CENTER FOR DATA INNOVATION

Picking the Right Policy Solutions for AI Concerns

By Hodan Omaar and Daniel Castro | May 20, 2024

INTRODUCTION

Policymakers find themselves amid a chorus of calls demanding that they act swiftly to address risks from artificial intelligence (AI). Concerns span a spectrum of social and economic issues, from AI displacing workers and fueling misinformation to threatening privacy, fundamental rights, and even human civilization. Some concerns are legitimate, but others are not. Some require immediate regulatory responses, but many do not. And a few require regulations addressing AI specifically, but most do not. Discerning which concerns merit responses and what types of policy action they warrant is necessary to craft targeted, impactful, and effective policies to address the real challenges AI poses while avoiding unnecessary regulatory burdens that will stifle innovation.

This report covers 28 of the prevailing concerns about AI, and for each one, describes the nature of the concern, if and how the concern is unique to AI, and what kind of policy response, if any, is appropriate. To be sure, there are additional concerns that could have been included and others that will be raised in the future, but from a review of the literature on AI and the growing corpus of AI regulatory actions, these are the major concerns that policymakers have to contend with. This report takes 28 of the concerns du jour and groups them into 8 sections: privacy, workforce, society, consumers, markets, catastrophic scenarios, intellectual property, and safety and security. Each concern could warrant a report of its own, but the goal here is to distill the essence of each concern and offer a pragmatic, clear-eyed response.

For each issue, we categorize the appropriate policy response as follows:

Pursue Regulation That Is…

AI-specific: Some concerns about AI are best addressed by enacting or updating regulation that specifically targets AI systems. These regulations may prohibit certain types of AI systems, create or expand regulatory oversight of AI systems, or impose obligations on the developers and operators of AI systems, such as requiring audits, information disclosures, or impact assessments.

General: Some concerns about AI are best addressed by enacting or updating regulation that does not specifically target AI but instead creates broad legal frameworks that apply across various industries and sectors. Examples of these regulations include data privacy laws, political advertising laws, and revenge porn laws.

Pursue Nonregulatory Policies That Are…

AI-specific: Some concerns about AI are best addressed by implementing nonregulatory policies that target AI. Examples of these policies include funding AI research and development or supporting the development and use of AI-specific industry standards.

General: Some concerns about AI are best addressed by implementing nonregulatory policies that do not target AI but instead focus on the broader technological and societal context in which AI systems operate. Examples of these policies include job dislocation policies to mitigate the risks of a more turbulent labor market or policies to improve federal data quality.

No Policy Needed

Some concerns are best addressed by existing policies or by allowing society and markets to adapt over time. Policymakers do not need to implement new regulatory or nonregulatory policies at this time.

CONTENTS

OVERVIEW OF POLICY NEEDS FOR AI CONCERNS

- **Concerns that warrant AI-specific regulations:**

  1.3. AI may enable government surveillance.

  3.6. AI may make harmful decisions.

  8.1. AI may enable fraud and identity theft.

  8.3. AI may create safety risks.

- **Concerns that warrant general regulations:**

  1.1. AI may expose PII in a data breach.

  1.5. AI may infer sensitive information.

  1.6. AI may help bad actors harass and publicly shame individuals.

  3.2. AI may fuel deepfakes in elections.

  6.1. AI may make it easier to build bioweapons.

  7.3. AI may infringe on publicity rights.

- **Concerns that warrant AI-specific nonregulatory policies:**

  1.4. AI may enable workplace surveillance.

  3.3. AI may manipulate voters.

  3.5. AI may perpetuate discrimination.

  6.2. AI may create novel biothreats.

  6.3. AI may become God-like and "superintelligent."

  6.4. AI may cause energy use to spiral out of control.

  7.1. AI may unlawfully train on copyrighted content.

  8.2. AI may enable cyberattacks.

- **Concerns that warrant general nonregulatory policies:**

  1.2. AI may reveal PII included in training data.

  2.2. AI may dislocate blue collar workers.

  2.3. AI may dislocate white collar workers.

  3.1. AI may have political biases.

  7.2. AI may create infringing content.

- **Concerns that do not warrant new policies:**

  2.1. AI may cause mass unemployment.

  3.4. AI may fuel unhealthy personal attachments.

  4.1. AI may exacerbate surveillance capitalism.

  5.1. AI may enable firms with key inputs to control the market.

  5.2. AI may reinforce tech monopolies.

1. PRIVACY

#	Risk	Policy needs	Policy solution
1.1	AI may expose personally identifiably information in a data breach.	General regulations	Policymakers should require companies to publish security policies to promote transparency with consumers. Congress should pass federal data breach notification legislation.
1.2	AI may reveal sensitive information included in training data.	General nonregulatory policies	Policymakers should fund research for privacy- and security-enhancing technologies and there should be support for industry-led standards for responsible web-scraping.
1.3	AI may enable government surveillance.	AI-specific regulations	Congress should direct the Department of Justice (DOJ) to establish guidelines for use by state and local law enforcement in investigations that outline specific use cases and capabilities, including when a warrant is necessary for use, as well as transparency guidelines for when to notify the public of law enforcement using AI.
1.4	AI may enable workplace surveillance.	AI-specific nonregulatory policy	Policymakers should help set the quality and performance standards of AI technologies used in the workplace
1.5	AI may infer sensitive information.	General regulations	Policymakers should craft and enact comprehensive national privacy legislation that addresses the risks of data-driven inference in a tech-neutral way.
1.6	AI may help bad actors harass and publicly shame individuals.	General regulations	Congress should outlaw the nonconsensual distribution of all sexually explicit images, including deepfakes that duplicate individuals' likenesses in sexually explicit images, and create a federal statute that prohibits revenge porn, including those with computer-generated images.

○ AI-specific regulation
● **General regulation**
○ AI-specific nonregulatory policy
○ General nonregulatory policy
○ No policy needed

Issue 1.1: AI May Expose Personal Information in a Data Breach

The issue: Data breaches occur when someone gains unauthorized access to data. For instance, an attacker might circumvent security measures to obtain sensitive data, or an insider might inappropriately access confidential information. Users may share personally identifiable information (PII) with AI systems, such as chatbots, offering legal, financial, or health services. In the event of a data breach, the transcripts of these conversations could be exposed and accessed improperly, revealing sensitive information. An example of a data breach is a much-reported incident that occurred with OpenAI's ChatGPT chatbot in March 2023. Due to a bug in an open-source library the system uses, some users were able to see titles from other users' chat histories.[1]

While it is true that AI systems could be subject to data breaches, just like any IT system, they have not created or exacerbated the underlying privacy and security risks. Data breaches have been an unfortunate, yet regular, occurrence for the past two decades. In 2022, there were nearly 1,800 data breaches in the United States impacting hundreds of millions of Americans.[2]

The solution: Policymakers should address the larger problem of data breaches rather than focus exclusively on data breaches involving AI systems. One thing Congress can do is require companies to publish security policies to promote transparency with consumers. Most companies publish privacy policies, which create a transparent and accountable mechanism for regulators to ensure companies are adhering to their stated policies. But no such practice exists for information security practices, which has resulted in vague standards, regulation by buzzword, and information asymmetry in markets. By publishing security policies, companies would be motivated to describe the types of security measures they have in place rather than just make claims of taking "reasonable security measures." This is a concrete step that policymakers can take to improve security practices in the private sector.[3]

Moreover, Congress should pass data breach notification legislation that preempts conflicting state laws.[4] All 50 states, as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, have data breach laws; however, each jurisdiction has its own set of rules on how quickly to report a data breach or to whom a security incident should be reported. This patchwork quilt of differing requirements provides decidedly uneven protection for consumers and creates an unnecessarily complex situation for companies, which must spend more time navigating this murky legal terrain than actually protecting consumer data.[5]

○ AI-specific regulation
○ General regulation
○ AI-specific nonregulatory policy
● **General nonregulatory policy**
○ No policy needed

Issue 1.2: AI May Reveal Personal Information Included in Training Data

The issue: Data leaks occur when AI systems reveal private information included in training data. For example, an AI model trained on confidential user data, such as private contracts or medical records, may unintentionally reveal this private information to users. A case in point was the incident wherein popular chatbot ChatGPT appeared to reveal some of the bits of data it had been trained on when researchers prompted it to repeat random words forever.[6] Similarly, AI systems may disclose private information when it is inadvertently included in training data, such as personal information scraped from public websites.[7]

While data leaks are a legitimate privacy concern, they are not unique to AI. Data leaks were an early concern about search engines too, as attackers could use search engines to discover a trove of sensitive data, such as credit card information, Social Security numbers, and passwords, that was scattered across the Internet, often without the affected individuals' awareness.[8] Internet search engines also widely deploy web crawlers, which are automated programs that index the content of webpages, and to address risks in this area in the past, nongovernment solutions to the risks posed by the scraping of publicly available data have been successful.

The solution: Policymakers can help minimize or eliminate the need for AI-enabled services to process confidential data while still maintaining the benefits of those services by investing in research for privacy- and security-enhancing technologies. These are not specific to AI, but they will have important uses for AI. For instance, policymakers should support additional research on topics such as secure multiparty computation, homomorphic encryption, differential privacy, federated learning, zero-trust architecture, and synthetic data.[9] They should also fund research exploring the use of "data privacy vaults" to isolate and protect sensitive data in AI systems.[10] In this scenario, any PII would be replaced with deidentified data so that large language models (LLMs) would not have access to any sensitive data, thereby preventing data leaks during training and inference and ensuring only authorized users could access the PII. Regarding AI systems that scrape publicly available data, policymakers should support the already burgeoning set of industry-led standards for web scraping.[11] The private sector is already taking steps to give website operators more control over whether AI web crawlers scrape their sites.[12] Indeed, many websites can use the existing Robots Exclusion Protocol to restrict web crawlers from popular AI companies.

There may be instances when PII ends up on public websites that AI systems scrape and consumers don't want this information there. Federal data privacy legislation would create a baseline set of consumer rights for how organizations collect and use personal data. This legislation should preempt state laws, ensure reliable enforcement, streamline regulation, and minimize the impact on innovation.[13]

● **AI-specific regulation**
○ General regulation
○ AI-specific nonregulatory policy
○ General nonregulatory policy
○ No policy needed

Issue 1.3: AI May Enable Government Surveillance

The issue: AI makes it easier to analyze large volumes of data, including about individuals, which may lead to increased government surveillance. For instance, governments can track individuals in public spaces, such as through facial recognition technology, or infer sensitive information about individuals based on less-sensitive data.

There can be legitimate reasons for this concern. Governments in certain countries have disturbing histories of intruding into the private lives of their citizens and many fear that they may revert to this type of activity in the future. And some countries, such as China, significantly limit the personal freedoms of their citizens and use surveillance to threaten human rights. Indeed, critics point out that China uses AI-enabled tracking and emotion-recognition technology as part of its domestic surveillance activities, most notably against its Uyghur population, and argue that democratic nations should not use the same technology.[14] They fear a slippery slope wherein Western governments might exploit AI for nefarious purposes that trample on citizens' basic rights.

The solution: Law enforcement agencies should take preemptive steps to recognize the potential impacts of AI on perceptions of acceptable government use of technology for law enforcement activities. Congress should direct DOJ to establish guidelines for use by state and local law enforcement in investigations that outline specific use cases and capabilities, including when a warrant is necessary for use, as well as transparency guidelines for when and how to notify the public of AI use by law enforcement officials. The Facial Recognition Technology Warrant Act introduced in 2019, which requires federal law enforcement to obtain a court order before using facial recognition technology to conduct targeted ongoing public surveillance of an individual, could serve as a useful model to establish limitations on use, legal requirements for appropriate use, transparency, and approval processes for other AI-enabled law enforcement technologies.[15] In addition, as new AI products for law enforcement become available, they should undergo a predeployment review to ensure they meet First and Fourth Amendment protection standards, just as any new technology should. Such assessments should be conducted by federal officials familiar with existing legal requirements and potential applications. DOJ should also conduct independent testing of police tech, as the National Institute of Standards and Technology (NIST) has done for facial recognition algorithms during its Face Recognition Vendor Test, to ensure the technology is accurate and unbiased.[16] The General Services Administration (GSA) should establish guidelines to assist agencies in complying with existing government-wide privacy requirements when implementing AI solutions. These guidelines should address different government use cases, including for training, service provision, and research.

○ AI-specific regulation
○ General regulation
● **AI-specific nonregulatory policy**
○ General nonregulatory policy
○ No policy needed

Issue 1.4: AI May Enable Workplace Surveillance

The issue: One concern about the use of AI in the workplace is that employee monitoring may become unduly invasive, stemming in part from the fact that workers may not know how or when their employers are using the technology. For instance, the Trades Union Congress (TUC), a national trade union center representing 48 unions across the United Kingdom, published a report in 2020 that finds that 50 percent of U.K. employees believe their companies may be using AI systems they are not aware of.[17] A more complex concern is that the data AI systems collect can reveal or enable employers to infer information with varying sensitivity levels, which, if misused, risks autonomy violations. Consider an AI system with eye-tracking technologies, which monitors the behavior of delivery drivers by tracking their gaze patterns. Many studies have found that people with autism react differently to stimuli when driving so an employer may infer from eye-tracking AI software which drivers have autism, even though employees may want to keep this information private.[18]

However, as a general rule, employees in the United States have little expectation of privacy while on company grounds or using company equipment, including company computers or vehicles, according to judicial rulings by U.S. courts and existing federal laws.[19] Addressing AI surveillance concerns with AI-specific regulation would not align with the current legal framework for employee privacy and therefore any legal reforms should address employee privacy expectations more broadly.

