investing: Practices, progress and challenges*. OECD Paris. [www.oecd.org/finance/ESG-Investing-Practices-Progress-and-Challenges.pdf](http://www.oecd.org/finance/ESG-Investing-Practices-Progress-and-Challenges.pdf)

Brookings Institution. [https://www.washingtonpost.com/business/the-way-to-police-big-tech-is-through-us-states/2022/09/22/aab2c0de-3a7f-11ed-b8af-0a04e5dc3db6\\_story.html](https://www.washingtonpost.com/business/the-way-to-police-big-tech-is-through-us-states/2022/09/22/aab2c0de-3a7f-11ed-b8af-0a04e5dc3db6_story.html)

Broukhim, B, Carney, B., & Jovanovic, S. (2023, February 20). *Oral argument review: Gonzalez, et al. v. Google and Twitter, Inc. v. Taamneh, et al.* Lawfare. <https://www.lawfareblog.com/oral-argument-preview-gonzalez-et-al-v-google-and-twitter-inc-v-taamneh-et-al>

Buolamwini, J. (2019, February 7). Artificial intelligence has a problem with gender and racial bias. *Time*. <https://time.com/5520558/artificial-intelligence-racial-gender-bias/>

Burgess, M. (2022, December 1). Iran's protests reveal what's lost if Twitter crumbles. *Wired*. <https://www.wired.com/story/protests-in-iran-twitter/>

Business Wire. (2021, June 24). *Strategy analytics: Half the world owns a smartphone*. <https://www.businesswire.com/news/home/20210624005926/en/Strategy-Analytics-Half-the-World-Owns-a-Smartphone>

Canadian Broadcasting Corporation. (2024, January 10). AI law too vague, companies like Amazon and Meta say. CBC News. <https://www.cbc.ca/news/politics/ai-law-too-vague-companies-say-1.7108393>

- Cao, Y., Li, S., Liu, Y., Yan, Z., Dai, Y., Yu, P. S., & Sun, L. (2023). A comprehensive survey of AI-generated content (AIGC): A history of Generative AI from GAN to ChatGPT. *ArXiv*. <https://doi.org/10.48550/arXiv.2303.04226>
- Carnegie Endowment for International Peace. (2024, December). *Can democracy survive the disruptive power of AI?* Carnegie Endowment for International Peace. <https://carnegieendowment.org/research/2024/12/can-democracy-survive-the-disruptive-power-of-ai?lang=en>
- CNBC. (2025, February 20). *OpenAI tops 400 million users despite Deepseek's emergence*. <https://www.cnbc.com/2025/02/20/openai-tops-400-million-users-despite-deepseeks-emergence.html>
- CNN. (2024, January 22). *Fake Joe Biden robocall investigated by authorities*. CNN. <https://www.cnn.com/2024/01/22/politics/fake-joe-biden-robocall/index.html>
- Coate, P. (2021, January 25). *Remote work before, during, and after the pandemic*. National Council on Compensation Insurance. [https://www.ncci.com/SecureDocuments/QEB/QEB\\_Q4\\_2020\\_RemoteWork.html](https://www.ncci.com/SecureDocuments/QEB/QEB_Q4_2020_RemoteWork.html)
- Coghlan, A. F, Gioco, C., McCosh, L, Mencarini, F., Migliora, G., Moulder, M, Roure, O. L., Saha, U., Soverini, A, Su, R., & Leiser, M. (2021). Special rapporteur on the promotion and protection of the right to freedom of opinion and expression: A report by students at Leiden Law School. <https://www.ohchr.org/sites/default/files/Documents/Issues/Expression/disinformation/3-Academics/Leiden-University-Law-School.pdf>
- Cohen, J. (2023, January 25). What the past year of tech lobbying looked like. The Hustle. <https://thehustle.co/01262023-tech-lobbying/>

