| | |
|---|---|
| In the Matter of | ) |
| AI Accountability Policy Request for Comment | ) |
| | )    Docket No. 230407-0093 |
| | ) |
| | ) |

## COMMENTS OF PUBLIC KNOWLEDGE

Nicholas P. Garcia
Policy Counsel
Public Knowledge
1818 N Street, NW
Suite 410
Washington, DC 20036

June 12, 2023

## I.    INTRODUCTION

AI, as broadly defined in the National Telecommunication and Information Administration (NTIA) Request for Comment (RFC)[1], encompasses a variety of different technologies, approaches, and use cases. It is a field of development that is changing rapidly, with all the excitement, uncertainty, confusion, speculation, and hope that accompanies any potentially transformative new technology. Critics and optimists alike can envision the application of AI in almost every area imaginable, including some that even a few years ago many would have firmly defended as the sole domain of humans. But whether that AI-saturated future is one of promise or danger turns on the decisions we are called to make now. With a wide potential scope of applicability, comes a broad spectrum of risks and potential issues, many of which may be difficult to even imagine today.

Approaching the issue of AI accountability and regulation therefore requires a perspective of caution and humility. It is easy to look back on regulatory efforts from the early days of computers and the internet and see laws and policies—many of which we are still living with—that missed the mark; not because of misaligned intentions or lack of state-of-the-art knowledge, but because of a narrow view of the technology as it currently existed and reliance on rigid or overly prescriptive models that failed to evolve with the times and technology. In other domains, policymakers failed to take action at all, allowing practices like commercial surveillance, addictive attention-based design, and anticompetitive consolidation to take hold. To put a fine point on it: when it comes to AI accountability and assurance, even the best methods or

---

[1] AI Accountability Policy Request for Comment,  88 FR 22433 (Apr. 13, 2023), Docket No. 230407-0093, https://www.federalregister.gov/documents/2023/04/13/2023-07776/ai-accountability-policy-request-for-comment ("AI Accountability RFC").

recommendations of today may be insufficient to meet the challenges of tomorrow, much less the uncertainties of the next years or decades.

Therefore, the most important actions that we can take now are to establish durable and responsive approaches for the ongoing challenge of AI policymaking. We need a combination of expertise and adaptability to rise to this challenge. We prescribe a hybrid approach of reliance on our sector specific regulators, already deeply embedded in the domains that matter to us most, to avert immediate and anticipated harms, while also cultivating new expertise with a centralized AI regulator that can adapt with the technology and provide a broader view of the full ecosystem.

But policymakers cannot simply pass these challenges off to regulators: effective AI accountability will require groundwork to ensure a healthy AI ecosystem. First, experts and policymakers need to break down existing barriers to effective AI accountability. We must address uncertainty about where liability lies for AI-driven harms to ensure that stakeholders in every phase of the AI lifecycle are contributing responsibly to the overall health of our AI ecosystem. Second, oversight and accountability must be coupled with policies and investments that will promote continued innovation, responsible research, open access, and vigorous competition. AI technologies have enormous potential, and the overall goal of any regulatory system should be realizing that potential, not overburdening its development or allowing its benefits to be inequitably captured. And third, there is still a lot of catching up to do from the last technology revolution. By addressing the worst excesses of the Information Age that policymakers didn't anticipate, we can establish a healthier environment for the progress of AI. A sector specific digital regulator for online platforms and a comprehensive privacy law are long overdue steps that are urgently needed now, but will also leave us better prepared for the future.

## II. AI ACCOUNTABILITY MEASURES MUST BE ENFORCEABLE AND DEMOCRATICALLY CONTROLLED

Accountability mechanisms such as certifications, audits, and assessments serve a crucial purpose in establishing a trustworthy and socially beneficial AI ecosystem. Questions 1 and 2 ask about the purpose of accountability mechanisms and what their value is.[2] These procedures ought to be viewed as potential tools which will likely need to be deployed alongside other regulatory instruments to build a trustworthy and publicly beneficial AI ecosystem. It is important to recognize that these procedures alone cannot ensure accountable AI. The function of certifications, audits, assessments, and testing should not be to create a set of "trust seals" for a more informed marketplace or to simply reward good actors. Rather, to ensure their effectiveness, certifications, audits, assessments, and testing should be supported by an enforceable regulatory framework, drawing upon existing consumer, product, and public safety regulations.