The solution: Policymakers should support the responsible adoption of AI in the workplace, including by helping set the quality and performance standards of AI technologies used in the workplace.[20] For instance, they should fund independent testing of commercial systems that measure behaviors and performance of employees, much like the U.S. Department of Commerce did when it launched a multistakeholder process for commercial use of facial recognition, and in June 2016, a group of stakeholders reached a consensus on a set of best practices that offered guidelines for protecting consumer privacy.[21] Doing so would help fill knowledge gaps ranging from the accuracy of different workplace tools to the efficacy of these tools to the potential uses of these technologies in specific workforce-related applications.

Additionally, the Equal Employment Opportunity Commission (EEOC) should investigate the potential autonomy violations from processing employee data as part of its AI and algorithmic fairness initiative. There Is currently no comprehensive understanding of the adoption, design, and impact of AI tools that process employee data.[22] The EEOC's agency-wide initiative currently focuses on potential harms from bias and discrimination, but the work it is doing to hold listening sessions with key stakeholders about algorithmic tools and their employment ramifications would be valuable for gaining insights from potential autonomy violations.

○ AI-specific regulation
● **General regulation**
○ AI-specific nonregulatory policy
○ General nonregulatory policy
○ No policy needed

Issue 1.5: AI May Infer Sensitive Information

The issue: AI can infer information about people's identities, habits, beliefs, preferences, and medical conditions, including information that individuals may not know themselves based on other data about those individuals. AI systems can use computational techniques, such as machine learning, to make data-driven inferences. For instance, an AI system may be able to detect rare genetic conditions from an image of a child's face, or AI-enabled online advertising may infer information about users, such as predicting their age or political leanings based on their online activity. Disclosure of such information without a user's consent or knowledge can lead to significant reputational harm or embarrassment socially, politically, or professionally when the nature of the inferred information is particularly sensitive or highly personal. While data-driven inferences may present novel risks, these types of inferences can also occur in the absence of AI systems using standard statistical methods.

The solution: Policymakers should craft and enact comprehensive national privacy legislation that addresses the risks of data-driven inference in a tech-neutral way. This would better position regulators and developers alike to ensure necessary safeguards are consistently implemented as these technologies continue to evolve.[23] Policymakers should enact privacy legislation that establishes clear guidelines for the collection, processing, and sharing of various types of data with consideration for varying levels of sensitivity; implements user data privacy rights and safeguards against risks of harm; and strengthens notice, transparency, and consent practices to ensure users can make informed decisions about the data they choose to share, including sensitive biometric and biometrically derived information.

Because biometric information is central to many emerging tech use cases and has inference-related risks, any privacy regulations should include clear definitions of biometric identifying and biometrically derived data and present transparency, consent, and choice requirements consistent with the purpose of its collection and risks of harm.

The relevant federal agencies and regulatory bodies that oversee existing privacy regulations should also provide explicit guidance on their application for any new questions arising from AI. For example, the Department of Health and Human Services could offer guidance on when predictions made by AI systems constitute "protected health information" under HIPAA (the Health Insurance Portability and Accountability Act).

○ AI-specific regulation
● **General regulation**
○ AI-specific nonregulatory policy
○ General nonregulatory policy
○ No policy needed

Issue 1.6: AI May Help Bad Actors Harass and Publicly Shame Individuals

The issue: AI makes it easier to create fake images, audio, and videos of individuals, which can be used to harass them and harm their personal and professional reputations. Deepfakes, a portmanteau of "deep learning" and "fake," have been around since the end of 2017, created mostly by people editing the faces of celebrities into pornography. As with all types of nonconsensual pornography, deepfake revenge porn that portrays an individual in a sexual situation that never actually happened can have devastating consequences for victims' lives and livelihoods. More recently, deepfakes have raised risks for noncelebrities too. In one recent case, students at a New Jersey high school allegedly used AI image generators to produce fake nude images of their female classmates.[24] Deepfakes present a unique challenge, as they can fool both humans and computers, which makes it difficult to moderate this content.

While the private sector is taking this concern seriously, and companies such as Google, Adobe, and Meta have announced significant partnerships with academic researchers to explore technical solutions, current deepfake detection technologies such as digital watermarks, embedding metadata, and uploading media to a public blockchain have limited effectiveness.[25] This makes non-technical solutions focused on limiting the spread of deepfakes key.

The solution: Policymakers should implement policies that seek to stop the distribution of this content. There is currently no federal law criminalizing nonconsensual pornography, though such laws exist in 48 states and the District of Columbia and the Violence Against Women Act Reauthorization Act of 2022 allows victims of nonconsensual pornography to sue for damages in federal court.[26] Additionally, 16 states have laws addressing deepfakes.[27] Congress should outlaw the nonconsensual distribution of all sexually explicit images, including deepfakes that duplicate individuals' likenesses in sexually explicit images, and also create a special unit in the Federal Bureau of Investigation (FBI) to provide immediate assistance to victims of actual and deepfake nonconsensual pornography. Moreover, most of the laws criminalizing revenge porn—intimate images and videos of individuals shared online without their permission—do not include computer-generated images and only about a dozen states have updated their laws to close this loophole. Here too Congress has an opportunity to act by creating a federal statute that prohibits such activity. The Preventing Deepfakes of Intimate Images Act introduced in May 2023 would update the Violence Against Women Act to extend civil and criminal liability to anyone who discloses or threatens to disclose digitally created or altered media containing intimate depictions of individuals with the intent to cause them harm or with reckless disregard to potential harm.[28]

2. WORKFORCE

#	Risk	Policy needs	Policy solution
2.1	AI may cause mass unemployment.	No policies needed	Policymakers do not need to focus on concerns about mass unemployment from AI adoption because the economic evidence does not support this materializing.
2.2	AI may dislocate blue collar workers.	General nonregulatory policies	Policymakers should support full employment, nationally and regionally, not just with macro-economic stabilization policies, but also with robust regional economic development policies; ensure as many workers as possible have needed education and skills before they are laid off; reduce the risk of income loss and other financial hardships when workers are laid off; and provide better transition assistance to help laid off workers find new employment.
2.3	AI may dislocate white collar workers.	General nonregulatory policies	Policymakers should ensure that job dislocation policies and programs support all workers whose jobs are impacted by automation so they can train for new jobs. They should also proactively support IT modernization in the public sector, including the adoption of generative AI.

○ AI-specific regulation
○ General regulation
○ AI-specific nonregulatory policy
○ General nonregulatory policy
● **No policy needed**

Issue 2.1: AI May Cause Mass Unemployment

Issue: In a 2023 discussion with British Prime Minister Rishi Sunak, tech entrepreneur Elon Musk predicted that AI would make all jobs obsolete, stating that "you can have a job if you want a job … but the AI will be able to do everything."[29] Some economists, such as Anton Korinek, economics professor at the Darden School of Business at the University of Virginia, share in Musk's belief of a potentially jobless future. In a 2023 testimony before the U.S. Senate, Korinek warned that AI systems, if able to match human cognitive abilities, could lead to the obsolescence of human workers.[30] Korinek further argued that there is about a 10 percent chance AI systems reach artificial general intelligence (AGI) in the near future, which could lead to widespread devaluation of human work in all areas.[31]

However, many concerns about traditional AI leading to mass unemployment are typically based on the "lump of labor fallacy," the idea that there is a fixed amount of work, and thus productivity growth will reduce the number of jobs.[32] The logic goes, if there is a fixed amount of work and workers can now produce twice as much as before, half of the previous workforce becomes jobless. But the data shows this is not the case. Labor productivity has grown steadily for the past century (even if that growth has been slower recently) and unemployment is near an all-time low.[33] AI will likely bring changes to the types of work people do and create disruptions, but the economy has mechanisms and institutions in place to adapt and maintain overall employment levels, as long as policymakers effectively manage these transitions. The challenge of AI is therefore not mass unemployment, but greater levels of worker transition.

The concerns about joblessness from AGI hinge on the existence of AGI, which is a speculative scenario that may take decades or may never fully materialize. There is no scientific consensus saying it will or is likely to.

The solution: Policymakers do not need to focus on concerns about mass unemployment from traditional AI adoption because the economic evidence does not support this materializing.

○ AI-specific regulation
○ General regulation
○ AI-specific nonregulatory policy
● **General nonregulatory policy**
○ No policy needed

Issue 2.2: AI May Displace Blue Collar Workers

The issue: Before the very recent advent of generative AI, concerns about job dislocation centered around AI-enabled automation and robotics. The main concern has been that these technologies will lead to the elimination of certain blue collar jobs because machines can perform repetitive and routine tasks more efficiently than humans, with jobs in industries such as manufacturing, data entry, and customer service being particularly vulnerable.

It is true that AI-enabled automation will eliminate some blue collar jobs, much like earlier general-purpose technologies such as the steam engine or electricity-automated jobs of the past, but the first thing to note is that the current evidence of adoption shows that there is not a tsunami of destruction as some fear. Few companies that have blue collared jobs currently use AI in a significant way. In manufacturing, where the advent of AI can transform how firms design, fabricate, operate, and service products, as well as the operations and processes of manufacturing supply chains, 89 percent of manufacturers report that they are not using AI at all according to a 2022 report from the National Science Foundation (NSF).[34] In key manufacturing industries such as machinery, electronic products, and transportation equipment, less than 7 percent of companies report using AI as a production technology in any capacity. The same is true in nonmanufacturing industries; less than 3 percent of companies in retail trade reported using AI.[35] While these numbers will grow, the rate of adoption, such as all other technologies in the past, is likely to be slow. But more importantly, AI-enabled automation will be a net good if there are policies in place to ensure those who are dislocated transition easily into new jobs and new occupations. AI-enabled automation—indeed all automation—allows workers to be more productive, and more productivity growth is a path to economic and income growth that benefits society. This is because better tools enable companies to produce better products and provide services more efficiently. By boosting productivity, workers can earn more and companies can lower prices, both of which increase living standards.

The solution: Policymakers should ensure that workers are better positioned to navigate a potentially more turbulent, but ultimately beneficial, labor market.[36] Policymakers should support full employment, nationally and regionally, not just with macro-economic stabilization policies but also with robust regional economic development policies; ensure as many workers as possible have needed education and skills before they are laid off; reduce the risk of income loss and other financial hardships when workers are laid off; and provide better transition assistance to help laid off workers find new employment.

○ AI-specific regulation
○ General regulation
○ AI-specific nonregulatory policy
● **General nonregulatory policy**
○ No policy needed

Issue 2.3: AI May Displace White-Collar Workers

The issue: Some people are concerned that generative AI will eliminate white collar jobs. A headline from *The New York Times* in August 2023 encapsulates this sentiment: "In Reversal Because of A.I., Office Jobs Are Now More at Risk."[37]

But policymakers should not mistake technical feasibility for economic viability.[38] Just because a job is exposed to LLM automation, doesn't determine whether the technology is likely to replace white collar workers or merely augment their skills.[39] Tools such as ChatGPT might be able to draft a legal document in half the time a human legal secretary can, but that doesn't necessarily mean law firms can or should substitute their staff in favor of LLMs, as these tools are still at a stage where they can misrepresent key facts and cite evidence that doesn't exist; they still need humans to verify and check their outputs. Instead, AI can revalorize the jobs still performed best by humans such as nursing and teaching, making people's skills more valuable and supplement a diminishing workforce.[40] David Autor, an economics professor at Massachusetts Institute of Technology (MIT) who has spent his career exploring how technological change affects jobs, wages, and inequality, underscored this point, when he wrote that "the unique opportunity that AI offers to the labor market is to extend the relevance, reach, and value of human expertise."[41] Moreover, other MIT researchers published a recent paper examining the productivity effects of ChatGPT on mid-level professional writing tasks and found that using the chatbot not only increased productivity but job satisfaction too.[42]

The solution: Policymakers should ensure that job dislocation policies and programs support all workers whose jobs are impacted by automation so they can train for new jobs, including through regional economic development policies, skills retraining policies, and transition assistance policies.

Policymakers should also proactively support the IT modernization in white collar roles in the public sector, including the adoption of generative AI, to ensure workers reap the productivity, efficiency, and societal gains. The federal government struggles with a variety of challenges, such as slow services and backlogs, significant administrative burden and bureaucratic processes, and impending budget constraints. Taking advantage of new tools at their disposal, including generative AI, will boost mission delivery and help reduce the perceived risk of the technology and boost domestic demand for AI.[43]

3. SOCIETY

#	Risk	Policy needs	Policy solution
3.1	AI may have political biases.	General nonregulatory policy	Policymakers should treat chatbots like the news media, which is subject to market forces and public scrutiny, but is not directly regulated by the government when it comes to expressing political perspectives.
3.2	AI may fuel deepfakes in elections.	General regulation	Policymakers should update state election laws to make it unlawful for campaigns and other political organizations to knowingly distribute materially deceptive media.
3.3	AI may manipulate voters.	AI-specific nonregulatory policy	Policymakers should update digital literacy programs to include AI literacy, which teaches individuals to understand and use AI-enabled technologies.
3.4	AI may fuel unhealthy personal attachments.	No policy needed	Not enough evidence of impacts to society yet.
3.5	AI may perpetuate discrimination.	AI-specific nonregulatory policy	Policymakers should support the development of tools that help organizations provide structured disclosures about AI models and related data.
3.6	AI may make harmful decisions.	AI-specific regulation	Policymakers should consider prohibiting the government from using AI systems in certain high-risk, public sector contexts. They should upskill regulators with better AI expertise and develop tools to monitor and address sector-specific AI risks, as the United Kingdom has done.