- Colorado General Assembly. (2024). Senate Bill 24-205: Act concerning consumer protections in interactions with artificial intelligence systems. <https://leg.colorado.gov/bills/sb24-205>
- Constantz, J. (2023, February 3). *California's new gold rush: Big tech moves to gain the edge in AI*. Bloomberg. <https://www.bloomberg.com/news/articles/2023-02-03/big-tech-earnings-call-mentions-of-ai-spike-after-chatgpt-went-viral>
- Consumer Financial Protection Bureau (2021a, March 3). *Consumer Financial Protection Bureau takes action against payment processor and its former CEO for supporting internet-based technical-support scams*. <https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-takes-action-against-payment-processor-and-its-former-ceo-for-supporting-internet-based-technical-support-scams/>
- Consumer Financial Protection Bureau (2021b, October 21). *CFPB Orders Tech Giants to Turn Over Information on their Payment System Plans*. <https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-tech-giants-to-turn-over-information-on-their-payment-system-plans/>
- Consumer Financial Protection Bureau (2022, October 31). *CFPB seeks further public input on big tech payment platforms*. <https://www.consumerfinance.gov/about-us/blog/cfpb-seeks-further-public-input-on-big-tech-payment-platforms/>  
<https://www.consumerfinance.gov/about-us/blog/cfpb-seeks-further-public-input-on-big-tech-payment-platforms/>
- Consumer Financial Protection Bureau (2023). "The Bureau." <https://www.consumerfinance.gov/about-us/the-bureau/>
- Coyne, S. M., Rogers, A. A., Zurcher, J. D., Stockdale, L., & Booth, M. (2020). Does time spent using social media impact mental health?: An eight year longitudinal study. *Computers in Human Behavior*, 104, Article 106160. <https://doi.org/10.1016/j.chb.2019.106160>

- Crawford, K. (2016, June 25). Artificial intelligence's white guy problem. *New York Times*.  
<https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html>
- du Plessis, C., McQue, K., Martins, L., & Bhattacharya, A. (2025, January 20). The global struggle over how to regulate AI. Rest of World. <https://restofworld.org/2025/global-ai-regulation-big-tech/>
- Duhigg, C. (2023, December 11). The inside story of Microsoft's partnership with OpenAI. The New Yorker. <https://www.newyorker.com/magazine/2023/12/11/the-inside-story-of-microsofts-partnership-with-openai>
- Electronic Privacy Information Center (2023). "About Us." <https://epic.org/about/>
- Elhai, J. D., Dvorak, R. D., Levine, J. C., & Hall, B. J. (2016). Problematic smartphone use: A conceptual overview and systematic review of relations with anxiety and depression psychopathology. *Journal of Affective Disorders*, 207, 251–259.  
<https://doi.org/10.1016/j.jad.2016.08.030>
- European Union. (2023). *The digital services act package*. <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>
- European Union. (2024). Artificial Intelligence Act: Rules for AI. European Commission.  
<https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>
- ESG Dive. (2023, March 28). *Tech industry AI energy demands growing ESG use cases, reporting data*. ESG Dive. <https://www.esgdive.com/news/tech-industry-ai-energy-demands-growing-esg-use-cases-reporting-data/738161/>
- Everypixel Journal. (n.d.). *AI image statistics: The state of the synthetic media industry*. Everypixel Journal. <https://journal.everypixel.com/ai-image-statistics>

Facebook. (2023). Climate science center. Facebook.

[https://www.facebook.com/hubs/climate\\_science\\_information\\_center](https://www.facebook.com/hubs/climate_science_information_center)

Favaretto, M., De Clercq, E. & Elger, B.S. (2019). Big data and discrimination: Perils, promises and solutions. A systematic review. *Journal of Big Data* 6(12), 1–27.

<https://doi.org/10.1186/s40537-019-0177-4>

Federal Trade Commission. (1999). Children’s online privacy rule; proposed rule. *Federal Register* 64(80), 22750–22767.

Felton, J. (2022, May 11). *The AI that led to children being re-homed and the fall of an elected government*. IFLscience. <https://www.iflscience.com/the-ai-that-led-to-children-being-rehomed-and-the-fall-of-an-elected-government-63622>

Fitri, A. (2022, March 15). *Can fines break big tech monopolies?* Techmonitor.

<https://www.wsaz.com/2023/02/27/supreme-court-agrees-hear-case-challenging-consumer-financial-protection-bureaus-funding/>

Forbes. (2024, November 17). AI-driven dark patterns: How artificial intelligence is supercharging digital manipulation. *Forbes*.