It is imperative to move beyond mere auditing and develop a comprehensive oversight process for AI. AI systems operate as black boxes, necessitating specialized regulatory oversight. Although transparency requirements have long been part of consumer protection measures, the nature of transparency in the AI context is distinct. Transparency could involve providing explanations of algorithmic decisions to affected users, conducting independent audits prior to AI deployment, or enabling regulators to thoroughly examine models, even when trade secrets or intellectual property laws protect them. Implementing transparency requirements for AI would necessitate deciding who the requirements are meant to benefit, and who is responsible for ensuring compliance. The federal government should spearhead the implementation of transparency requirements to ensure universal adherence and regular accuracy testing.

---

[2] AI Accountability RFC, Questions 1, 2.

AI audits and assessments should encompass a range of accountability metrics, addressing human rights, privacy protection, security, and diversity, equity, inclusion, and accessibility goals. These broader considerations are crucial to promoting a fair and equitable AI ecosystem.

Given the rapidly evolving nature of AI technology, current state of the art answers about specific auditing, assessment, and testing methodologies may become outdated as the technology continues to rapidly change and develop. For instance, recent developments like prompt injection in response to the widespread deployment of Large Language Models (LLMs) highlight the need for adaptable approaches. Similarly, totally different auditing and assessment models will be required for discriminative and generative systems, and more context-specific needs are likely to become apparent as deployment of AI systems start to interact with existing structures. Instead of fixating on current best practices, emphasis should be placed on building long-term capacity for maintaining expert knowledge and updating standards and practices in an enforceable manner.

Effective government oversight of AI systems will involve active participation in the writing and development of assessments. By shaping assessment criteria, the government prevents private entities from hijacking accountability measures and ensuring that evaluations remain aligned with the public interest. This approach will lead to robust standards that address transparency, privacy, security, and fairness, enabling comprehensive evaluations and continuous improvement. Government involvement in assessment development also fosters democracy and inclusivity by ensuring diverse stakeholder input and enhancing public trust in the oversight process.

## III. AI REQUIRES EXPERT AND ADAPTABLE REGULATION

NTIA has asked what role government policy should play in the AI accountability ecosystem, and whether that policy should be sectoral, horizontal, or a combination of the two.[3] Because AI technologies have enormous potential to be used for good—or to exacerbate inequality, undermine civil liberties, and supercharge information disorder[4]—oversight and accountability cannot be left to industry standards, corporate policies, or voluntary certifications. Government must take a leading role; we need expert regulators with the power to prevent AI-based harms and enforce AI accountability policies and standards. The development of an innovative, trustworthy, and publicly beneficial AI sector is contingent on having well-informed and flexible regulators to enact government AI policy.

Given AI's potential application across varied domains, each presenting potentially unique risks or challenges, a combined sectoral and horizontal regulation scheme is essential. Expertise and adaptability are the essential elements of an effective technology regulation environment. That means taking advantage of existing regulatory structures where experience already resides—such as with housing, financial, and consumer protection authorities—while also cultivating new AI-specific expertise and oversight capacities. We can and should rely on existing regulators to tackle the harms within their jurisdictions, while also empowering a new AI-specific federal regulator that can provide coordination, expertise, and oversight across the field more broadly.

---

[3] AI Accountability RFC, Questions 30 and 30(a)

[4] Claire Wardle & Hossein Derakhshan, *INFORMATION DISORDER: Toward an interdisciplinary framework for research and policy making* (Sep. 27, 2017), Council of Europe Report DGI(2017)09, https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77.