○ AI-specific regulation
○ General regulation
● **AI-specific nonregulatory policy**
○ General nonregulatory policy
○ No policy needed

Issue 3.1: AI May Have Political Biases

The issue: Both sides of the aisle accuse AI companies of designing tools that reflect the partisan views of the leadership of the companies. The most pervasive concerns come from conservatives who argue generative AI systems display a liberal bias, and cite plenty of anecdotal evidence to back up their claims. One of the most oft-reported anecdotes in early 2023 was a claim made on microblogging site X that said ChatGPT wrote an ode to President Biden when prompted but declined to write a similar poem about former President Donald Trump.[44] More recently, Google decided to block the ability of its AI image generator Gemini from generating images of people after it was criticized for depicting specific white figures, such as the U.S. Founding Fathers or German soldiers, as people of color.[45]

However, there is limited academic research into whether generative AI systems display anti-conservative bias, and some of the research supporting concerns of anti-conservative biases have been heavily critiqued. For instance, when the prompts from a paper published in the social science journal *Public Choice* found that ChatGPT was more predisposed to answer in ways that aligned with liberal parties internationally were replicated in a different order by other researchers, ChatGPT exhibited bias in the opposite direction, in favor of Republicans.[46] That is not to say chatbots may not exhibit political biases. They very well might lean toward certain ideologies or orientations in their answers either intentionally or inadvertently, but it would be impossible to build an "unbiased" chatbot because bias itself is relative—what one person considers neutral, another might not.[47] Some bias in generative AI systems may be the unintentional result of attempts to implement technical safeguards. Google's AI generator, for instance, was designed to maximize diversity in an effort to subvert the system from amplifying racial and gender stereotypes but resulted in an overcorrection.[48]

The solution: First amendment protections place limits on what policymakers can do to regulate AI chatbots' answers on political speech. The best course of action is for policymakers to treat chatbots like the news media, which is subject to market forces and public scrutiny but is not directly regulated by the government when it comes to expressing political perspectives.[49] The availability of open source AI models means people of all political backgrounds can create their own custom AI models and evaluate potential biases in their responses. Independent third-party testers can also evaluate proprietary chatbots to see the extent to which they are biased, much like media watchdog organizations scrutinize the news media. For instance, in January 2023, a team of researchers at the Technical University of Munich and the University of Hamburg posted a preprint of an academic paper explaining how they had prompted ChatGPT with 630 political statements and claimed to uncover the chatbot's "pre-environmental, left-libertarian ideology."[50] Policymakers can foster oversight and accountability by funding more research into how to measure political bias in AI models through NSF.

○ AI-specific regulation
● **General regulation**
○ AI-specific nonregulatory policy
○ General nonregulatory policy
○ No policy needed

Issue 3.2: AI May Fuel Deepfakes in Elections

The issue: Individuals or organizations seeking to influence elections, including foreign adversaries, may exploit advances in generative AI to create realistic media that appears to show people doing or saying things that never happened—a type of media commonly referred to as "deepfakes." Deepfakes have the potential to influence elections. For example, voters may believe false information about candidates based on fake videos that depict them making offensive statements they never made, thus hurting their electoral prospects. Similarly, a candidate's reputation could be harmed by deepfakes that use other people's likeness, such as a fake video showing a controversial figure falsely supporting that candidate.[51] For example, in June 2023, Florida Governor Ron DeSantis's campaign shared an attack ad showing fake AI-generated images of his primary opponent former President Donald Trump hugging former health official expert Dr. Anthony Fauci. [52] Finally, if deepfakes become commonplace in elections, voters may simply no longer believe their own eyes and ears, and they may distrust legitimate digital media showing a candidate's true past statements or behaviors.

Policymakers are rightfully concerned that bad actors will exploit advances in generative AI to influence elections. The public and private sectors have already launched multiple initiatives to create technical solutions to address deepfakes, including research to identify fake content and developing standards to improve attribution for authentic content.[53] But focusing exclusively on technical interventions, as many proposed legislative bills seek to do, will not comprehensively address the risk—though some technical interventions are worthwhile.

The solution: State lawmakers should update state election laws to make it unlawful for campaigns and other political organizations to knowingly distribute materially deceptive media that uses a person's likeness to injure a candidate's reputation or manipulate voters into voting against that candidate without a clear and conspicuous disclosure that the content they are viewing is fake. Such a requirement would prevent, for example, an opposing campaign from running advertisements using deepfakes without full transparency to potential voters that the media is fake. This transparency requirement should apply to all deceptive media in elections, regardless of whether it is produced with AI. State election laws should focus on setting rules for political organizations that create and share deepfakes, not on the intermediaries, such as email providers, streaming video providers, or social media networks, used by political operatives to share this content.[54] Policymakers should pair these rules with effective enforcement mechanisms. Otherwise, a campaign could spread deepfakes about an opponent a few days before an election knowing that no oversight and consequences would occur until after people had voted.[55]

○ AI-specific regulation
○ General regulation
● **AI-specific nonregulatory policy**
○ General nonregulatory policy
○ No policy needed

Issue 3.3: AI May Manipulate Voters

The issue: AI is changing how candidates for elected office conduct their campaigns. In 2023, there were a smattering of examples of generative AI being used in U.S. political ads, raising concerns that AI-driven political persuasion could lead to the dissemination of manipulative content. The Democratic Party tested the use of generative AI tools to write first drafts of some fundraising messages in March 2023.[55] Some worry that political operatives could use AI to craft personalized messages to manipulate voters at scale with targeted disinformation.[56] For example, campaigns could flood voters' social media feeds with AI-created political propaganda designed around their interests. However, while AI may make this problem more acute, the core of the issue is electoral harms from deceptive political outreach and advertising, not specific technologies.

The solution: First amendment protections place limits on what policymakers can do. The best course of action at this time is for policymakers to update digital literacy programs to include AI literacy.[57] AI literacy teaches individuals to understand and use AI-enabled technologies. Whereas existing digital literacy programs might teach individuals how to use a search engine effectively, how to evaluate different sources, and how to interpret statistics, AI literacy would help individuals understand how to spot deepfakes and whether to verify the results of a ChatGPT prompt are necessarily factual or not.

Furthermore, there are existing federal laws against fraudulent misrepresentation in campaign communications and existing federal civil rights laws that prohibit the use of misinformation to deprive people of their right to vote.[58] DOJ and states' attorneys general should commit to enforcing existing civil rights protections related to the electoral process for AI—just as U.S. law-enforcement agencies committed to enforcing existing laws for civil rights, fair competition, consumer protection, and equal opportunity to AI systems in early 2023.[59] Congress and state policymakers should support these efforts by allocating funding for law enforcement to explore how best to safeguard the electoral process in new technological contexts.

○ AI-specific regulation
○ General regulation
○ AI-specific nonregulatory policy
○ General nonregulatory policy
● **No policy needed**

Issue 3.4: AI May Fuel Unhealthy Personal Attachments

The issue: AI companions, which are AI systems designed to interact with humans in a way that mimics companionship or friendship in the form of chatbots, virtual assistants, or even physical robots, are raising concerns about isolation and the formation of unrealistic societal expectations. Some experts are concerned that relying on AI companions may hinder individuals from forming genuine human relationships, leading to increased social isolation. This isolation could have negative effects on mental health and well-being.[60] Other experts, such as Dorothy Leidner, who teaches business ethics at the University of Virginia, worry that the idealized representations in physical appearance and emotional responses that AI companions present could lead to a distorted perception of what is considered normal or desirable in human interactions, impacting broader cultural expectations in relationships and behavior.[61]

Speculating about the role of AI in loneliness is not surprising, as a *Washington Post* series on technology and loneliness states that "one of our national pastimes is guessing who or what is responsible for loneliness, the ancient human condition. Is it social media? Remote work? The nuclear family? Not enough sidewalks?"[62] But the question of whether any technology, including AI, impacts loneliness is too broad and lacks the necessary nuance to understand its specific effects. It's crucial to consider specific types of technology, who is using them, and their purposes. For instance, a 2023 study from Stanford University researchers finds that about 50 percent of older adults believe using virtual reality (VR) alongside their caregivers is "very or extremely" beneficial to their relationship.[63] Meanwhile, social media apps such as TikTok have become a resource for parents to discuss loneliness, online dating apps have become the most common way romantic couples meet, and friend-making apps are becoming a boon for young adults.

The solution: AI companions are not inherently detrimental to social well-being. Policymakers should recognize the diverse ways in which this technology could impact loneliness and social connections. There is little to no research on which segments of society are using AI companions and for what purposes, and therefore, to get enough of a sense of the impacts to society yet. Without sufficient data to understand the full scope of impacts on society, policymakers should exercise caution in their approach, lest they inadvertently hinder unforeseen benefits.

○ AI-specific regulation
○ General regulation
● **AI-specific nonregulatory policy**
○ General nonregulatory policy
○ No policy needed

Issue 3.5: AI May Perpetuate Discrimination

The issue: A concern about AI systems is that they may mirror and amplify existing biases and discrimination in society, leading to unfair and unjust outcomes. Biased algorithms may produce results or decisions that systemically treat certain individuals less favorably than similarly situated individuals due to a protected characteristic such as their race, sex, religion, disability, or age.[64] There have long been calls for policymakers to mitigate these risks by requiring algorithmic transparency, explainability, or both; or to create a master regulatory body to oversee algorithms.

While the concern of biased AI is legitimate, U.S. regulators have acknowledged that existing civil rights laws apply to AI systems and new authorities are not necessary to effectively oversee the use of this technology at this time.[65] Many new regulatory solutions proposed thus far would be inadequate. Some are impractical, such as those that would require audits for all high-risk AI systems because the ecosystem for AI audits is still immature, while some others stifle innovation, such as by prohibiting the use of algorithms that cannot explain their decision-making—despite being more accurate than those that can.[66]

The solution: Policymakers should focus on supporting the development of tools, which would help organizations provide structured disclosures about AI models and related data to bolster much-needed information flows along the AI value chain that could identify and remedy harmful bias and generally foster AI accountability.[67] The National Telecommunications and Information Administration's (NTIA's) AI Accountability Report in 2024 rightly recommends that federal agencies improve standard information disclosures using artifacts such as datasheets, model cards, system cards, technical reports, and data nutritional labels.[68] Policymakers should also help mitigate issues of bias emanating from source data by mandating specific data for AI training, as some countries have proposed, although doing so is problematic and typically at odds with the technical realities faced by AI developers. At the same time, policymakers should proactively improve datasets by ensuring the fair and equitable representation and use of data for all Americans, including improving federal data quality by developing targeted outreach programs for underrepresented communities; enhancing data quality for non-government data; directing federal agencies to update or establish data strategies to ensure data collection is integrated into diverse communities; and amending the Federal Data Strategy to identify data divides and direct agency action.[69] Federal agencies should support the development of best practices for dataset labeling and annotation, and aid the development of high-quality, application-specific training and validation data in sensitive and high-value contexts, such as in healthcare and transportation.

Issue 3.6: AI May Make Harmful Decisions

● **AI-specific regulation**
○ General regulation
○ AI-specific nonregulatory policy
○ General nonregulatory policy
○ No policy needed

The issue: As the public and private sectors increasingly rely on algorithms in high-impact sectors such as consumer finance and criminal justice, a flawed algorithm may potentially cause harm at higher rates. When these algorithms make mistakes, the sheer volume of their decisions could end up significantly amplifying the potential negative impact of these flaws. Consider a human decision-maker at a bank evaluating loan applications. Their output is only a handful of loan applications per week, routinely making errors while evaluating them. However, a flawed algorithm misevaluating hundreds of loan applications per week across an entire bank branch would clearly cause harm on a much larger scale.

In many cases, flawed algorithms hurt the organization using them. Banks making loans would be motivated to ensure their algorithms are accurate because, by definition, errors such as granting a loan to someone who should not receive one or not granting a loan to someone who is qualified costs banks money. However, using an AI system to make decisions in certain contexts may introduce more potential for harm when multiple entities use the same ones, even if an algorithmic tool is more accurate than human evaluators and less error prone than other tools on the market.[70] This is somewhat analogous to monoculture in agriculture, wherein a lack of diversity in crops can make the entire system vulnerable to widespread failures. For example, imagine multiple banks using the same algorithmic model to screen and assess loan applications. Even though it might be rational for each bank in isolation to adopt an algorithm, accuracy can become lower than using human evaluators when multiple entities use the same one. While this seems counterintuitive, the potential for this result derives from how probabilistic properties of rankings work. The key thing is, in some contexts, independence may be more important than accuracy for reducing errors. That said, algorithmic monoculture could be desirable in some settings. It may be the case that in other high-risk areas, multiple decision-makers using a single centralized algorithmic system may reduce errors. In education, for instance, economists have found outcomes have improved as algorithms for school assignment have become more centralized.[71] Perhaps in healthcare, the allocation of scarce resources by different hospitals would be best done if they all used the same algorithmic systems. Perhaps not. It isn’t known because it has not been studied yet.

