Comments of the Software & Information Industry Association on the Request for Information to the Update of the National Artificial Intelligence Research and Development Strategic Plan

Submitted to the Office of Science and Technology Policy

March 4, 2022

On behalf of the Software & Information Industry Association (SIIA), we appreciate the opportunity to provide input on the Request for Information to the Update of the National Artificial Intelligence Research and Development Strategic Plan.

SIIA, a non-profit organization, is the principal trade association for the software and digital information industries worldwide. Our members include over 450 companies reflecting the diversity of the information landscape, from creation to dissemination to productive and responsible use. They include digital content providers and users in academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide, and companies specializing in data analytics and information services. Our members support policies that foster innovation and a healthy digital ecosystem, including consumer privacy protections, responsible and ethical AI, and DEI initiatives.

Input on Strategy 3: Understand and address the ethical, legal, and societal implications of AI; and Strategy 4: Ensure the safety and security of AI systems.

The OECD Principles on Artificial Intelligence were only a month old when the U.S. government issued the 2019 Strategic Plan. Since then, public and private research into ethical and responsible AI and methods to operationalize these objectives has grown exponentially. Governments around the world have launched councils to study ethical AI, international and multi-stakeholder efforts at the OECD and through GPAI have brought needed high-level engagement, and academic research centers have pioneered new ways to hone AI. This still-burgeoning field has led to numerous advances in the quality of AI datasets and algorithms that are more accurate, transparent, and fair. Moreover, private sector companies have taken steps to build and enhance internal governance frameworks to operationalize principles.

We support continued federal funding of AI research and development into the ethical, legal, and societal implications of AI along with initiatives to ensure the safety and security of AI systems. We support efforts by the National Science Foundation, the Department of Energy and other agencies, and the National Institute of Standards and Technology (NIST) to support work in this area. Likewise, we support the work of the Office of Science and Technology Policy (OSTP) to craft an "AI Bill of Rights" that would reflect principles for responsible and ethical development and use of AI that support diversity, equity, inclusion, accessibility, and fairness in how AI systems are applied.

Need for an AI Governance Framework

Despite these efforts, alongside world-leading innovation, research, and investment, the United States has fallen behind in formal AI governance. The European Union (EU) is advancing an AI Act that has many admirable qualities but will also impose significant costs on U.S. companies and barriers to innovation. These costs and barriers are likely to make it harder to maximize the benefits of AI while achieving appropriate protections individual rights, privacy, and security. Other jurisdictions around the world, such as the UK, Brazil, and Singapore, have made significant strides in formulating AI governance frameworks, and some, like China, have already implemented algorithm regulations. Municipalities in the United States are beginning to do the same.

Because these laws will have effects on U.S. companies and their innovation, we have concern that the United States is missing out on an opportunity to shape AI governance framework as has happened in the privacy context following implementation of the EU's General Data Protection Regulation.

We recommend that the Strategic Plan include as a strategic aim a dedicated effort to develop frameworks of rules and regulations to guide AI R&D and use by both the private and public sectors. To achieve this, we recommend that OSTP convene a council of legal, policy, and technical experts with a concrete timeline to generate specific proposals.

We have suggested elements and the structure of such a framework at the back of this submission. (See "*Annex – Advancing a Democratic Vision of Data Governance*".)

Input on Strategy 5: Develop shared public datasets and environments for AI training and testing.

The availability of robust, reliable, and trustworthy data sets is a key impediment to AI innovation. While data is an essential component of the AI stack, developing robust data sets that meet the standards for responsible AI and minimize privacy concerns is extremely costly for most companies and entrepreneurs. That cost both limits the potential of AI and allows AI tools to be built on unreliable, untrustworthy, or potentially biased information. Data sets that do not comport with standards of accuracy, reliability, trustworthiness, and bias present significant societal risk.[1]

Shared public datasets are critical to fostering new and better uses of AI technologies and ensuring that the data relied on by AI algorithms meets quality standards. We support continued work by the U.S. government in this space. Below we suggest specific additional measures that the U.S. government can undertake to create more robust shared datasets.

[1] Joshua New, AI Needs Better Data, Not Just More Data, Center for Data Innovation (Mar. 20 2019); Tasha Austin, et al., Trustworthy Open Data for Trustworthy AI, Deloitte Insights (Dec. 10, 2021).