### A. Sector Specific Regulators

As PK noted in a 2018 policy paper on AI regulation, AI will inevitably permeate the jurisdictions of numerous existing government agencies that cater to specific sectors.[5] Rather than be defined by sweeping legislative efforts, the twentieth century was marked by a substantial surge in the quantity and importance of executive and independent regulators. These regulators address the increasingly intricate and specialized policy challenges arising from an advanced economy. Consequently, there are already well-developed structures for tackling some of the potential risks associated with AI systems. Existing sectoral regulators are generally already empowered to identify and deal with harms that flow from the use of AI. Whether it be issues of discrimination, consumer protection, or health and safety, it must be the clear policy of the United States that the use of novel technology like AI does not bypass existing safeguards and protections.

The White House has already taken strides down this road in the wake of the release of the Blueprint for an AI Bill of Rights.[6] An OSTP fact sheet described how numerous departments and agencies are applying their existing powers and expertise to the problems of their domain. For example, the Equal Employment Opportunity Commission (EEOC) and Department of Justice (DOJ) began updating guidance on antidiscrimination policies to account for algorithmic screening technologies,[7] the Consumer Financial Protection Bureau (CFPB) affirmed its longstanding rules about explanatory requirements for adverse financial decisions

---

[5] Ryan Clough, *The Inevitability of AI Law & Policy: Preparing Government for the Era of Autonomous Machines* (Oct. 2018), Public Knowledge, https://publicknowledge.org/policy/the-inevitability-of-ai-law-policy-preparing-government-for-the-era-of-autonomous-machines/ ("2018 PK AI Policy Paper").

[6] *Blueprint for an AI Bill of Rights*, The White House Office of Science and Technology Policy, available at https://www.whitehouse.gov/ostp/ai-bill-of-rights/ (last accessed Jun. 12, 2023) ("WH Blueprint").

[7] Artificial Intelligence and Algorithmic Fairness Initiative, Equal Employment Opportunity Commission, https://www.eeoc.gov/ai (last accessed Jun. 12, 2023); U.S. EEOC and U.S. Department of Justice Warn against Disability Discrimination (May 12, 2022), Equal Employment Opportunity Commission, https://www.eeoc.gov/newsroom/us-eeoc-and-us-department-justice-warn-against-disability-discrimination.

from creditors,[8] and the Department of Housing and Urban Development (HUD) provided

guidance about how AI systems used to screen tenants may violate the Fair Housing Act.[9] The

Federal Trade Commission (FTC), DOJ, CFPB, and the EEOC also issued a joint pledge to

enforce their respective laws and regulations against harmful automated systems.[10] The FTC has

gone even further stating in a New York Times OpEd that the Commission's full competition and

consumer protection authority will be used to make sure that "we continue to be the home of

world-leading technology without accepting race-to-the-bottom business models and

monopolistic control."[11] These actions highlight that, while the technology may be new, the

potential harms or misuse cases are familiar: discrimination, for example, is still discrimination

whether it comes from an AI system or not. Placing a shiny technological veneer over prohibited

practices cannot be allowed to thwart the clear jurisdiction of regulators.

In addition, these swift actions to head off issues stemming from the application of new

technologies in familiar domains highlights the value of enabling expert regulators to make

reasoned evaluations of the pressing risks in their domain and develop an effective response.

Question 17 asks about how AI accountability measures should be scoped depending on the risk

of the technology or deployment context. The simple, if unsatisfying, answer is that it may be

highly contextual and best left to sector specific regulators to make those evaluations of risk and

---

[8] Adverse action notification requirements in connection with credit decisions based on complex algorithms (May 26, 2022), Consumer Financial Protection Circular 2022-03, https://www.consumerfinance.gov/compliance/circulars/circular-2022-03-adverse-action-notification-requirements-in-connection-with-credit-decisions-based-on-complex-algorithms/.

[9] Justice Department Files Statement of Interest in Fair Housing Act Case Alleging Unlawful Algorithm-Based Tenant Screening Practices (Jan. 9, 2023), Department of Justice Office of Public Affairs, https://www.justice.gov/opa/pr/justice-department-files-statement-interest-fair-housing-act-case-alleging-unlawful-algorithm.