<https://www.forbes.com/sites/federicoguerrini/2024/11/17/ai-driven-dark-patterns-how-artificial-intelligence-is-supercharging-digital-manipulation/>

Fried, I. (2023, March 1). *Judges, not lawmakers, are setting 2023’s tech policy*. Axios.

[https://www.axios.com/newsletters/axios-login-837037ce-44b8-49a3-95eb-877fd8fedd68.html?utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=newsletter\\_axioslogin&stream=top](https://www.axios.com/newsletters/axios-login-837037ce-44b8-49a3-95eb-877fd8fedd68.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioslogin&stream=top)

Fukuyama, F., Richman, B., & Goel, A. (2020, November 24). *How to save democracy from technology*. Foreign Affairs. <https://www.foreignaffairs.com/articles/united-states/2020-11-24/fukuyama-how-save-democracy->

technology?check\_logged\_in=1&utm\_medium=promo\_email&utm\_source=lo\_flows&utm\_campaign=registered\_user\_welcome&utm\_term=email\_1&utm\_content=20230223

Gerstein, J., & Kern, R. (2023, February 21). *Google appears to dodge disaster as justices review tech law*. Politico. <https://www.politico.com/news/2023/02/21/supreme-court-section-230-google-youtube-00083824>

Gillmor, D. K., & Stanley, J. (2023, February 15). *New mobile phone service shows we can have both privacy and nice things*. ACLU. <https://www.aclu.org/news/privacy-technology/new-mobile-phone-service-shows-we-can-have-both-privacy-and-nice-things>

Gisondi, M. A., Barber, R., Faust, J. S., Raja, A., Strehlow, M. C., Westafer, L. M., & Gottlieb, M. (2022). A deadly infodemic: social media and the power of COVID-19 misinformation. *Journal of Medical Internet Research*, 24(2), e35552. <https://doi.org/10.2196/35552>

Greenwald, G. (2015). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. Picador.

Gresko, J. (2023, February 27). *Supreme Court agrees to hear case challenging Consumer Financial Protection Bureau's funding*. WSAZ. <https://www.wsaz.com/2023/02/27/supreme-court-agrees-hear-case-challenging-consumer-financial-protection-bureaus-funding/>

Grundy, A. (2022, June 7). *Internet crushes traditional media: From print to digital*. United States Census. <https://www.census.gov/library/stories/2022/06/internet-crushes-traditional-media.html>

Guardian News and Media. (2018, October 10). *Amazon scrapped 'sexist AI' tool for hiring women*. The Guardian. <https://www.theguardian.com/technology/2018/oct/10/amazon-hiring-ai-gender-bias-recruiting-engine>

- Gueguen, C., Al Majali, S., & Hakspiel, J. (2020, April 13). Making digital finance work for women in the MENA region: 8 lessons from the field. SEEP.  
<https://seepnetwork.org/Blog-Post/Making-Digital-Finance-Work-for-Women-in-the-MENA-Region-8-Lessons-from-the-Field>
- Hadhazy, A. (2017, April 18). *Biased bots: Artificial-intelligence systems echo human prejudices*. Princeton University. <https://www.princeton.edu/news/2017/04/18/biased-bots-artificial-intelligence-systems-echo-human-prejudices>
- Haidt, J. (2022, July 28). Yes, social media really is undermining democracy. *The Atlantic*.  
<https://www.theatlantic.com/ideas/archive/2022/07/social-media-harm-facebook-meta-response/670975/>
- Haugen, F. (2021, October 4). Statement of Frances Haugen.  
<https://www.commerce.senate.gov/services/files/FC8A558E-824E-4914-BEDB-3A7B1190BD49>
- Heikkilä, M. (2022, March 29). Dutch scandal serves as a warning for Europe over risks of using algorithms. Politico. <https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/>
- Hern, A. (2018, May 6). Cambridge Analytica: How did it turn clicks into votes? *The Guardian*.  
<https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>
- Hermann, E., & Puntoni, S. (2024). Artificial intelligence and consumer behavior: From predictive to generative AI. *Journal of Business Research*, *168*, 83–99.  
<https://doi.org/10.1016/j.jbusres.2024.03.010>
- Hoffman, J. S. (2022). *Your data, their billions: Unraveling and simplifying big tech*. Post Hill Press.