The solution: Policymakers should investigate how different factors affect desired outcomes such as fairness in high-stakes public sector contexts, where market forces are muted and the cost of the error falls largely on the subject of the algorithmic decision. Where there is evidence that consumer welfare is significantly lowered, regulators should consider prohibiting the government from using AI systems for such decisions. They should invest in upskilling regulators in AI expertise and developing tools to monitor and address sector-specific AI risks, as the United Kingdom has done, which will better equip policymakers to establish and enforce sector-specific rules for AI where necessary, such as potential transparency or reporting requirements.[72]

4. CONSUMER CONCERNS

#	Risk	Policy needs	Policy solution
4.1	AI may exacerbate surveillance capitalism.	No policy needed	Rather than pushing for restrictions on targeted advertising, policymakers and civil society should allow the private sector to do what it does best: innovate and develop novel technologies that improve welfare.

○ AI-specific regulation
○ General regulation
○ AI-specific nonregulatory policy
○ General nonregulatory policy
● **No policy needed**

Issue 4.1: AI May Exacerbate Surveillance Capitalism

The issue: A November 2023 op-ed in the *Financial Times* reads, "We must stop AI replicating the problems of surveillance capitalism."[73] It warns that AI is making it easier for large tech companies to monetize and profit from the collection, analysis, and use of personal data and user behaviors—an issue dubbed "surveillance capitalism," as detailed in Shoshana Zuboff's book of the same name.[74] When it comes to AI, the concern is that companies will be able to better commodify user data and exploit consumers even more than they already do because algorithms will enable them to better analyze user data, better anticipate user preferences, and better personalize user experiences. One of the chief ways powerful companies are doing this, critics say, is by using algorithms and personal data for targeted advertising, trampling consumer privacy and rights.

But despite claims that targeted ads are a massive intrusion on consumer privacy, most ad platforms deliver these ads to Internet users without revealing consumers' personal data to the advertisers. And critics of targeted advertising do not acknowledge the ample benefits of personalization to advertisers, publishers, and consumers alike, especially how these ads fund the Internet economy.[75] Indeed, targeted online ads form an essential part of the digital economy: Advertisers can link consumers to specific queries and interests and then show them relevant ads as they visit different websites. This has three positive effects: First, consumers see ads for items that are likelier to be relevant to them than the nontargeted ads they encounter in traditional media. Second, advertisers spend their marketing budgets on ads that are likelier to generate a response from the audience, which makes their ad spend more cost-effective and affordable than traditional forms of marketing. This is why personalized ads have been a godsend to small businesses: Millions of enterprises benefit from being able to show their wares to interested customers, rather than wasting money on ads shown to uninterested audiences. Third, websites and app publishers can sell inventory on their sites to advertisers, earning them valuable income and allowing them to offer content and services to users for free.

The solution: Policymakers should not introduce laws that ban targeted advertising, as doing so would hurt consumers, businesses, and publishers. Rather than pushing for restrictions on targeted advertising, policymakers and civil society should allow the private sector to do what it does best: innovate and develop novel technologies that improve welfare for everyone, including publishers (who can continue to earn billions in advertising income), consumers (who can obtain the benefits of free, ad-supported apps and websites, plus prefer to see ads tailored to their needs rather than being blanketed with irrelevant messages), and advertisers (who can continue to access affordable, effective ads, instead of relying on the kinds of pre-digital marketing that only helps large brands).[76]

5. MARKET CONCERNS

#	Risk	Policy needs	Policy solution
5.1	AI may enable firms with key inputs to control the market.	No policy needed	There is no evidence of significant entry barriers to the AI market. If this should change, antitrust policy is already capable of handling most clear threats to competition.
5.2	AI may reinforce tech monopolies.	No policy needed	Antitrust agencies already have the powers they need to stop problematic acquisitions and partnerships, but they should recognize that vertically integrated AI ecosystems are not inherently problematic and can have procompetitive effects that benefit consumers overall.

○ AI-specific regulation
○ General regulation
○ AI-specific nonregulatory policy
○ General nonregulatory policy
● **No policy needed**

Issue 5.1: AI May Enable Firms With Key Inputs to Control The Market

The issue: The top U.S. antitrust regulators, Federal Trade Commission (FTC) Chair Lina Khan and DOJ's antitrust chief Jonathan Kanter, recently argued that government action may be warranted to prevent large technology companies from using anticompetitive tactics to protect their standing in the emerging AI market.[77] For example, Kanter warned that the AI industry has a "greater risk of having deep moats and barriers to entry."[78] Similar, FTC staff penned an article in June 2023 arguing that generative AI depends on a set of necessary inputs—such as access to data, computational resources, and talent—and "incumbents that control key inputs or adjacent markets, including the cloud computing market, may be able to use unfair methods of competition to entrench their current power or use that power to gain control over a new generative AI market."[79]

However, the generative AI market is still in its early stages, and as of now, there is no evidence of significant entry barriers. Concerns about data being an entry barrier in AI are speculative and unsubstantiated. Firms seeking to create generative AI models can use data from various sources, including publicly available data on the Internet, government and open-source datasets, datasets licensed from rightsholders, data from workers, and data shared by users. They also have the option to generate synthetic data to train their models.[80] Some firms, such as OpenAI, Anthropic, and Mistral AI, have succeeded in creating leading generative AI models despite not having access to the large corpus of user data held by social media companies such as Meta and X.com. Additionally, companies with internal data can leverage it to build specialized models tailored to specific tasks or fields, such as financial services or healthcare. Similarly, compute resources required for training generative AI models have not proven to be an entry barrier. There are numerous players in the cloud server market that provide the necessary infrastructure for training and running AI models. For example, Anthropic used Google Cloud to train its Claude AI models.[81] In terms of chips, Nvidia's graphics processing units (GPUs) are popular but face meaningful potential competition from firms such as AMD and Intel.[82] Other firms are also investing in chip design and manufacturing, fostering competition in the market.[83] For example, Google has invested heavily in Tensor Processing Units (TPUs), which are specialized chips designed to train and run AI models.

The solution: Competition regulations should allow the AI industry to continue to develop new and innovative products without unwarranted restrictions so that both businesses and consumers can access the benefits of AI. If there are documented cases of AI companies engaging in anticompetitive behavior, resulting in harm to consumers, antitrust authorities already can—and should—act. Antitrust policy is already capable of handling most clear threats to competition, and as the FTC itself notes, it is no stranger to dealing with emerging technologies.[84]

○ AI-specific regulation
○ General regulation
○ AI-specific nonregulatory policy
○ General nonregulatory policy
● **No policy needed**

Issue 5.2: AI May Reinforce Tech Monopolies

The issue: A brewing concern is that large, vertically integrated firms that control the entire AI stack, from cloud infrastructure to applications, may engage in anticompetitive practices, such as excluding downstream rivals. This could involve restricting access to essential cloud resources or copying and integrating features from competitors, which results in effectively squeezing them out of the market due to their own scale and reach. Additionally, these firms might prefer their own AI products and services within their ecosystem, further limiting market access for new entrants. Instead, several competition authorities would like to see "mix-and-match" competition at and between all layers of the vertical chain rather than vertical integration.

However, a mix-and-match environment may not drive the same level of competition between generative AI models as ones with vertical ecosystems.[85] Imagine a cloud provider and an AI model developer partnering in a vertically integrated system. In this setup, if the integrated system loses customers downstream (using AI models), it not only loses those specific sales but also faces reduced scale and revenue potential for its other services higher up in the chain (e.g., cloud services). This means that a loss in one part of the system affects the entire chain more significantly than a system wherein different parts operate independently. Vertical integration can result in a competitive AI market in which several ecosystems exert pressure on each other, and supporting the emergence of new vertical ecosystems at this early stage of AI industry could help ensure the AI market does tip to the monopoly. [86] It is also important that there are developments in both closed source (proprietary) and open source (accessible to the public) ecosystems, which further contributes to stimulating competition.

The solution: Antitrust agencies already have the powers they need to stop problematic acquisitions and partnerships, but they should recognize that vertically integrated AI ecosystems are not inherently problematic and can have procompetitive effects that benefit consumers overall. They should base decisions on a detailed understanding of markets, including current and future sources of innovation, and focus on increasing social welfare. Agency guidelines explain that nonprice terms also matter when evaluating a merger or acquisition, including "reduced product quality, reduced product variety, reduced service, or diminished innovation."[87] Vertical ecosystems in the AI industry often prioritize differentiation over price competition, emphasizing offering unique features, innovative solutions, and high-quality services to distinguish themselves in the market. Regulators should consider this focus on differentiation when evaluating the competitive landscape of AI ecosystems.

6. CATASTROPHIC SCENARIOS

#	Risk	Policy needs	Policy solution
6.1	AI may make it easier to build bioweapons.	General regulation	Policymakers should clarify and strengthen existing policies related to biosecurity and biosafety oversight. They should update existing biosecurity practices to include guidance for how providers of labs can verify who is using the lab (customer screening) and what it is being used for (experiment screening).
6.2	AI may create novel biothreats.	AI-specific nonregulatory policies	Congress should task the Department of Homeland Security (DHS) and Department of Energy (DOE) with developing state-of-the-art evaluations for dangerous biological capabilities. Benchmarks are needed to scope any future regulations.
6.3	AI may become God-like and "superintelligent."	AI-specific nonregulatory policies	Policymakers should establish a Search for Artificial General Intelligence (SAGI) Institute focused on identifying advanced machine intelligence.
6.4	AI may cause energy use to spiral out of control.	AI-specific nonregulatory policies	Policymakers should support the development of energy transparency standards for AI models. They should also accelerate the use of AI across government agencies to decarbonize government operations.

○ AI-specific regulation
● **General regulation**
○ AI-specific nonregulatory policy
○ General nonregulatory policy
○ No policy needed

Issue 6.1: AI May Make It Easier To Build Bioweapons

The issue: General-purpose AI capabilities could impact the creation of biological threats by increasing malicious actors' access to information and expertise. For instance, some are concerned that LLMs could provide detailed guides on acquiring, synthesizing, and spreading dangerous pathogens such as *Ebola*, potentially leading to a pandemic.[88]

This concern is particularly focused on AI-enabled chatbots, which could not only assist experts but also enable scientifically inexperienced users to gather information more easily. Chatbots can help decipher scientific concepts and offer step-by-step instructions, streamlining the information-gathering process. Chatbots could therefore act as biological research assistants, removing the need for users to track down information, decide between multiple sources, and combine these pieces of information into a plan themselves.[89]

However, while the threat is legitimate, thinking of chatbots as the sole gatekeepers of information overstates how high the barrier to this information is.[90] Chatbots are trained on existing information that users could access independently and relatively easily. As the article notes, "[A] chatbot that lowers the information barrier should be seen as more like helping a user step over a curb than helping one scale an otherwise unsurmountable wall."[91] Furthermore, according to a 2024 report from the National Security Commission on Emerging Biotechnology, a congressionally mandated commission, "[LLMs do] not significantly increase the risk of the creation of a bioweapon."[92] Finally, even if users overcome the barrier to scientific information, being able to produce a known, existing pathogen or toxin will likely also require practical laboratory skills and materials for production.

The solution: Policymakers should focus on bolstering protections throughout the biothreat development process because accessing the basic information and resources to cause biological harm doesn't require advanced AI tools. To this end, policymakers should clarify and strengthen existing policies related to biosecurity and biosafety oversight. For instance, cloud labs, also known as online or virtual labs, are platforms that enable users to conduct scientific experiments and research remotely through cloud computing technology. Instead of needing physical laboratory space and equipment, cloud labs provide a virtual environment wherein users can access and operate scientific instruments, conduct experiments, analyze data, and collaborate with others over the Internet. Policymakers should update existing biosecurity practices to include guidance for how providers of labs can verify who is using the lab (customer screening) and what it is being used for (experiment screening).[93]

○ AI-specific regulation
○ General regulation
● **AI-specific nonregulatory policy**
○ General nonregulatory policy
○ No policy needed

Issue 6.2: AI May Create Novel Biothreats

The issue: General purpose AI capabilities could impact the creation of biological threats by increasing novelty, meaning they could assist malicious actors in developing novel biological threats or more harmful versions of existing threats.

This concern is particularly focused on bio-design tools (BDTs), which can predict and simulate biological molecules and processes that can help researchers understand large-scale biological patterns. Unlike LLMs, which enable users to better access existing information, BDTs generate novel information. Consider DeepMind's AlphaFold, an AI tool that predicts the shape of proteins, a scientific challenge necessary to make important biological discoveries.[94] Prior to AlphaFold, scientists had only determined the 3D shape of about 190,000 proteins, or 0.1 percent of known protein structures, each one of which likely took months or years to figure out. DeepMind's AI tool has now expanded that knowledge to more than 200 million predicted protein structures, covering almost every organism in the world that has had its genome sequenced, and made these structures available via a public database.

While such tools undoubtably drive significant innovation, there is a risk that bad actors could misuse and exploit them to design new pathogens or toxins. Additionally, these tools might aid malicious actors in evading detection. For instance, they could generate a protein sequence that mimics a regulated toxin's function while possessing a distinct genetic code, thereby circumventing sequence-based screening measures.[95] Because BDTs are specialized AI tools, scientific novices are unlikely to use them successfully. They need to understand how molecules work and how they can change with genetic, structural, functional, or chemical adjustments, as well as be able to compare different choices based on BDT predictions, make the biomolecule in a lab, and run tests to see if it works.[96]

Solution: Policymakers should identify specific scenarios in which scientifically knowledgeable users could potentially misuse BDTs and design policies to target these particular areas of concern, avoiding overbearing policies that hinder beneficial applications. Congress should task DHS and DOE with developing state-of-the-art evaluations for dangerous biological capabilities. The problem with the recent executive order on safe and secure AI is it directs DHS to assess the potential for AI to enhance chemical, biological, radiological, and nuclear6 threats through consultation with experts, but this will be difficult to do because there has been little progress on developing benchmarks or evaluations for BDTs.[97] Without evaluation capabilities, policymakers will not be able to scope any regulations or effectively balance safeguards against the potential benefits. Congress should also direct and fund DOE to establish a sandbox for testing evaluations on a variety of AI-enabled biological tools.