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

[11] Lina Khan, *Lina Khan: We Must Regulate A.I. Here's How* (May 3, 2023) The New York Times, https://www.nytimes.com/2023/05/03/opinion/ai-lina-khan-ftc-technology.html.

the sensitivity of the deployment contexts in the domains that they handle. Embracing a general standard, like the "sensitive domains" standard in the Blueprint,[12] might seem more parsimonious but could lead to over- and under-inclusion that might actually hamper effective enforcement by overburdening a regulator unnecessarily in some areas and inadvertently missing other contexts where the potential harm is significant but only a sector specific regulator might be aware of the issue.

This growing trend of action should not lull policymakers into a false sense of ease, however. While sector specific regulators are acting based on their existing authorities, they may not always have the resources they need to do their job effectively. Increased staffing, especially with allowances for more technologists, would bolster enforcement efforts. Additionally, where necessary new rules and statutory authority may be necessary to shore up gaps and loopholes to ensure regulators have the ability to address AI accountability issues effectively.

### B. The United States Needs An Expert AI Regulator

The field of AI comprises many different technologies, technical approaches, and use cases. It has grown both steadily and also in surprising leaps and bounds that have often taken policymakers, and the public, by surprise. It is also a field with both tremendous potential and risk. While existing sector specific regulators are well-suited to taking on existing and emerging harms in their own domains, AI technology is too important, wide-ranging, and technically complex to rely on disjointed regulatory efforts. Therefore, Congress must either dramatically expand the jurisdiction of an existing agency or create a new agency specifically charged to regulate AI.

---

[12] WH Blueprint, *Definitions*, available at https://www.whitehouse.gov/ostp/ai-bill-of-rights/definitions/ (last accessed Jun. 12, 2023).

PK's 2018 policy paper on AI regulation outlined five key advantages and essential features of a expert AI authority: (1) bolstering sector-specific regulators and confronting overarching policy challenges raised by AI; (2) protecting public values in government procurement and implementation of AI; (3) attracting AI practitioners to civil service, and building centralized and durable AI expertise within government; (4) identifying major gaps in the laws and regulatory frameworks that govern AI; and (5) coordinating strategies and priorities for international AI governance.[13] These features have only become more critical in the five years since the paper was published. While the paper does not reflect the latest developments in AI technology, its discussion of the importance of the role of an expert AI regulator has only increased in relevance.

While the 2018 paper focused exclusively on the five features listed above, it has become apparent that an expert federal regulator with rulemaking and enforcement authority over the AI sector is not only necessary, but would be warmly welcomed by key stakeholders including industry leaders like Open AI,[14] Google,[15] and Microsoft.[16] Going beyond serving as an expert coordinating agency that oversees government action into regulation of private AI development and deployment would necessitate a broad, public interest focused mandate and carefully crafted authority to allow the agency to remain maximally flexible. An expert regulator would be able to make nuanced judgements about the technology, bypassing the need for speculative or narrow

---

[13] 2018 PK AI Policy Paper at 2,3.
[14] Cecilia Kang, OpenAI's Sam Altman Urges A.I. Regulation in Senate Hearing (May 16, 2023), The New York Times, https://www.nytimes.com/2023/05/16/technology/openai-altman-artificial-intelligence-regulation.html.
[15] Kent Walker, A Shared agenda for responsible AI progress (Mar. 28, 2023), The Keyword, https://blog.google/technology/ai/a-shared-agenda-for-responsible-ai-progress/ ("When it comes to AI, we need both good individual practices and shared industry standards. But society needs something more: Sound government policies that promote progress while reducing risks of abuse…As we've said for years, AI is too important not to regulate — and too important not to regulate well.").
[16] Brad Smith, *How do we best govern AI?* (May 25, 2023), Microsoft. https://blogs.microsoft.com/on-the-issues/2023/05/25/how-do-we-best-govern-ai/ ("There will then be a need to develop new law and regulations for highly capable AI foundation models, best implemented by a new government agency.").

legislative prescriptions; it is important to avoid the kinds of technology classification problems

that have occasionally stymied other regulators like the Federal Communications Commission.