- Hu, K. (2023, February 1). ChatGPT sets record for fastest-growing user base - analyst note. Reuters. <https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/>
- Hutson, M. (2017, April 13). Even artificial intelligence can acquire biases against race and gender. *Science*. <https://www.science.org/content/article/even-artificial-intelligence-can-acquire-biases-against-race-and-gender>
- Ienca, M., & Vayena, E. (2018, March 30). *Cambridge analytica and online manipulation*. Scientific American. <https://blogs.scientificamerican.com/observations/cambridge-analytica-and-online-manipulation/>
- Ihnatchyck, Y. (2023, October 27). Introduction to GenAI: What are LLM models, and how are they used in GenAI? Datafloq. <https://datafloq.com/read/introduction-gen-ai-llm-models/>
- Illinois General Assembly. (n.d.). *Illinois Artificial Intelligence Video Interview Act*. <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4015&ChapterID=68>
- Infosys (2022). Infosys research: Nine out of ten executives report ESG delivers ROI. <https://www.infosys.com/newsroom/press-releases/2022/esg-delivers-roi-report.html>
- International Organization of Securities Commissions (2021, November). Environmental, social, and governance (ESG) ratings and data products providers: Final report. <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD690.pdf>
- Journal of Democracy. (2024). *How AI threatens democracy*. *Journal of Democracy*. <https://www.journalofdemocracy.org/articles/how-ai-threatens-democracy/>
- J. A. Shamsi, J.A., & Khojaye, M. A. (2018). Understanding privacy violations in big data Systems. *IT Professional*, 20(3), 73–81. <https://ieeexplore.ieee.org/document/8378964/similar#similar>

- Karim, F., Oyewande, A. A., Abdalla, L. F., Chaudhry Ehsanullah, R., & Khan, S. (2020). Social media use and its connection to mental health: A systematic review. *Cureus, 12*(6), e8627. <https://doi.org/10.7759/cureus.8627>
- Koning, M. (2021, October 25). *Dutch childcare benefit scandal an urgent wake-up call to ban racist algorithms*. Amnesty International. <https://www.amnesty.org/en/latest/news/2021/10/xenophobic-machines-dutch-child-benefit-scandal/>
- Konstantinovic, D. (2023, February 3). Google misses the mark in Q4, setting up a challenging 2023 for digital advertising. Insider Intelligence. <https://www.insiderintelligence.com/content/google-misses-mark-q4-setting-up-challenging-2023-digital-advertising>
- Lapowsky, I. (2022, July 7). *In its battle with big tech, the CFPB is building an army of engineers*. Protocol. <https://www.protocol.com/policy/cfpb-hiring-tech>
- Laricchia, F. (2023, January 13). *Leading tech companies worldwide 2002, by market cap*. Statista. <https://www.statista.com/statistics/1350976/leading-tech-companies-worldwide-by-market-cap/#:~:text=In%202022%2C%20Apple%20was%20the,also%20in%20the%20top%20te>n.
- Lee, E. (2025, April 16). Appeals panel weighs pause on order blocking Trump administration from dismantling CFPB. The Hill. <https://thehill.com/regulation/court-battles/5243351-appeals-panel-cfpb-dismantle/>