○ AI-specific regulation
○ General regulation
● **AI-specific nonregulatory policy**
○ General nonregulatory policy
○ No policy needed

Issue 6.3: AI May Become God-Like and "Superintelligent"

The issue: Most doomsday scenarios predicting catastrophic outcomes stem from the development of what tech entrepreneur and investor Ian Hogarth dubbed "God-like AI" in a now-viral *Financial Times* article.[98] Talking about AGI or "superintelligence," Hogarth asserted "A three-letter acronym doesn't capture the enormity of what AGI would represent, so I will refer to it as what is: God-like AI. A superintelligent computer that learns and develops autonomously, that understands its environment without the need for supervision and that can transform the world around it."[99]

There are three broad ways developing God-like AI could hypothetically result in existential harms, which for the purposes of this report, means those harms that would annihilate humanity or permanently and drastically curtail its potential: First are accidents; those creating God-like AI systems could unwittingly develop systems that display unintended and harmful behavior that results in existential or catastrophic harm to human civilization. For example, advanced AI systems that do not "align" with human values (commonly referred to as the "alignment problem") may launch (or refuse to launch) military weapons systems. Second is misuse; malicious actors, such as a rogue state or terrorist organization, could use a God-like AI system to intentionally cause harm. For example, a malicious actor could use advanced AI capabilities to exploit vulnerabilities in LLMs to make them release information on how to design new pathogens that cause mass death. Finally, there could be structural disruptions; God-like AI systems could destabilize the broader environment by creating "structural risks" in harmful ways that do not fall into the accident-misuse dichotomy.[100] For example, AI systems that identify or assess the retaliatory capabilities of an adversarial nation could disturb the equilibrium of mutual assured destruction and drastically increase the risk of a nuclear war.

However, while there are true believers in the risks of dangerous superintelligent AI wiping out human civilization, as well as those who are skeptical or agnostic, these risks are hypothetical and currently remain unprovable. Other hypothetical but unprovable claims such as the probability of finding adversarial extraterrestrial life does not paralyze policymaking around issues such as radio signals, space exploration, or national defense. [101]

The solution: Policymakers should remain clear eyed in the face of grandiose, uncertain claims. To contend with existential risks, one of the most necessary functions at this stage is to better understand the threat vectors. Policymakers should establish an SAGI Institute focused on identifying advanced machine intelligence. Its goal should be to develop consensus around signs of AGI, how to test for AGI, different levels of AGI, and what researchers should do if they ever identify AGI.[102]

○ AI-specific regulation
○ General regulation
● **AI-specific nonregulatory policy**
○ General nonregulatory policy
○ No policy needed

Issue 6.4: AI May Cause Energy Use to Spiral Out of Control

The issue: Concerns about the energy and carbon footprint of AI have been around since at least 2019. *New Scientist* ran the headline "Creating an AI can be five times worse for the planet than a car" in June 2019.[103] The concerns have gotten more acute, with some worrying that the rapid adoption of AI in recent years combined with an increase in the size of deep learning models will lead to a massive increase in energy use, causing potentially devastating environmental impact.[104] An October 2023 piece in *Scientific American* reads, "The AI Boom Could Use a Shocking Amount of Electricity."[105]

However, looking at the energy cost of AI in isolation—without addressing the benefits—does not answer the question of whether developing an AI model makes sense. AI models have a wide range of applications, including in the climate and energy context. Indeed, powerful AI technologies enable other sectors to become more energy efficient. From powering intelligent transportation systems to enabling smart grids to improving city operations and maintenance, AI is already supporting smarter energy use and reducing greenhouse gas emissions.[106] Even the large natural language processing models critics disparage are helping researchers understand the solar panel innovation process and identify climate risks and investment opportunities from public company disclosures.[107] The question should not be whether AI models use energy, but rather whether the energy consumption involved generates net-positive societal benefits.

The solution: The impact of AI on energy and the environment should be part of the policy debate, but policymakers should also be careful not to overreact. There are reasonable steps policymakers can take to ensure AI is part of the solution, not part of the problem, when it comes to the environment.[108] First, policymakers should support the development of energy transparency standards for AI models, both for training and inference. In the United States, for example, NIST should work with DOE to develop a recommended best practice for assessing the training and inference energy costs. The White House should continue its dialogue with leading AI companies to seek a voluntary commitment to publicly disclose the energy required to train and operate these foundation models, as well as the associated carbon emissions, especially for cloud-based AI service providers.

In addition, policymakers should accelerate the use of AI across government agencies to decarbonize government operations. The president should sign an executive order directing the Technology Modernization Fund—a relatively new funding system for federal government IT projects—to include environmental impact as one of the core priority investment areas for projects to fund.

7. INTELLECTUAL PROPERTY CONCERNS

#	Risk	Policy needs	Policy solution
7.1	AI may unlawfully train on copyrighted content.	AI-specific nonregulatory policies	Policymakers should fund research on technical measures that AI firms can use to reduce the risk of inadvertently training on copyrighted content, such as the development of machine-readable opt-out standards. They should also support the creation of training datasets with high-quality data in the public domain.
7.2	AI may create infringing content.	General nonregulatory policies	Policymakers should consider developing a similarity checker to help courts assess substantial similarity for musical works, regardless of whether a work is created with AI or not.
7.3	AI may infringe on publicity rights.	General regulation	Congress should provide rightsholders with a federal cause of action for publicity rights to ensure some basic jurisdictional consistency within the United States.

○ AI-specific regulation
○ General regulation
● **AI-specific nonregulatory policy**
○ General nonregulatory policy
○ No policy needed

Issue 7.1: AI May Unlawfully Train on Copyrighted Content

The issue: Generative AI systems may train their models on text, audio, images, and videos that are legally accessible to Internet users but are also protected by copyright. AI firms argue that they cannot train LLMs without access to copyrighted work, but they are finding themselves entangled in legal battles with content creators and rights holders who claim copyright infringement. *The New York Times* sued OpenAI and Microsoft in 2023 accusing them of "unlawful use" of its work to create their products.[109] Getty Images, which owns one of the largest photo libraries in the world, is suing the creator of AI art generator Stable Diffusion for alleged copyright breaches.[110] And three of the biggest music publishers are suing AI company Anthropic, alleging that it is misusing copyrighted song lyrics to train its Claude chatbot.[111]

The underlying question in all these cases is whether training AI models on copyrighted materials falls under the "fair use" doctrine (or other exceptions to copyright law in other countries).[112] The concept of fair use is a well-established principle in copyright law that allows for the limited use of copyrighted material without the need for permission from the copyright holder under certain circumstances.[113] While it will ultimately be up to the courts to decide whether a particular use of generative AI infringes on copyright, there is precedent for them to find most uses to be lawful and not in violation of rightsholders' exclusive rights.

The solution: Policymakers should fund research on technical measures that AI firms can use to reduce the risk of inadvertently training on copyrighted content.[114] For example, creating standardized opt-out protocols could allow content publishers to indicate that AI firms should not train AI models on their content, and tools to score training data could help provide information on whether an output was influenced by a particular copyrighted text. These attribution scores can then be used as a measure for evaluating the copyright infringement risk associated with the output.[115] However, policymakers should not mandate technical mitigations because some may negatively impact other values, such as free speech.[116]

Policymakers should also support the creation of training datasets with high-quality data in the public domain, as the French government has done. The French-Public Domain-Book, or French-PD-Books, is a collection of 289,000 books (containing more than 16 billion words) from the French National Library. The dataset is thought to be the largest AI training dataset composed entirely of text that is in the public domain.[117] Some organizations, such as the nonprofit Fairly Trained, have created certifications for LLMs built on such databases.[118]

○ AI-specific regulation
○ General regulation
○ AI-specific nonregulatory policy
● **General nonregulatory policy**
○ No policy needed

Issue 7.2: AI May Create Infringing Content

The issue: In addition to the concern that generative AI systems may unlawfully train on copyright-protected content, generative AI may allow creators to produce output that is similar to existing copyrighted works. While the latest generative AI systems mostly produce novel content, it is possible for these systems to replicate content from training data. The law allows creators to produce similar works, but it does not allow them to produce identical or nearly identical works. Copyright owners, including those of literary, musical, and artistic works, can claim infringement if someone produces a work that is substantially similar to their own because they have an exclusive right to produce derivative works. Courts have repeatedly intervened in these cases, including for sampling small portions of a song, such as when Queen and David Bowie successfully sued Vanilla Ice because the bass line in "Ice Ice Baby" came directly from "Under Pressure," and for replicating key elements of a song, such as when the estate of Marvin Gaye successfully sued Robin Thicke and Pharrell Williams for the similarities between "Blurred Lines" and "Got to Give It Up."[119] Artists can and should continue to enforce their rights in court when someone produces nearly identical work that unlawfully infringes on their copyright, whether that work was created entirely by human hands or involved the use of generative AI.

The solution: Policymakers should develop a similarity checker to help courts assess substantial similarity for musical works, regardless of whether the work is created with AI or not.[120] Currently, judges or juries, depending on the specific legal procedure and jurisdiction, evaluate works in question to determine if there's sufficient similarity between them to warrant a finding of infringement. However, this legal test is one of the most maligned tests in the legal field for being inconsistently applied and being opaque and mystifying for courts and litigants.[121] Congress should make things more consistent, accurate, and fair by directing and funding the Copyright Office to launch a competition for the private sector to come up with an AI-enabled tool to compare how similar a musical composition or recording is to existing copyright-protected works. This service should be modeled after the popular Turnitin online service that educators use to check how similar their students' written submissions are to existing written works. Importantly, these tools do not claim to identify plagiarism. Instead, they simply flag similarity and provide educators with the information they need to make a judgment. They can work to check similarity regardless of whether a work was written exclusively by a human or with the help of generative AI tools such as ChatGPT. Perhaps most crucially, creating such a tool would give artists the ability ex ante to anticipate whether their work likely infringes on any existing copyrighted works. Having a portal where artists can check their work before they release it gives them an opportunity to identify areas of risk and change the parts that are flagged as potentially infringing.

○ AI-specific regulation
● **General regulation**
○ AI-specific nonregulatory policy
○ General nonregulatory policy
○ No policy needed

Issue 7.3: AI May Infringe on Publicity Rights

The issue: The right of publicity is the intellectual property right that protects individuals from the unauthorized commercial use of their identity. This right is especially important for celebrities, as it enables them to control how others use their likeness commercially, such as in advertisements or in film and TV. Generative AI—specifically deepfake technology—makes it easier to create content that impersonates someone else. YouTube star MrBeast and actor Tom Hanks have recently warned of AI ads that ape their faces and voices to falsely show them endorsing products.[122] And music publishers and labels were disquieted earlier this year by a viral song created with AI-generated vocals imitating recording artists Drake and The Weeknd that racked up millions of listens before being taken down.[123] Generative AI also raises concerns about who will get to own the rights to certain character elements. For example, if a movie studio wants to create a sequel to a film, can it use generative AI to digitally recreate a character (including the voice and image) or does the actor own those rights? And does it matter how the film will depict the character, including whether the character might engage in activities or dialogue that could reflect negatively on the actor?

However, generative AI has not changed the fact that individuals can and should continue to enforce their publicity rights by bringing cases against those who violate their rights. Courts have repeatedly upheld this right, including for cases involving indirect uses of an individual's identity. In one notable case, game show hostess Vanna White won damages for an advertisement that depicted a robot meant to impersonate her. In another, late-night television star Johnny Carson won a claim against a portable toilet company that used the phrase "Here's Johnny!" without his permission. And questions about ownership will likely be settled through contracts performers sign addressing who has rights to a performer's image, voice, and more. The Screen Actors Guild - American Federation of Television and Radio Artists (SAG-AFTRA) signed a deal with leading AI voice company Replica Studios in January 2024 that sets terms for SAG-AFTRA members to license their digital voice replicas to Replica. The agreement includes protections for performers, such as fair compensation, protection of voice data, and the need for a performer's consent before a replicated voice can be used in a project.

The solution: Congress should provide rightsholders with a federal cause of action for publicity rights to ensure some basic jurisdictional consistency within the United States. Currently, publicity rights vary widely within the United States, and the legal concept is sparsely recognized in international jurisdictions. However, the scope of any federal right of publicity should be limited so as not to stifle free speech or impede creative expression. It could, for instance, provide a minimum set of protections for an individual's name, signature, image, and voice against commercial exploitation during their lifetime.[124]

8. SAFETY AND SECURITY

#	Risk	Policy needs	Policy solution
8.1	AI may enable fraud and identity theft.	AI-specific regulation	Financial regulatory agencies should update security guidelines to ensure financial institutions do not rely solely on voice authentication for customers
8.2	AI may enable cyberattacks.	AI-specific nonregulatory policy	Congress should address the cybersecurity workforce shortage within the federal government by establishing and funding an AI Center of Excellence dedicated to building AI tools and capacity to augment cybersecurity operations.
8.3	AI may create safety risks.	AI-specific regulation	Congress should charge the newly created AI Safety Institute—housed in the Department of Commerce's NIST—with creating a national AI incident database and a national AI vulnerability database.