Public-Private Dataset Initiatives

We recommend that the Strategic Plan advance efforts to build public-private partnerships to develop large, high-quality, and privacy-protective data sets that are accessible and usable by a wide range of actors would promote innovation and entrepreneurship while greatly reducing these risks. We offer two proposals for consideration.

First, we recommend a public-private effort to create **large synthetic data pools** that would be accessible by researchers, government, and across industry. Synthetic datasets can enable algorithms to run on data that reflect, rather than rely on, real-world data. This approach would allow for the creation of a robust data lake that can be vetted to ensure accuracy, reliability, fairness, and so on. Moreover, it would not present privacy and individual rights concerns that may arise from the collection, retention, sharing, and use of datasets that are built directly from personal information. We understand there is interest in the private sector to work with the government on this sort of initiative.

Second, we recommend a public-private effort to create **large open data sets** of personal information collected through enhanced notice and consent procedures. This could be modeled on the Casual Conversations dataset developed by Meta.[2] That dataset consists of over 45,000 videos of conversations with paid actors who consented to their information being used openly to help industry to test bias in AI systems.

Under either proposal, we would recommend that NIST lead the effort to ensure that the large data set is appropriately screened before it is put into wide use. The data pools should be subject to intensive test, evaluation, verification, and validation procedures in accordance with NIST standards and with the involvement of government and private sector experts.

Improving International Collaboration through Shared Datasets

We also encourage the Strategic Plan to advance recommendations for international, multilateral, and bilateral research efforts that can use shared datasets to support innovation. Two such models are as follows:

For example, an international or multilateral research effort built on shared datasets could be modeled on the Multilateral AI Research Institute (MAIRI), recommended by the National Security Commission on Artificial Intelligence.[3] As proposed, MAIRI would "facilitate joint efforts to develop technologies that advance responsible, human-centric, and privacy-preserving AI/ machine learning (ML) that better societies and allow allies to pool their talents and resources. It will provide a model for equitable, multilateral research, facilitate AI R&D that builds on like-minded countries' strengths, and foster a global AI workforce for the next generation." It would be a U.S.-led effort that would benefit from a federated network of global research institutes and leverage shared datasets to foster innovation in line with democratic technology values.

[2] Meta AI, Casual Conversations Dataset (April 2021).

[3] National Security Commission on Artificial Intelligence, Final Report (March 2021) at 192, 244, 249, 535-40.

Another approach would be to encourage more targeted, bilateral efforts, with much the same objectives as MAIRI.[4] A bill introduced in the current Congress would create a joint U.S.-Israel center "to leverage the experience, knowledge, and expertise of institutions of higher education and private sector entities in the United States and Israel to develop more robust research and development cooperation" in several critical AI areas.

Input on Strategy 8: Expand Public-Private Partnerships to accelerate advances in AI.

We encourage the Strategic Plan to call for further public-private efforts to advance AI, especially in areas of democratic affirming technology and technology that provides other important societal benefits.[5] Below, we highlight two areas where we believe government action can help to address societal challenges and foster greater innovation.

Promoting Privacy Enhancing Technologies (PETs)

Privacy enhancing technologies (PETs) refer to a group of technologies that protect the privacy and security of sensitive information. NIST, a long-time champion of PETs, will recognize that a host of what were once "emerging" PETs—such as homomorphic encryption, differential privacy, federated learning, and synthetic data—now have established uses in a wide range of contexts, including research, health care, financial crime detection, human trafficking mitigation, intelligence sharing, criminal justice, and more.[6]

PETs can be an essential part of a democratic model of emerging technology in practice, as a counter to a model that sacrifices privacy, trust, safety, and transparency.[7] PETs can enable the secure sharing of data between entities and across jurisdictional boundaries, expanding data access and utility and enabling organizations to reduce risk while making faster, better-informed decisions.[8] PETs are one way to solve (as a technical but not legal matter) privacy-based restrictions on EU-US data flows.[9]

---

[4] S.2120, The United States-Israel Artificial Intelligence Center Act (June 17, 2021).

[5] SIIA recently published a series of case studies highlighting uses of our members' technology to assist in a range of socially beneficial efforts, including tracking financial crime and human trafficking, finding missing children, supporting and advancing resources for the disabilities community, and more.