- Lee, N. T. (2018). Detecting racial bias in algorithms and machine learning. *Journal of Information, Communication and Ethics in Society*, 16(3), 252–260.  
<https://doi.org/10.1108/JICES-06-2018-0056>
- LegalDive. (2024, February 19). SaaS companies use dark patterns, FTC, ICPEN, GPEN, COPPA say. *LegalDive*. <https://www.legaldive.com/news/saas-companies-use-dark-patterns-FTC-ICPEN-GPEN-COPPA/721091/>
- Li, J. M., Lu, S., & Nassar, S. (2021). Corporate social responsibility metrics in S&P 500 firms' 2017 sustainability reports. Rustandy Center for Social Innovation.  
[https://www.chicagobooth.edu/-/media/research/sei/docs/csr-metrics-rustandy-center-report\\_final.pdf](https://www.chicagobooth.edu/-/media/research/sei/docs/csr-metrics-rustandy-center-report_final.pdf)
- Microsoft. (2024, November 20). Ignite 2024: Why nearly 70% of the Fortune 500 now use Microsoft 365 Copilot. Microsoft News. <https://news.microsoft.com/en-hk/2024/11/20/ignite-2024-why-nearly-70-of-the-fortune-500-now-use-microsoft-365-copilot/>
- MIT Sloan Management Review. (2024.). *Organizations face challenges in timely compliance with the EU AI Act*. <https://sloanreview.mit.edu/article/organizations-face-challenges-in-timely-compliance-with-the-eu-ai-act/>
- McChesney, R. W. (2015). *Rich media, poor democracy*. The New Press.
- Minevich, M. (2021, January 27). *What is the social responsibility of big tech? An American lesson from 2020*. Forbes. <https://www.forbes.com/sites/markminevich/2021/01/27/what-is-the-social-responsibility-of-big-tech-an-american-lesson-from-2020/?sh=3530873b2848>

- Moscaritolo, A. (2022, January 18). *What does big tech know about you? Basically everything*. PCmag.com. <https://www.aclu.org/news/privacy-technology/new-mobile-phone-service-shows-we-can-have-both-privacy-and-nice-things>
- Nahmias, Y., & Perel, M. (2021). The oversight of content moderation by AI: Impact assessments and their limitations. *Harvard Journal on Legislation*, 58, 145. <https://advance-lexis-com.ezproxy.mnsu.edu/api/document?collection=analytical-materials&id=urn:contentItem:62J9-8XP1-F956-S26X-00000-00&context=1516831>.
- National Conference of State Legislators (2022). State laws related to digital privacy. <https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy#:~:text=Five%20states%E2%80%94California%2C%20Colorado%2C,of%20personal%20information%2C%20among%20others> Wheeler, Tom. (2021, February 10). *A focused federal agency is necessary to oversee big tech*.
- NBC News. (2024, February 5). *AI Taylor Swift endorsement for Trump was originally a Biden meme*. NBC News. <https://www.nbcnews.com/tech/tech-news/ai-taylor-swift-endorsement-trump-shared-was-originally-biden-meme-rcna170945>
- New York City Department of Consumer and Worker Protection. (n.d.). *Automated Employment Decision Tools*. February 22, 2025, <https://www.nyc.gov/site/dca/about/automated-employment-decision-tools.page>
- NewsGuard. (2024). *AI multilingual failure in Russian and Chinese disinformation*. NewsGuard. <https://www.newsguardtech.com/press/ai-multilingual-failure-russian-chinese/>
- NPR. (2018). NPR/Marist Poll: Amazon is a colossus in a nation of shoppers. NPR. <https://www.npr.org/about-npr/617470695/npr-marist-poll-amazon-is-a-colossus-in-a-nation-of-shoppers>

- O'Donnell, K. (2025, February 25). *'There will continue to be a CFPB': Trump administration says it won't shut bureau*. POLITICO. <https://www.politico.com/news/2025/02/25/cfpb-remaining-trump-administration-says-00205913>
- O'Neill, S. (2022, July 6). What is the difference between CSR and ESG? Corporate Governance Institute. <https://www.thecorporategovernanceinstitute.com/insights/lexicon/what-is-the-difference-between-csr-and-esg/>
- Okafor, A., Adeleye, B. N., & Adusei, M. (2021). Corporate social responsibility and financial performance: Evidence from US tech firms. *Journal of Cleaner Production*, 292, 1–11.
- Olson, P. (2022, September 22). The way to police big tech is through US states. *Washington Post*. [https://www.washingtonpost.com/business/the-way-to-police-big-tech-is-through-us-states/2022/09/22/aab2c0de-3a7f-11ed-b8af-0a04e5dc3db6\\_story.html](https://www.washingtonpost.com/business/the-way-to-police-big-tech-is-through-us-states/2022/09/22/aab2c0de-3a7f-11ed-b8af-0a04e5dc3db6_story.html)
- Pandey, E. (2017, November 9). Sean Parker: Facebook was designed to exploit human “vulnerability.” Axios. <https://www.axios.com/2017/12/15/sean-parker-facebook-was-designed-to-exploit-human-vulnerability-1513306782>
- Penna, C. (2022, February 14). *Technological revolutions and the role of the state in the governance of digital technologies*. Centre for International Governance Innovation. <https://www.cigionline.org/articles/technological-revolutions-and-the-role-of-the-state-in-the-governance-of-digital-technologies/>
- Petrosyan, A. (2023, February 20). *United States internet penetration 2000-2023*. Statista. <https://www.statista.com/statistics/209117/us-internet-penetration/#:~:text=As%20of%202023%2C%20approximately%2092,internet%20users%20in%20the%20country.>
- Polanyi, K. (2001). *The great transformation: The political and economic origins of our time*. Beacon Press. (Original work published 1944)