- ● **AI-specific regulation**
- ○ General regulation
- ○ AI-specific nonregulatory policy
- ○ General nonregulatory policy
- ○ No policy needed

Issue 8.1: AI May Enable Fraud and Identity Theft

The issue: In recent months, there has been a concerning rise in nefarious uses of AI-enabled voice cloning. Bad actors have targeted families and small businesses with fraudulent extortion scams. The scams themselves are not new, the term "virtual kidnapping scam" has been around for many years to describe the ways fraudsters trick victims into paying a ransom to free a loved one they believe is being threatened. But AI has made these scams more sophisticated, as the technology can be trained on audio of regular people—which is relatively easy to find from social media platforms such as TikTok, Instagram, and YouTube—and made to sound incredibly authentic, further blurring the line between genuine communication and malicious manipulation.

The concerns about AI-enabled voice cloning are legitimate and need concerted efforts across borders.

The solution: Financial regulatory agencies should update security guidelines to ensure financial institutions do not rely solely on voice authentication for customers. Some banks use voice recognition for customer authentication when accessing accounts or conducting transactions over the phone. Given the novel threat vectors of AI voice-cloning, regulators should update these guidelines to incorporate robust multi-factor authentication protocols that do not use voice recognition to enhance security measures against evolving risks.

Because fraudulent scam calls can come from any part of the world, policymakers should internationalize their efforts to find solutions to detect and mitigate voice clones. FTC has already launched an exploratory challenge to foster comprehensive solutions to prevent, monitor, and evaluate malicious voice cloning, while the EU's support network for SMEs, the Enterprise Europe Network, is trying to find international business partners for the EU companies that have already found promising solutions.[125] Rather than working in siloes, governments should prioritize working together to find, grow, and adopt the most cutting-edge solutions. Governments should also prioritize voice cloning research in tandem with clone detection research, as this best allows for a comprehensive understanding of both the vulnerabilities and the effective countermeasures. The United Kingdom is already home to several notable research partnerships in this space, such as Edinburgh University's Centre for Speech Technology's ASVspoof program. Policymakers should seek to bolster these efforts, especially with international pools of voice data.

○ AI-specific regulation
○ General regulation
● **AI-specific nonregulatory policy**
○ General nonregulatory policy
○ No policy needed

Issue 8.2: AI May Enable Cyberattacks

The issue: AI may increase the scale and success rate of cyberattacks. In the near term, AI provides attackers with new methods to facilitate cyberattacks, such as using it to help attackers better identify vulnerabilities, hide malicious code, craft targeted phishing attacks, and evade cyber defenses. Finally, AI systems themselves may be targets of cyberattacks, from denial-of-service attacks to more advanced data poisoning attacks intended to corrupt AI models to produce harmful results.

On the other hand, many cyberattacks still require human labor.[126] A recent report from Georgetown's CSET notes that "even if machine learning technology continues to advance at a rapid pace in other areas, it does not follow that it will also immediately transform offensive cyber operations. For some parts of cyber operations, machine learning techniques may never matter."[127] Indeed, attackers are only likely to apply AI for automating cyberattacks if they perceive unique advantages or benefits, but as the report goes on to say, there are many limitations and shortcomings to doing so.[128] For instance, there are few large public datasets available for training AI models for cyberattacks. Attackers would likely have to spend time and money to build these themselves in order to create sufficiently good models.

However, attackers can quickly adopt AI tools where they will be effective whereas the government agencies and corporations they are targeting tend to react to technological changes less quickly. For example, the Government Accountability Office (GAO) noted in a 2023 report that since 2010, it has made over 100 recommendations on how to protect critical infrastructure from cyberattacks, but agencies have implemented fewer than half of them.[129] Likewise, another 2023 GAO report finds that 70 percent of federal civilian agencies have "ineffective" information security programs, leaving them vulnerable to cyberattacks.[130]

The solution: Policymakers have taken steps to use AI to address cybersecurity risks. For example, President Biden's AI Executive Order directs agencies to "deploy AI capabilities effectively for cyber defense."[131] In addition, the Cybersecurity and Infrastructure Security Agency (CISA) published a roadmap for AI that includes using AI for cyber defense and expanding AI expertise.[132] However, the federal government continues to face a cybersecurity workforce shortage, limiting its ability to address cyber threats, including those from AI.[133] Congress should do more to address this problem by establishing and funding an AI Center of Excellence dedicated to building AI tools and capacity that can augment and automate cybersecurity operations to close the workforce skills gap.

- ● **AI-specific regulation**
- ○ General regulation
- ○ AI-specific nonregulatory policy
- ○ General nonregulatory policy
- ○ No policy needed

Issue 8.3: AI May Create Safety Risks

The issue: AI may cause real-world health and safety risks if an AI system fails. For example, an autonomous vehicle may crash if the onboard system fails to recognize a roadway hazard, or an AI-enabled medical device may incorrectly diagnose or treat a patient leading to undesirable health outcomes. AI already assists in high-stakes domains such as healthcare, criminal justice, and financial services, and the technology's impact on society will only grow as models become more capable—and in some of these areas, society may deem certain risks to be acceptable, such as if AI-enabled vehicles reduce total injuries and fatalities but do not eliminate them.

In many cases, the entities responsible for creating or deploying AI systems will have strong market incentives to address safety risks to maintain a brand's reputation and mitigate their liability costs. In addition, in many regulated sectors, such as health care and transportation, existing regulators may also impose safety obligations on companies before they can bring their products to the market, such as independent testing or certification requirements.

However, safety testing for AI systems is still a developing field and neither businesses nor regulators know the optimal ways to reliably test the safety and reliability of AI systems. As a result, despite best efforts to test and evaluate AI systems, some may still contain unknown safety risks.

The solution: Congress should charge the newly created AI Safety Institute—housed in NIST—with creating both a national AI incident database and a national AI vulnerability database.[134] There is no process in place to systematically track AI failures, vulnerabilities, and incidents to learn from mistakes and uphold public trust. To address this problem, Congress should pass AI-specific legislation to standardize tracking of incidents from AI systems and monitor AI-specific vulnerabilities, which are not the same as cybersecurity vulnerabilities. The AI Safety Institute should work with other countries to create a common vulnerability reporting and naming standard to facilitate information sharing among stakeholders globally.

CONCLUSION

Proposals to “regulate AI” mirror the fears being expressed and the harms advanced in the unfolding narrative of AI, where the shadows of concern cast longer than the promises of progress. While certain issues may require regulation, most are better addressed through other policy actions. By thoughtfully evaluating each concern and tailoring actions accordingly, policymakers can forge targeted, impactful policies that mitigate risks, safeguard fundamental rights, and nurture responsible AI advancement. This strategy is crucial to ensuring that AI continues to drive positive change while mitigating potential risks.

APPENDIX: THE RIGHT POLICY SOLUTIONS FOR AI CONCERNS

- ● **AI-specific regulation**
- ○ General regulation
- ○ AI-specific nonregulatory policy
- ○ General nonregulatory policy
- ○ No policy needed

Table 1: Concerns that warrant AI-specific regulations

#	Risk	Policy Solution
1.3	AI may enable government surveillance.	Congress should direct the Department of Justice (DOJ) to establish guidelines for use by state and local law enforcement in investigations that outline specific use cases and capabilities, including when a warrant is necessary for use, as well as transparency guidelines for when to notify the public of law enforcement using AI.
3.6	AI may make harmful decisions.	Policymakers should consider prohibiting the government from using AI systems in certain high-risk, public sector contexts. They should upskill regulators with better AI expertise and develop tools to monitor and address sector-specific AI risks, as the United Kingdom has done.
8.1	AI may enable fraud and identity theft.	Financial regulatory agencies should update security guidelines to ensure financial institutions do not rely solely on voice authentication for customers
8.3	AI may create safety risks.	Congress should charge the newly created AI Safety Institute—housed in the Department of Commerce's NIST—with creating a national AI incident database and a national AI vulnerability database.

○ AI-specific regulation
● **General regulation**
○ AI-specific nonregulatory policy
○ General nonregulatory policy
○ No policy needed

Table 2: Concerns that warrant general regulations

#	Risk	Policy Solution
1.1	AI may expose personally identifiable information in a data breach.	Policymakers should require companies to publish security policies to promote transparency with consumers. Congress should pass federal data breach notification legislation.
1.5	AI may infer sensitive information.	Policymakers should craft and enact comprehensive national privacy legislation that addresses the risks of data-driven inference in a tech-neutral way.
1.6	AI may help bad actors harass and publicly shame individuals.	Congress should outlaw the nonconsensual distribution of all sexually explicit images, including deepfakes that duplicate individuals' likenesses in sexually explicit images, and create a federal statute that prohibits revenge porn, including those with computer-generated images.
3.2	AI may fuel deepfakes in elections.	Policymakers should update state election laws to make it unlawful for campaigns and other political organizations to knowingly distribute materially deceptive media.
6.1	AI may make it easier to build bioweapons.	Policymakers should clarify and strengthen existing policies related to biosecurity and biosafety oversight. They should update existing biosecurity practices to include guidance for how providers of labs can verify who is using the lab (customer screening) and what it is being used for (experiment screening).
7.3	AI may infringe on publicity rights.	Congress should provide rightsholders with a federal cause of action for publicity rights to ensure some basic jurisdictional consistency within the United States.

○ AI-specific regulation
○ General regulation
● **AI-specific nonregulatory policy**
○ General nonregulatory policy
○ No policy needed

Table 3: Concerns that warrant AI-specific nonregulatory policies

#	Risk	Policy Solution
1.4	AI may enable workplace surveillance.	Policymakers should help set the quality and performance standards of AI technologies used in the workplace
3.3	AI may manipulate voters.	Policymakers should update digital literacy programs to include AI literacy, which teaches individuals to understand and use AI-enabled technologies.
3.5	AI may perpetuate discrimination.	Policymakers should support the development of tools that help organizations provide structured disclosures about AI models and related data.
6.2	AI may create novel biothreats.	Congress should task the Department of Homeland Security (DHS) and Department of Energy (DOE) with developing state-of-the-art evaluations for dangerous biological capabilities. Benchmarks are needed to scope any future regulations.
6.3	AI may become God-like and "superintelligent."	Policymakers should establish a Search for Artificial General Intelligence (SAGI) Institute focused on identifying advanced machine intelligence.
6.4	AI may cause energy use to spiral out of control.	Policymakers should support the development of energy transparency standards for AI models. They should also accelerate the use of AI across government agencies to decarbonize government operations.
7.1	AI may unlawfully train on copyrighted content.	Policymakers should fund research on technical measures that AI firms can use to reduce the risk of inadvertently training on copyrighted content, such as the development of machine-readable opt-out standards. They should also support the creation of training datasets with high-quality data in the public domain.
8.2	AI may enable cyberattacks.	Congress should address the cybersecurity workforce shortage within the federal government by establishing and funding an AI Center of Excellence dedicated to building AI tools and capacity to augment cybersecurity operations.

- ○ AI-specific regulation
- ○ General regulation
- ○ AI-specific nonregulatory policy
- ● **General nonregulatory policy**
- ○ No policy needed

Table 4: Concerns that warrant general nonregulatory policies

#	Risk	Policy Solution
1.2	AI may reveal personally identifiable information included in training data.	Policymakers should fund research for privacy- and security-enhancing technologies and there should be support for industry-led standards for responsible web-scraping.
2.2	AI may dislocate blue collar workers.	Policymakers should support full employment, nationally and regionally, not just with macro-economic stabilization policies, but also with robust regional economic development policies; ensure as many workers as possible have needed education and skills before they are laid off; reduce the risk of income loss and other financial hardships when workers are laid off; and provide better transition assistance to help laid off workers find new employment.
2.3	AI may dislocate white collar workers.	Policymakers should ensure that job dislocation policies and programs support all workers whose jobs are impacted by automation so they can train for new jobs. They should also proactively support IT modernization in the public sector, including the adoption of generative AI.
3.1	AI may have political biases.	Policymakers should treat chatbots like the news media, which is subject to market forces and public scrutiny, but is not directly regulated by the government when it comes to expressing political perspectives.
7.2	AI may create infringing content.	Policymakers should consider developing a similarity checker to help courts assess substantial similarity for musical works, regardless of whether a work is created with AI or not.

- ○ AI-specific regulation
- ○ General regulation
- ○ AI-specific nonregulatory policy
- ○ General nonregulatory policy
- ● **No policy needed**

Table 5: Concerns that do not warrant new policies

#	Risk	Policy Solution
2.1	AI may cause mass unemployment.	Policymakers do not need to focus on concerns about mass unemployment from AI adoption because the economic evidence does not support this materializing.
3.4	AI may fuel unhealthy personal attachments.	Not enough evidence of impacts to society yet.
4.1	AI may exacerbate surveillance capitalism.	Rather than pushing for restrictions on targeted advertising, policymakers and civil society should allow the private sector to do what it does best: innovate and develop novel technologies that improve welfare.
5.1	AI may enable firms with key inputs to control the market.	There is no evidence of significant entry barriers to the AI market. If this should change, antitrust policy is already capable of handling most clear threats to competition.
5.2	AI may reinforce tech monopolies.	Antitrust agencies already have the powers they need to stop problematic acquisitions and partnerships, but they should recognize that vertically integrated AI ecosystems are not inherently problematic and can have procompetitive effects that benefit consumers overall.

ENDNOTES

1. “March 20 ChatGPT Outage: Here’s What Happened,” *OpenAI Blog*, March 24, 2023, https://openai.com/blog/march-20-chatgpt-outage.

2. “2022 Annual Data Breach Report,” Identity Theft Resource Center, January 25, 2023, https://www.idtheftcenter.org/post/2022-annual-data-breach-report- reveals-near-record-number-compromises/.