With experts at the wheel, able to adapt to the changing technology and its ongoing

implementation, researchers and companies, sector specific regulators would be able to focus on

their areas of expertise rather than scrambling to fill gaps in our national AI policy. In addition to

being the most effective strategy for achieving the public interest mandates mentioned above,

this would also be a boon for innovation because "an agency with broader authority over

autonomous systems, cutting across multiple sectors and applications, will be more likely to

prioritize innovation and technological development, particularly if they are written into its

founding mandate."[17]

While we encourage NTIA to review the paper in full, a few key points from that paper

are directly responsive to questions in the instant proceeding. Questions 19 and 30(D) both ask

about how government should approach assessment and accountability for its own AI systems.[18]

An important function of an expert AI regulator would be to coordinate standards for

government adoption and implementation of AI systems. An expert AI regulator could set, and

oversee, standards for the development, acquisition, and ongoing assessment of AI systems

across the government. This would create uniformity, ensure that public values are respected, and

enhance public trust in government AI systems.

Question 34 asks "Is it important that there be uniformity of AI accountability

requirements and/or practices across the United States? Across global jurisdictions?" The extent

to which accountability requirements are universalizable across sectors given the varied

technologies and use cases is a complex analysis but suited to ongoing technical analysis.

---

[17] 2018 PK AI Policy Paper at 33.
[18] AI Accountability RFC, Questions 19, 30(d).

Certainly uniformity would provide researchers and developers confidence about the systems they are building and has value for independent watchdogs and civil society organizations that wish to provide oversight of AI systems as they are deployed. All this is to say that, to the extent uniformity is desirable, a single expert regulator is the simplest model for centralizing the analysis, adoption, and oversight of such standards. In addition, the a patchwork framework of sector specific regulators and various agencies independently attempting to develop AI competence without a single expert AI agency poses a significant challenge to international efforts to coordinate accountability requirements.

## IV. BREAK DOWN BARRIERS TO ACCOUNTABILITY THROUGHOUT THE AI ECOSYSTEM

Policymakers must break down barriers and address uncertainties surrounding effective AI accountability. A key obstacle we wish to emphasize is the lack of clarity regarding liability at different phases of the AI ecosystem, as raised in Questions 15 and 16.[19] In order to safeguard innovation and develop an effective accountability system, it is essential to establish a clear understanding of which actors bear responsibility for what. This clarity is especially important to ensure that harms can be adequately addressed and also so that academic researchers, new market entrants, and users can engage with AI with clarity about their responsibilities and confidence surrounding their risk.

The AI ecosystem involves four main participants: developers and creators of the foundational model, implementers or deployers of the model, data providers contributing to the model, and the end users of the system. Assigning liability based on the entity that caused the harm is generally the preferred approach. For instance, if harm arises from poorly sourced or

---

[19] AI Accountability RFC, Questions 15, 16.

inaccurate data, the data provider should be held responsible. If there are flaws in the underlying design of the model, the developer should shoulder the blame. If flawed implementation or inappropriate use of a foundational model in a specific deployment context leads to harm, the system's deployer should be held accountable. Lastly, if an end user employs the program for illegal or unethical purposes, the user themselves should be liable.

Unfortunately, identifying the party responsible for introducing problems into the AI system can be challenging, even though the resulting harms may be evident. While much has been written on different legal regimes and their effectiveness in addressing AI-related harms,[20] less attention has been given to determining the specific entities in the chain of development and use who bear responsibility. By clarifying these points and addressing the lack of liability clarity, policymakers can establish a framework that ensures accountability while nurturing innovation and protecting the interests of researchers, users, and startups.

To accomplish this, it is crucial for experts and policymakers to collaborate in removing existing barriers to effective AI accountability. This includes fostering a shared understanding among stakeholders throughout the AI lifecycle and encouraging responsible contributions to the overall health of the AI ecosystem. Instead of shifting responsibility entirely to specific phases, we advocate for a comprehensive approach that acknowledges the role of data collectors and curators, foundational model developers, API users or downstream developers focused on specific products, and the responsibility of users and AI system adopters themselves.