Prinstein, M. (2023, February 14). Written testimony.

file:///Users/Antonia2016iMac/Desktop/TECH%20CSR%20ARTICLE/2023-02-14%20-%20Testimony%20-%20Prinstein.pdf

Quinn, M. (2025, June 2). *Trump administration asks Supreme Court to allow mass federal layoffs*. CBS News. <https://www.cbsnews.com/news/trump-supreme-court-reductions-in-force-layoffs-federal-workers/>

Reuters. (2025). *Trump revokes Biden executive order addressing AI risks*. Reuters.

<https://www.reuters.com/technology/artificial-intelligence/trump-revokes-biden-executive-order-addressing-ai-risks-2025-01-21/>

Robertson, A. (2023, February 16). *The Supreme Court could be about to decide the legal fate of AI search*. The Verge. <https://www.theverge.com/2023/2/16/23591290/supreme-court-section-230-gonzalez-google-bard-bing-ai-search-algorithms>

Rubado, M. E., & Jennings, J. T. (2019). Political consequences of the endangered local watchdog: Newspaper decline and mayoral elections in the United States. *Urban Affairs Review, 56*(5), 1327–1356. <https://doi.org/10.1177/1078087419838>

Seo.ai. (n.d.). *How many people use Google?* <https://seo.ai/blog/how-many-people-use-google>

Shearer, E. (2021, January 12). *More than eight-in-ten Americans get news from digital devices*.

Pew Research Center. <https://www.pewresearch.org/fact-tank/2021/01/12/more-than-eight-in-ten-americans-get-news-from-digital-devices/>

Simpson, E., & Conner, A. (2021, November 16). *How to regulate tech: A technology policy framework for online services*. Center for American Progress.

<https://www.americanprogress.org/article/how-to-regulate-tech-a-technology-policy-framework-for-online-services/>

- Smith, A. (2025, February 21). *Tech experts Trump fired from U.S. watchdog say consumers at risk*. Context. <https://www.context.news/big-tech/tech-experts-trump-fired-from-us-watchdog-say-consumers-at-risk>
- Solon Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104, 671. <https://www.californialawreview.org/wp-content/uploads/2016/06/2Barocas-Selbst.pdf>
- Southerland, V. M. (2021). The intersection of race and algorithmic tools in the criminal legal system, *Maryland Law Review*, 80. <https://digitalcommons.law.umaryland.edu/mlr/vol80/iss3/1>
- Spice, B. (2015, July 7). *Questioning the fairness of targeting ads online*. Carnegie Mellon University News. <https://www.cmu.edu/news/stories/archives/2015/july/online-ads-research.html>
- Srinivasan, D. (2020). Why Google dominates advertising markets: Competition policy should lean on the principles of financial market regulation. *Stanford Technology Law Review*, 24(1), 55–175.
- Stanford University Institute for Human-Centered Artificial Intelligence. (2024). *Rethinking privacy in the AI era: Policy provocations for a data-centric world*. <https://hai.stanford.edu/white-paper-rethinking-privacy-ai-era-policy-provocations-data-centric-world>
- Statista. (2024). Facebook product: Daily active users (DAU). Statista. <https://www.statista.com/statistics/1092227/facebook-product-dau/>
- Steiner, M. (2022, January 13). *The US journalism crisis is a democracy crisis*. Real News Network. <https://therealnews.com/the-us-journalism-crisis-is-a-democracy-crisis>