3. Daniel Castro, “How Congress Can Fix ‘Internet of Things’ Security,” *The Hill*, October 28, 2016, http://thehill.com/blogs/pundits-blog/technology/303302-how-congress-can-fix-internet-of-things-security.

4. Ashley Johnson, “How Congress Can Foster a Digital Single Market in America” (ITIF, February 20, 2024), https://itif.org/publications/2024/02/20/how-congress-can-foster-a-digital-single-market-in-america/.

5. Lucian Constantin, “Opinion: Why we need a robust national standard for data breach notification,” *The Christian Science Monitor*, June 10, 2015, https://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0610/Opinion-Why-we-need-a-robust-national-standard-for-data-breach-notification.

6. Pranav Dixit, “A ‘silly’ attack made ChatGPT reveal real phone numbers and email addresses,” *Engadget*, November 29, 2023, https://www.engadget.com/a-silly-attack-made-chatgpt-reveal-real-phone-numbers-and-email-addresses-200546649.html.

7. Ibid.

8. Johnny Long, “Google Hacking for Penetration Testers,” *Black Hat USA 2005*, July 2005, https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf.

9. National Science and Technology Council, “National Strategy to Advance Privacy-Preserving Data Sharing and Analytics” (Washington, D.C., March 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-DataSharing-and-Analytics.pdf.

10. Joseph Williams and Lisa Nee, “Privacy Engineering,” *Computer*, Vol 55, No 10, October 2022, https://ieeexplore.ieee.org/document/9903879.

11. Morgan Stevens and Daniel Castro, “In the Wake of Generative AI, Industry-Led Standards for Data Scraping Are a Must” (Center for Data Innovation, September 1, 2023), https://datainnovation.org/2023/09/in-the-wake-of-generative-ai-industry-led-standards-for-data-scraping-are-a-must/.

12. Ibid.

13. Ashley Johnson and Daniel Castro, “Maintaining a Light-Touch Approach to Data Protection in the United States” (ITIF, August 8, 2022), https://itif.org/publications/2022/08/08/maintaining-a-light-touch-approach-to-data-protection-in-the-united-states/.

14. Daniel Castro, “Is Mona Lisa Happy? EU Would Ban AI That Could Answer This Question” (Center for Data Innovation, August 21, 2023), https://datainnovation.org/2023/08/is-mona-lisa-happy-eu-would-ban-ai-that-could-answer-this-question/.

15. Facial Recognition Technology Warrant Act of 2019, 116th Congress (2019), https://www.congress.gov/bill/116th-congress/senate-bill/2878.

16. Patrick Grother, Mei Ngan, and Kayee Hanaoka, “Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects” (NIST, December 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

17. Trades Union Congress, “Technology managing people: The worker experience,” November 2020, https://www.tuc.org.uk/sites/default/files/2020-11/Technology_Managing_People_Report_2020_AW_Optimised.pdf.

18. Joshua Wade et al., “A Pilot Study Assessing Performance and Visual Attention of Teenagers with ASD in a Novel Adaptive Driving Simulator” (NCBI, November 1, 2018), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5693648/pdf/nihms896479.pdf.

19. Lewis Maltby, “Employment Privacy: Is There Anything Left?” American Bar Association, May 1, 2013, https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/2013_vol_39/may_2013_n2_privacy/employment_privacy/.

20. Hodan Omaar, “Principles to Promote Responsible Use of AI for Workforce Decisions” (Center for Data Innovation, August 9, 2021), https://www2.datainnovation.org/2021-ai-workforce-decisions.pdf.

21. National Telecommunications and Information Administration, “Privacy Best Practice Recommendations For Commercial Facial Recognition Use,” accessed January 20, 2024, https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facia l_recogntion.pdf.

22. U.S. Equal Employment Opportunity Commission, “Artificial Intelligence and Algorithmic Fairness Initiative,” accessed April 26, 2024, https://www.eeoc.gov/ai.

23. Alan McQuinn and Daniel Castro, “A Grand Bargain on Data Privacy Legislation for America” (ITIF, January 14, 2019), https://itif.org/publications/2019/01/14/grand-bargain-data-privacy-legislation-america/.

24. Tim McNicholas, “New Jersey high school students accused of making AI-generated pornographic images of classmates,” *CBS News*, November 2, 2023, https://www.cbsnews.com/newyork/news/westfield-high-school-ai-pornographic-images-students/.

25. Betsy Morris, “Tech Companies Step Up Fight Against ‘Deepfakes’,” *The Wall Street Journal*, November 22, 2019, https://www.wsj.com/articles/tech-companies-step-up-fight-against-deepfakes-11574427345.

26. “Nonconsensual Distribution of Intimate Images,” Cyber Civil Rights Initiative, accessed January 9, 2024, https://cybercivilrights.org/nonconsensual-distribution-of-intimate-images/.

27. “‘Deep Fake’ or Synthetic Media Laws,” Cyber Civil Rights Initiative, accessed January 9, 2024, https://cybercivilrights.org/deep-fake-laws/.

28. Daniel Castro, “Blame Lawmakers, Not AI, for Failing to Prevent the Fake Explicit Images of Taylor Swift” (ITIF, January 28, 2024), https://itif.org/publications/2024/01/28/blame-lawmakers-not-ai-for-failing-to-prevent-fake-explicit-images-of-taylor-swift/.

29. Will Henshall, “Elon Musk Tells Rishi Sunak AI Will Eliminate the Need for Jobs,” *Time Magazine*, November 2, 2023, https://time.com/6331056/rishi-sunak-elon-musk-ai.

30. Anton Korinek, “Preparing the Workforce for an Uncertain AI Future,” *University of Virginia Darden School of Business blog*, November 1, 2023, https://news.darden.virginia.edu/wp-content/uploads/2023/11/Korinek_Statement_final.pdf.

31. Anton Korinek, “Scenario Planning for an A(G)I future” (International Monetary Fund, December 2023), https://www.imf.org/en/Publications/fandd/ issues/2023/12/Scenario-Planning-for-an-AGI-future-Anton-korinek.

32. “Countering the ‘Lump of Labor’ Fallacy: Two Lessons,” Federal Reserve Bank of St. Louis, January 6, 2021, https://www.stlouisfed.org/open-vault/2021/january/refuting-lump-labor-fallacy-two-lessons.

33. U.S. Department of Commerce, “News: Unemployment is at its Lowest Level in 54 years,” February 3, 2023, https://www.commerce.gov/news/blog/2023/02/news-unemployment-its-lowest-level-54-years.

34. Hodan Omaar, “NSF Data Shows AI Adoption in the United States Remains Low But Big Companies Are Leading the Way” (Center for Data Innovation, March 17, 2022), https://datainnovation.org/2022/03/nsf-data-shows-ai-adoption-in-the-united-states-remains-low-but-big-companies-are-leading-the-way/.

35. Ibid.

36. Robert D. Atkinson, “How to Reform Worker-Training and Adjustment Policies for an Era of Technological Change” (ITIF, February 2018), https://www2.itif.org/2018-innovation-employment-workforce-policies.pdf.

37. Claire Cain Miller and Courtney Cox, “In Reversal Because of A.I., Office Jobs Are Now More at Risk,” *The New York Times*, August 24, 2023 (updated August 30,2023), https://www.nytimes.com/2023/08/24/upshot/artificial-intelligence-jobs.html.

38. Louis Hyman, “The Problem with Blaming Robots for Taking Our Jobs,” *The New Yorker*, May 18, 2022, https://www.newyorker.com/books/under-review/the-problem-with-blaming-robots-for-taking-our-jobs.

39. Lydia DePillis and Steve Lohr, “Tinkering With ChatGPT, Workers Wonder: Will This Take My Job?” *The New York Times*, March 28, 2023, updated April 3, 2023, https://www.nytimes.com/2023/03/28/business/economy/jobs-ai-artificial-intelligence-chatgpt.html.

40. Ibid.

41. David Autor, “Applying AI to Rebuild Middle Class Jobs,” NBER Working Paper No. 32140, February 2024, https://www.nber.org/papers/w32140.

42. Shakked Noy and Whitney Zhang, “Experimental Evidence on the Productivity Effects of Generative Artificial Intelligence,” MIT, March 10, 2023, https://economics.mit.edu/sites/default/files/inline-files/Noy_Zhang_1_0.pdf.

43. Eric Egan, “Generative AI Offers Federal Agencies Common-Sense Opportunities to Simplify and Improve How They Work” (ITIF, June 28, 2023), https://itif.org/publications/2023/06/28/generative-ai-offers-federal-agencies-common-sense-opportunities-to-simplify-and-improve/.

44. Dan Evon, “ChatGPT Declines Request for Poem Admiring Trump, But Biden Query Is Successful,” *Snopes*, February 1, 2023, https://www.snopes.com/fact-check/chatgpt-trump-admiring-poem/.

45. Tom Warren, “Google apologizes for ‘missing the mark’ after Gemini generated racially diverse Nazis,” *The Verge*, February 21, 2024, https://www.theverge.com/2024/2/21/24079371/google-ai-gemini-generative-inaccurate-historical.

46. Derek Robertson, “The problem behind AI’s political ‘bias’,” *Politico*, August 24, 2023, https://www.politico.com/newsletters/digital-future-daily/2023/08/24/the-tricky-problem-behind-ai-bias-00112845.

47. Jeremy Baum and John Villasenor, “The politics of AI: ChatGPT and political bias” (Brookings, May 8, 2023), https://www.brookings.edu/articles/the-politics-of-ai-chatgpt-and-political-bias/.

48. Warren, “Google apologizes for ‘missing the mark’ after Gemini generated racially diverse Nazis.”.

49. Ibid.

50. Jochen Hartman et al., “The political ideology of conversational AI: Converging evidence on ChatGPT's pro-environmental, left-libertarian orientation,” preprint *arXiv*, January 5, 2023, https://arxiv.org/abs/2301.01768.

51. Steve Contorno and Donie O’Sullivan, “DeSantis campaign posts fake images of Trump hugging Fauci in social media video,” *CNN*, June 8, 2023, https://www.cnn.com/2023/06/08/politics/desantis-campaign-video-fake-ai-image/index.html.

52. “FEC moves toward potentially regulating AI deepfakes in campaign ads,” *PBS,* August 10, 2023, https://www.pbs.org/newshour/politics/fec-moves-toward-potentially-regulating-ai-deepfakes-in-campaign-ads.

53. Morris, “Tech Companies Step Up Fight Against ‘Deepfakes’.”.

54. Daniel Castro, “Testimony to the Alaska State Senate Regarding AI, Deepfakes, Cybersecurity, and Data Transfers” (ITIF, February 2, 2024), https://itif.org/publications/2024/02/02/testimony-to-the-alaska-state-senate-regarding-ai-deepfakes-cybersecurity-and-data-transfers/.

55 Ibid.

55. Shane Goldmacher, “A Campaign Aide Didn’t Write That Email. A.I. Did,” *The New York Times*, March 28, 2023, https://www.nytimes.com/2023/03/28/us/politics/artificial-intelligence-2024-campaigns.html.

56. Thor Benson, “The Disinformation Is Just for You,” *Wired,* August 1, 2023, https://www.wired.com/story/generative-ai-custom-disinformation/

57. Gillian Diebold, “States Should Update Digital Literacy Programs to Include AI Literacy” (Center for Data Innovation, March 9, 2023), https://datainnovation.org/2023/03/states-should-update-digital-literacy-programs-to-include-ai-literacy/

58. Scott Babwah Brennen and Matt Perault, “Policy frameworks for political ads in an age of AI” (Center on Technology Policy at the University of North Carolina at Chapel Hill, November 2023), https://techpolicy.unc.edu/wp-content/uploads/2023/11/GAI-and-political-ads.pdf.

59. Federal Trade Commission, “FTC Chair Khan and Officials from DOJ, CFPB, and EEOC Release Joint Statement on AI,” April 25, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/04/ftc-chair-khan-officials-doj-cfpb-eeoc-release-joint-statement-ai.

60. Ryan Heath, “AI’s Loneliness Crisis,” *Axios*, May 15, 2023, https://www.axios.com/2023/05/15/ai-loneliness-crisis-mental-health-pets.

61. Christina Jackson, “Humans Seek Connections with AI Chatbots,” *Voice of America Learning English*, February 15, 2024, https://learningenglish.voanews.com/a/humans-seek-connections-with-ai-chatbots/7487601.html.

62. Heather Kelly and Will Oremus, “We spent a year talking to lonely people. Here’s what we learned,” *The Washington Post*, December 19, 2023, https://www.washingtonpost.com/technology/2023/12/19/social-media-loneliness/.

63. Ryan C. Moore, Jeffrey T. Hancock, and Jeremy N. Bailenson, “From 65 to 103, Older Adults Experience Virtual Reality Differently Depending on Their Age: Evidence from a Large-Scale Field Study in Nursing Homes and Assisted Living Facilities,” Cyberpsychology, Behavior, and Social Networking 26, no. 12 (December 2023): 886–895, doi:10.1089/cyber.2023.0188, https://pubmed.ncbi.nlm.nih.gov/38011717/.

64. Reva Scwartz et al., *Toward a Standard of Identifying and Managing Bias in Artificial Intelligence* (March 2022), National Institute of Standards and Technology (NIST), U.S. Department of Commerce, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf.

65. Rohit Chopra et al., “Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems,” Federal Trade Commission, https://www.ftc.gov/system/files/ftc_gov/pdf/EEOC-CRT-FTC-CFPB-AI-Joint-Statement%28final%29.pdf.