By embracing a "both, and" solution to accountability and prioritizing clarity of liability, we can create an environment where large tech firms are held accountable for their AI-driven

---

[20] John Villasenor, *Products liability law as a way to address AI harms* (Oct. 31, 2019), Brookings, https://www.brookings.edu/research/products-liability-law-as-a-way-to-address-ai-harms/; Alina Glaubitz & Nathaniel Raymond, How should liability be attributed for harms caused by biases in Artificial Intelligence? (Apr. 29, 2021) Yale Department of Political Science, available at https://politicalscience.yale.edu/sites/default/files/glaubitz_alina.pdf.

actions, while also preserving the essential elements of innovation, research, user autonomy, and the growth of startups in the technology sector.

### V.  GOVERNMENT SHOULD PROVIDE RESOURCES TO PROMOTE INNOVATION AND COMPETITION, INCLUDING THROUGH A PUBLIC OPTION FOR AI

Oversight and accountability must be coupled with policies and investments that will promote continued innovation, responsible research, open access, and vigorous competition. AI technologies have enormous potential, and the overall goal of any regulatory system should be realizing that potential, not overburdening its development or allowing its benefits to be inequitably captured. Policymakers should balance regulation with support and incentives for ethical AI development and deployment that serves public interest values. As discussed above with regard to an expert AI regulator, there is a false dichotomy established between regulation and innovation; expert oversight can, and often does, promote responsible development and preserve competition that drives innovation. Expert oversight which can adaptably choose to enforce requirements or exercise forbearance is essential in a rapidly developing field where the interest of early incumbents, new entrants, and other stakeholders need to be carefully balanced.

#### A.  A National AI Research Resource Could Advance Innovation, Competition, and Accountability.

A key mechanism for promoting innovation and competition is the government's ability to directly subsidize research. Questions 31 and 32 ask about government funding and incentives to promote AI accountability. Government funding and incentives for AI development should always center accountability and responsibility, with projects developed in line with public values and aimed towards the public's benefit.  Earlier this year, the National Artificial Intelligence Research Resource (NAIRR) Task Force published its report containing

recommendations for the establishment of a NAIRR: "a shared research infrastructure that would provide AI researchers and students with significantly expanded access to computational resources, high-quality data, educational tools, and user support"[21]

The report also concluded that a NAIRR "presents a unique and critical opportunity to 'design in' the standards for responsible AI research practices and governance processes that uphold our priority to develop and harness these groundbreaking technologies in a manner that reinforces our Nation's democratic values and Americans' personal freedoms."[22] The report concludes that NAIRR should be administratively located within a federal agency. The task force suggests the National Science Foundation (NSF) as a natural home, unsurprisingly given NSF's role in leading the task force and its longstanding research mission, but an expert AI regulator would make an even better choice to house NAIRR in order to more effectively integrate the government's accountability and public interest goals into its research infrastructure. The NAIRR could be a huge benefit to the development of safe, responsible, and publicly beneficial AI systems but the NAIRR needs more than the power of the purse backing it up in order to ensure that publicly-funded research and development remains publicly beneficial. Linking NAIRR resources with regulatory oversight would ensure enforcement of ethical and accountability standards and prevent public research resources from being unfairly captured for private benefit.

## B. Government Should Consider Developing a Public Option for AI.

Along these same lines, policymakers should consider that public computational resources, datasets, and expert oversight would enable not just public-private partnerships, but present the opportunity to develop publicly owned and operated AI systems. The idea of a

---

[21] *Strengthening and Democratizing the U.S. Artificial Intelligence Innovation Ecosystem: An Implementation Plan for a National Artificial Intelligence Research Resource* at ii (Jan. 2023), National Artificial Intelligence Research Resource Task Force, https://www.ai.gov/wp-content/uploads/2023/01/NAIRR-TF-Final-Report-2023.pdf.
[22] *Id*. at ii.

"public option" for AI has been promoted and discussed by various experts as an opportunity to put these powerful technologies squarely in the public sector, rather than rely on profit-driven private actors.[23] Rooted in the notion that the government could exercise stewardship over a shared data commons, or through its investment in publicly-funded computational resources,  a public option for AI would provide a competitive alternative to private models.