- Stergiou, C. L., Bompoli, E., & Psannis, K. E. (2023). Security and privacy issues in IoT-based big data cloud systems in a digital twin scenario. *Applied Sciences*, 13(2), 758.  
<https://doi.org/10.3390/app13020758>
- Stoller, M. (2019, October 17). Tech companies are destroying democracy and the free press. *New York Times*. <https://www.nytimes.com/2019/10/17/opinion/tech-monopoly-democracy-journalism.html>
- Susser, D., Roessler, B., & Nissenbaum, H. (2019). Technology, autonomy, and manipulation. *Internet Policy Review*, 8(2). <https://doi.org/10.14763/2019.2.1410>
- Sustainability Magazine. (2023, March 27). *The real cost of Meta, Google, Microsoft's AI investments*. Sustainability Magazine. <https://sustainabilitymag.com/articles/the-real-cost-of-meta-google-microsofts-ai-investments>
- Tiku, N. (2023, July 13). *FTC investigates OpenAI's ChatGPT over data privacy concerns*. The Washington Post. <https://www.washingtonpost.com/technology/2023/07/13/ftc-openai-chatgpt-sam-altman-lina-khan/>
- The Guardian. (2024, February 22). Google pauses AI-generated images of people after ethnicity criticism. The Guardian. <https://www.theguardian.com/technology/2024/feb/22/google-pauses-ai-generated-images-of-people-after-ethnicity-criticism>
- Trittin-Ulbrich, Scherer, A. G., Munro, I., & Whelan, G. (2021). Exploring the dark and unexpected sides of digitalization: Toward a critical agenda. *Organization*, 28(1), 8–25.
- U.S. Department of Justice (2020, October 20). Justice Department sues monopolist Google for violating antitrust laws. <https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws>

- U.S. Department of Labor. (2024, April 5). *OFCCP issues new guidance on AI and discrimination in hiring practices*.  
<https://www.dol.gov/newsroom/releases/ofccp/ofccp20240405>
- Verma, P. (2022, July 15). The never-ending quest to predict crime using AI. *Washington Post*.  
<https://www.washingtonpost.com/technology/2022/07/15/predictive-policing-algorithms-fail/>
- Vlasceanu, M., & Amodio, D. M. (2022). Propagation of societal gender inequality by internet search algorithms. *Proceedings of the National Academy of Sciences*, 119(29), 1–8.  
<https://doi.org/10.1073/pnas.2204529119>
- Waelen R., & Wiczorek, M. (2022). The struggle for AI's recognition: Understanding the normative implications of gender bias in AI with Honneth's theory of recognition. *Philosophy & Technology*, 35(53), 2–17. <https://doi.org/10.1007/s13347-022-00548-w>
- Wang, D. H., Chen, P., Yu, T. H., & Hsiao, C. (2015). The effects of corporate social responsibility on brand equity and firm performance. *Journal of Business Research*, 68, 2232–2236. <http://dx.doi.org/10.1016/j.jbusres.2015.06.003>
- Warren, T. (2022, January 28). Apple says it now has 1.8 billion active devices globally. The Verge. <https://www.theverge.com/2022/1/28/22906071/apple-1-8-billion-active-devices-stats>
- West, D. M. (2024). *One year later: How has the White House AI executive order delivered on its promises?* Brookings. <https://www.brookings.edu/articles/one-year-later-how-has-the-white-house-ai-executive-order-delivered-on-its-promises/>
- Wiggers, K. (2024, February 15). *GDPR, EU AI Act will overlap as businesses face enforcement*. TechTarget. <https://www.techtarget.com/searchcio/news/366579860/GDPR-EU-AI-Act-will-overlap-as-businesses-face-enforcement>

Morrison, S. (2023, July 27). *AI companies want your data. There's not much you can do about it.* Vox. <https://www.vox.com/technology/2023/7/27/23808499/ai-openai-google-meta-data-privacy-nope>

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* Public Affairs.

Zuboff (2021, February 19). *How surveillance capitalism is undermining democracy.* PBS. <https://www.pbs.org/wnet/amanpour-and-company/video/how-surveillance-capitalism-is-undermining-democracy/>