66. National Telecommunications and Information Administration, “AI Accountability Policy Report,” March 27, 2024, https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report.

67. Joshua New and Daniel Castro, “How Policymakers Can Foster Algorithmic Accountability” (Center for Data Innovation, May 21, 2018), https://www2.datainnovation.org/2018-algorithmic-accountability.pdf.

68. Ibid.

69. Gillian Diebold, “Closing the Data Divide for a More Equitable U.S. Digital Economy” (Center for Data Innovation, August 22, 2022), https://www2.datainnovation.org/2022-closing-data-divide.pdf.

70. Jon Kleinberg and Manish Raghavan, “Algorithmic monoculture and social welfare,” PNAS (2021), https://doi.org/10.1073/pnas.2018340118.

71. Atila Abdulkadiroglu, Nikhil Agarwal, and Parag A. Pathak, “The Welfare Effects of Coordinated Assignment: Evidence from the NYC HS Match,” National Bureau of Economic Research, 2015, https://www.nber.org/system/files/working_papers/w21046/w21046.pdf.

72. Ayesha Bhatti, “The UK’s Agile, Sector-Specific Approach to AI Regulation Is Promising” (Center for Data Innovation, February 7, 2024), https://datainnovation.org/2024/02/an-agile-sector-specific-approach-to-uk-ai-regulation-is-promising/.

73. Rana Foroohar, “We must stop AI replicating the problems of surveillance capitalism,” *Financial Times*, November 6, 2023, https://www.ft.com/content/d9063c16-a4d2-4580-b8f6-a4872083d0fa.

74. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books: London, 2018).

75. Benjamin Mueller and Daniel Castro, "The Value of Personalized Advertising in Europe" (Center for Data Innovation, November 2021), https://datainnovation.org/2021/11/the-value-of-personalized-advertising-in-europe/.

76. Benjamin Mueller, "Proposals to Restrict Targeted Ads Make Even Less Sense With Recent Innovations in AdTech" (Center for Data Innovation, July 2022), https://datainnovation.org/2022/07/proposals-to-restrict-targeted-ads-make-even-less-sense-with-recent-innovations-in-adtech/.

77. Morgan Stevens, "The FTC Should Avoid Unduly Restricting the US AI Industry" (Center for Data Innovation, August 2023), https://datainnovation.org/2023/08/the-ftc-should-avoid-unduly-restricting-the-us-ai-industry/.

78. Ann O'Brien et al., "AI Under the Antitrust Microscope: Competition Enforcers Focusing on Generative AI from All Angles," Sheppard Mullin Antitrust Law Blog, August 9, 2023, https://www.antitrustlawblog.com/2023/08/articles/criminal-doj/ai-under-the-antitrust-microscope-competition-enforcers-focusing-on-generative-ai-from-all-angles.

79. "Generative AI Raises Competition Concerns," Federal Trade Commission, June 29, 2023, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns.

80. Adam Zewe, "Synthetic Data Can Offer Real Performance Improvements," *MIT News*, November 3, 2022, https://news.mit.edu/2022/synthetic-data-ai-improvements-1103.

81. "Anthropic Partners with Google Cloud," Anthropic, February 3, 2023, https://www.anthropic.com/news/anthropic-partners-with-google-cloud.

82. Jacob Kastrenakes, "Nvidia Is Launching a New Must-Have AI Chip — as Customers Still Scramble for Its Last One," *The Verge*, November 13, 2023, https://www.theverge.com/2023/11/13/23958823/nvidia-h200-ai-gpu-announced-specs-release-date.

83. Emilia David, "Chip Race: Microsoft, Meta, Google, and Nvidia Battle It Out for AI Chip Supremacy," *The Verge*, February 1, 2024, https://www.theverge.com/2024/2/1/24058186/ai-chips-meta-microsoft-google-nvidia.

84. "Generative AI Raises Competition Concerns," Federal Trade Commission, June 29, 2023, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/06/generative-ai-raises-competition-concerns.

85. Ela Głowicka and Jan Málek, "Digital Empires Reinforced? Generative AI Value Chain," *Network Law Review*, March 18, 2024, https://www.networklawreview.org/glowicka-malek-generative-ai/.

86. Ibid.

87. US. Department of Justice and the Federal Trade Commission, Horizontal Merger Guidelines, August 19, 2010, 2, https://www.justice.gov/atr/horizontal-merger-guidelines-08192010.

88. "Building an early warning system for LLM-aided biological threat creation," *OpenAI*, January 31, 2024, https://openai.com/research/building-an-early-warning-system-for-llm-aided-biological-threat-creation.

89. Steph Batalis, “AI and Biorisk: An Explainer” (CSET, December 2023), https://cset.georgetown.edu/publication/ai-and-biorisk-an-explainer/.

90. Steph Batalis, “Can Chatbots Help You Build a Bioweapon?” *Foreign Policy,* November 5, 2023, https://foreignpolicy.com/2023/11/05/ai-artificial-intelligence-chatbot-bioweapon-virus-bacteria-genetic-engineering/.

91. Ibid.

92. Brendan Bordelon, “The fight over AI biosecurity risk takes a twist,” *Politico*, February 6, 2024, https://www.politico.com/newsletters/digital-future-daily/2024/02/06/the-fight-over-ai-biosecurity-risk-takes-a-twist-00139945.

93. Nazish Jeffery et al., “Bio X AI: Policy Recommendations For A New Frontier,” FAS, December 12, 2023, https://fas.org/publication/bio-x-ai-policy-recommendations/.

94. Madhumita Murgia, “DeepMind research cracks structure of almost every known protein,” *Financial Times*, https://www.ft.com/content/6a088953-66d7-48db-b61c-79005a0a351a.

95. Steph Batalis, “AI and Biorisk: An Explainer.”

96. Ibid

97. Nazish Jeffery et al., “Bio X AI: Policy Recommendations For A New Frontier.”

98. Ian Hogarth, “We must slow down the race to God-like AI,” *Financial Times*, April 13 2023, https://www.ft.com/content/03895dc4-a3b7-481e-95cc-336a524f2ac2.

99. Ibid.

100. Remco Zwetsloot and Allan Dafoe, “Thinking About Risks From AI: Accidents, Misuse and Structure,” *Lawfare blog*, February 11, 2019, https://www.lawfaremedia.org/article/thinking-about-risks-ai-accidents-misuse-and-structure.

101. Hodan Omaar, “Preparing for an AI Apocalypse Is As Preposterous As Preparing for an Alien Invasion” (Center for Data Innovation, June 2023), https://datainnovation.org/2023/06/preparing-for-an-ai-apocalypse-is-as-preposterous-as-preparing-for-an-alien-invasion/.

102. Daniel Castro, “Policymakers Should Use the SETI Model to Prepare for AI Doomsday Scenarios” (Center for Data Innovation, December 2023), https://datainnovation.org/2023/12/policymakers-should-use-the-seti-model-to-prepare-for-ai-doomsday-scenarios/.

103. Donna Lu, “Creating an AI can be five times worse for the planet than a car,” *New Scientist*, June 6, 2019, https://www.newscientist.com/article/2205779-creating-an-ai-can-be-five-times-worse-for-the-planet-than-a-car/.

104. Alex De Vries, “The Growing Energy Footprint of Artificial Intelligence,” Joule 7, no. 10 (October 1, 2023): 2191–94, https://doi.org/10.1016/j.joule.2023.09.004.

105. Lauren Leffer, “The AI Boom Could Use a Shocking Amount of Electricity,” *Scientific American*, October 13, 2023, https://www.scientificamerican.com/article/the-ai-boom-could-use-a-shocking-amount-of-electricity/.

106. Colin Cunliff, Ashley Johnson, and Hodan Omaar, “How Congress and the Biden Administration Could Jumpstart Smart Cities With AI” (ITIF, March 2021), https://www2.itif.org/2021-smart-cities-ai.pdf.

107. Hodan Omaar, “Innovation Wars: Episode AI - The Techlash Strikes Back” (Center for Data Innovation, January 2022), https://datainnovation.org/2022/01/innovation-wars-episode-ai-the-techlash-strikes-back/.

108. Daniel Castro, “Rethinking Concerns About AI’s Energy Use” (Center for Data Innovation, January 2024), https://www2.datainnovation.org/2024-ai-energy-use.pdf.

109. Aswin Prabhakar, “The New York Times’ Copyright Lawsuit Against OpenAI Threatens the Future of AI and Fair Use” (Center for Data Innovation, January 2024), https://datainnovation.org/2024/01/the-new-york-times-copyright-lawsuit-against-openai-threatens-the-future-of-ai-and-fair-use/.

110. James Vincent, “Getty Images sues AI art generator Stable Diffusion in the US for copyright infringement,” *The Verge*, February 6, 2023, https://www.theverge.com/2023/2/6/23587393/ai-art-copyright-lawsuit-getty-images-stable-diffusion.

111. David Salazar, “Music publishers just sued Claude AI maker Anthropic over song lyrics,” *Fast Company*, October 20, 2023, https://www.fastcompany.com/90970093/umg-abkco-concord-sue-anthropic-ai-copyright-infringement.

112. Daniel Castro, “Critics of Generative AI Are Worrying About the Wrong IP Issues” (Center for Data Innovation, March 2023), https://datainnovation.org/2023/03/critics-of-generative-ai-are-worrying-about-the-wrong-ip-issues/.

113. United States Patent and Trademark Office, “Copyright basics,” accessed January 23, 2024, https://www.uspto.gov/ip-policy/copyright-policy/copyright-basics.

114. Peter Henderson et al., “Foundation Models and Copyright Questions,” HAI Policy & Society, November 2023, https://hai.stanford.edu/sites/default/files/2023-11/Foundation-Models-Copyright.pdf.

115. Ibid.

116. Ibid.

117. Will Douglas Heaven, “Here’s Proof You Can Train an AI Model Without Slurping Copyrighted Content,” *Wired*, March 20, 2024, https://www.wired.com/story/proof-you-can-train-ai-without-slurping-copyrighted-content/

118. Ibid.

119. “Recent Cases,” Musicians Institute Library, December 2, 2022, https://library.mi.edu/musiccopyright/currentcases.

120. Hodan Omaar, “Congress Should Fund the Creation of a Similarity Checker for Music” (Center for Data Innovation, April 2024), https://datainnovation.org/2024/04/congress-should-fund-the-creation-of-a-similarity-checker-for-music/.

121. S. Sean Tu, “Use of Artificial Intelligence to Determine Copyright Liability for Musical Works,” *West Virginia Law Review* 123, no. 835 (2021): 1–38,

posted October 1, 2020, revised May 15, 2023, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3617300.

122. Patrick Coffee, “Can Congress Save MrBeast and Tom Hanks From AI Deepfakes?” *The Wall Street Journal*, November 6, 2023, https://www.wsj.com/articles/legislators-aim-to-help-celebrities-and-consumers-fight-deepfake-scam-ads-8d490bc6.

123. Adam White, “AI-generated song mimicking Drake and The Weeknd submitted for Grammy consideration,” *The Independent*, September 7, 2023, https://www.independent.co.uk/arts-entertainment/music/news/drake-and-weeknd-ai-song-heart-on-my-sleeve-b2406902.html.

124. United States Copyright Office, “Authors, Attribution, and Integrity: Examining Moral Rights in the United States,” April 2019, https://www.copyright.gov/policy/moralrights/full-report.pdf.

125. “Deepfake AI voice cloning detection against impersonation fraud,” Enterprise Europe Network, accessed February 20, 2024, https://een.ec.europa.eu/partnering-opportunities/deepfake-ai-voice-cloning-detection-against-impersonation-fraud.

126. Ben Buchanan et al., “Automating Cyber Attacks” (Center for Security and Emerging Technology, November 2020), https://cset.georgetown.edu/publication/automating-cyber-attacks/

127. Ibid.

128. Ibid.

129. GAO, “Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure,” Feb 7, 2023, https://www.gao.gov/products/gao-23-106441.

130. GAO, “Cybersecurity High-Risk Series: Challenges in Securing Federal Systems and Information,” January 31, 2023, https://www.gao.gov/products/gao-23-106428.

131. White House Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, October 30, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

132. CISA, “Roadmap for Artificial Intelligence,” November 2023, https://www.cisa.gov/sites/default/files/2023-11/2023-2024_CISA-Roadmap-for-AI_508c.pdf.

133. International Information System Security Certification Consortium, “How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce,” October 31, 2023, https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=52055d08ca644293bd7497725bb7fcb4.

134. Daniel Castro, “Tracking AI Incidents and Vulnerabilities” (Center for Data Innovation, April 4, 2024), https://datainnovation.org/2024/04/tracking-ai-incidents-and-vulnerabilities.

ABOUT THE AUTHORS

Hodan Omaar is a senior policy manager at the Center for Data Innovation. Previously, she worked as a senior consultant on technology and risk management in London and as an economist at a blockchain start-up in Berlin. She has an M.A. in Economics and Mathematics from the University of Edinburgh.

Daniel Castro is the director of the Center for Data Innovation and vice president of the Information Technology and Innovation Foundation. He has a B.S. in foreign service from Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

ABOUT THE CENTER FOR DATA INNOVATION

The Center for Data Innovation studies the intersection of data, technology, and public policy. With staff in Washington, London, and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as open data, artificial intelligence, and the Internet of Things. The Center is part of the Information Technology and Innovation Foundation (ITIF), a nonprofit, nonpartisan think tank.

Contact: info@datainnovation.org

datainnovation.org