Public foundational models or AI systems could be leveraged, not just for research, but to ensure that the public has the benefit of access to potent AI technologies and that AI is built and deployed consistent with democratic values. For example, companies developing Large Language Models (LLMs) "make decisions with huge consequences for democracy, but little democratic oversight. We don't hear about political trade-offs they are making. Do LLM-powered chatbots and search engines favor some viewpoints over others? Do they skirt controversial topics completely? Currently, we have to trust companies to tell us the truth about the trade-offs they face. A public option LLM would provide a vital independent source of information and a testing ground for technological choices with big democratic consequences."[24]

## VI.    OTHER DIGITAL POLICY CHANGES THAT WILL ENHANCE AI ACCOUNTABILITY EFFORTS

While the development of AI presents some challenges that demand AI-specific responses, there are also policy changes that would indirectly enhance AI accountability efforts.

---

[23] Ben Gansky, Michael Martin and Ganesh Sitaraman, *Artificial Intelligence Is Too Important to Leave to Google and Facebook Alone* ( Nov. 10, 2023) The New York Times, https://www.nytimes.com/2019/11/10/opinion/artificial-intelligence-facebook-google.html; Bruce Schneier, Henry Darrell, and Nathan E. Sanders, *How Artificial Intelligence Can Aid Democracy* (Apr. 21, 2023), Future Tense, Slate, https://slate.com/technology/2023/04/ai-public-option.html; Ezra Klein & Alondra Nelson, *Transcript: Ezra Klein Interviews Alondra Nelson* (Apr. 11, 2023), The New York Times, https://www.nytimes.com/2023/04/11/podcasts/ezra-klein-podcast-transcript-alondra-nelson.html.
[24] Bruce Schneier, Henry Darrell, and Nathan E. Sanders, *How Artificial Intelligence Can Aid Democracy* (Apr. 21, 2023), Future Tense, Slate, https://slate.com/technology/2023/04/ai-public-option.html.

A sector specific digital regulator for online platforms and a comprehensive privacy law are long overdue steps that are urgently needed now, but will also leave us better prepared for the future.

### A. Creating An Expert Digital Platform Regulator.

By addressing the online digital platforms and tech giants that have driven the explosion of digital data and use of algorithmically mediated content we can establish a healthier environment for the progress of AI. Public Knowledge has long advocated for the creation of a sector specific regulator for online platforms.[25] This idea has been growing in popularity, and has resulted in proposed legislation in Congress.[26] A regulator that oversees digital platforms, with robust consumer protection, competition policy, and regulatory authority would indirectly benefit AI accountability efforts. Online platforms currently exercise tremendous gatekeeping power through the consolidation in search, social media, e-commerce, mobile app stores, and messaging. This power, combined with their cloud computing holdings and vast troves of consumer data, means the online platforms are poised to become powerful actors in the AI space. Addressing these non-AI specific problems in the digital platform sector will pave the way towards a more open and accountable AI ecosystem.

Such a regulator would serve as a sector specific expert for oversight of AI in the domain of online platforms like social media, internet search, and digital commerce. This is a distinct proposal from the notion of an expert AI authority, whose mission would extend beyond online platforms or digital services to encompass AI and machine learning more broadly, but it may make organizational or legislative sense to connect these concepts together. Especially given how

---

[25] Harold Feld, The Case for the Digital Platform Act: Market Structure and Regulation of Digital Platforms, May 2019, available at https://publicknowledge.org/policy/the-case-for-the-digital-platform-act/; Harold Feld, *Platform Regulation Part I: Why Platform Regulation is Both Necessary and Hard* (Jul. 17, 2018), Public Knowledge, https://publicknowledge.org/platform-regulation-part-i-why-platform-regulation-is-both-necessary-and-hard/.

[26] *Welch, Bennet Reintroduce Landmark Legislation to Establish Federal Commission to Oversee Digital Platforms* (May 18, 2023), United States Senate, https://www.welch.senate.gov/press-releases/welch-bennet-reintroduce-landmark-legislation-to-establish-federal-commission-to-oversee-digital-platforms/.

the data collection practices of online platforms and their reliance on algorithmic processes are intertwined with the AI ecosystem, there may be good reasons to spin up a single agency with a mission that encompasses both AI and digital platforms.

### B. Comprehensive Privacy Legislation.

The lack of a comprehensive federal privacy law is another barrier to effective AI accountability. We have already seen large language models leak personally identifiable information[27] and chat histories.[28] But those data breaches are not the only reason AI accountability must include strong privacy protections.[29]

The development and training of generative AI chatbots using large language models pose specific concerns regarding the incorporation of personally identifiable information (PII). These language models are often trained on a combination of datasets, including data scraped from the internet - which can contain PII. Currently, in the US, there are very few restrictions on the PII that can be used to train these large language models.

There are significant knock-on effects that result from the widespread inclusion of PII. First, and foremost, it would be impossible for people to know if their data made its way into an AI model. The method of creating large datasets through scraping the internet does not give any notice to individuals that the scraping has occurred. Combine that lack of transparency with AI models being a black box, no one could know for certain what data had been included in the model. And if that information was incorrect, there would be no way for the person to correct or delete the data without having to delete the model.[30]

---

[27] Jon Porter, *ChatGPT bug temporarily exposes AI chat histories to other users* (Mar. 21, 2023), The Verge, https://www.theverge.com/2023/3/21/23649806/chatgpt-chat-histories-bug-exposed-disabled-outage
[28] Andrew Tarantola, *OpenAI says a bug leaked sensitive ChatGPT user data* (Mar. 24, 2023), Engadget, https://www.engadget.com/openai-says-a-bug-leaked-sensitive-chatgpt-user-data-165439848.html.
[29] Einaras von Gravrock, *Why artificial intelligence design must prioritize data privacy* (Mar. 31, 2023), World Economic Forum, https://www.weforum.org/agenda/2022/03/designing-artificial-intelligence-for-privacy/.
[30] Avi Gesser, Paul D. Rubin, and Anna R. Gressel, *Model Destruction – The FTC's Powerful New AI and Privacy Enforcement Tool* (Mar. 30, 2022), Compliance & Enforcement Blog, New York University School of Law,

We have already seen privacy enforcement occur against AI companies in other jurisdictions.[31] The Italian Data Protection Authority required OpenAI to publish an information notice, implement an age gate, update its legal basis for processing, provide users a way to exercise their personal rights over their data (including its continued use in the model), and conduct an awareness campaign in Italy.[32] And Canadian authorities have launched a probe into OpenAI's privacy practices focusing on if OpenAI obtained consent for the data it collected, used, and disclosed.[33] While most privacy laws do not have particular requirements for AI, they are a useful tool to ensure the safety and accountability of AI systems.

## VII.  CONCLUSION

In conclusion, the field of AI is rapidly evolving and holds both promise and potential risks. The decisions we make now regarding AI accountability and regulation are crucial for shaping its future. We need durable and responsive approaches to AI policymaking, marked by adaptability and understanding of the technology. A hybrid approach involving sector-specific regulators and a centralized AI regulator is recommended to mitigate both immediate and anticipated harms, while also building up expertise to adapt to this evolving technology more comprehensively. In addition, policymakers must also lay the groundwork for a healthy AI ecosystem by breaking down barriers to accountability, promoting innovation and responsible research, and addressing regulatory shortcomings in our existing digital environment. Establishing a sector-specific digital regulator and comprehensive privacy law are necessary steps for a healthier AI environment and better preparedness for the future.

---

https://wp.nyu.edu/compliance_enforcement/2022/03/30/model-destruction-the-ftcs-powerful-new-ai-and-privacy-enforcement-tool/.

[31] Kelvin Chan, *OpenAI: ChatGPT back in Italy after meeting watchdog demands* (Apr. 28, 2023), AP News, https://apnews.com/article/chatgpt-openai-data-privacy-italy-b9ab3d12f2b2cfe493237fd2b9675e21.

[32] Natasha Lomas, *Italy gives OpenAI initial to-do list for lifting ChatGPT suspension order* (Apr. 12, 2023), TechCrunch, https://techcrunch.com/2023/04/12/chatgpt-italy-gdpr-order/.

[33] *Canada to launch probe into OpenAI over privacy concerns* (May 26, 2023), Reuters, https://www.reuters.com/technology/canada-launch-probe-into-openai-over-privacy-concerns-2023-05-25/.