[6] The Center for Data Ethics and Innovation, PETs Adoption Guide, Repository of Use Cases. See also, e.g., Kaitlin Asrow and Spiro Samonos, Federal Reserve Bank of San Francisco, Privacy Enhancing Technologies: Categories, Use Cases, and Considerations (June 1, 2021); Luis T.A.N. Brandao and Rene Peralta, NIST Differential Privacy Blog Series, Privacy-Enhancing Cryptography to Complement Differential Privacy (Nov. 3, 2021).

[7] Andrew Imbrie, et al., Privacy Is Power: How Tech Policy Can Bolster Democracy, *Foreign Affairs* (Jan. 19, 2022).

[8] Two use cases involving SIIA members will help to illustrate this point. First is a partnership between Enveil (an SIIA member) and DeliverFund, the leading counter-human trafficking intelligence organization, which leveraged Enveil's PETs-powered solutions to accelerate reach and efficiency by allowing users to securely and privately screen existing assets at scale by cross-matching and searching across DeliverFund's extensive data. Second is Meta's use of secure multi-party computation, on-device learning, and differential privacy tools to minimize the amount of data collected in the advertising space while ensuring that personalized content reaches end users.

[9] See Asrow and Samonos, supra, at 4.

This is not just an industry view. As the White House stated in announcing the new US-UK challenge, PETs "present an important opportunity to harness the power of data in a manner that protects privacy and intellectual property, enabling cross-border and cross-sector collaboration to solve shared challenges."[10] In addition, the U.S. Census Bureau plans to launch a series of pilot projects to deploy PETs to "to build a platform that will enable secure multi-party computation, encryption technologies, and differential privacy to promote better data sharing both domestically and abroad."[11] This energy complements growing global interest. For example, the UK Information Commissioner's Office is exploring guidance on PETs and ways to incorporate PETs into data regulations. Recently, according to reports, the United Nations launched a "PETs Lab" to test PETs against data sets from the United States, the UK, Canada, Italy, and the Netherlands, and work with researchers and the private sector to develop use cases and create guidance.[12]

We therefore recommend that Congress and the executive branch **incentivize PET adoption by public and private entities**. The GDPR and other new privacy regimes have helped to foster increased attention in PET capabilities abroad. Official action by the U.S. government can have a similar effect and lead to the development and use of PETs designed to address critical needs around information privacy and security – enhancing innovation in the United States and helping to drive behavior globally. PETs can also help to drive up compliance with a range of laws and regulations in ways not possible when those laws and regulations were drafted.

We similarly encourage additional **public-private partnerships designed to establish use cases**. A bill under consideration in Congress, the Promoting Privacy Technologies Act (H.R. 847),[13] would promote fundamental research into PETs. The government has a critical role to play in fostering fundamental research – especially in areas, such as PETs, where robust markets have yet to develop. In addition to fundamental research, the government should look to establish partnerships focused on the application of already-mature PETs to new areas.

Promoting Content Provenance to Combat Disinformation

Maintaining a trustworthy digital ecosystem, one that addresses growing and malign influence efforts, is important for the health of the internet and entire digital ecosystem. Disinformation can erode social cohesion and human rights,[14] with a disproportionate effect on marginalized communities.[15] AI supercharges the ability of state and non-state actors to spread disinformation

[10] White House Office of Science and Technology Policy, US and UK to Partner on Prize Challenges to Advance Privacy-Enhancing Technologies (Dec. 2021); White House, Remarks of Jake Sullivan (July 13, 2021).
[11] White House, Fact Sheet: The Biden-Harris Administration is Taking Action to Restore and Strengthen American Democracy (Dec. 8, 2021).
[12] United Nations. Global Platform: Data for the World; The Economist, The UN is testing technology that processes data confidentially (Jan. 29, 2022).
[13] H.R.847 - 117th Congress (2021-2022): Promoting Digital Privacy Technologies Act (Jan. 19, 2022).
[14] Carme Colomina, et al., The impact of disinformation on democratic processes and human rights in the world, European Parliament (April 2021).
[15] Center for Democracy and Technology, Facts and their Discontents: A Research Agenda for Online Disinformation, Race, and Gender (2021).

creating a systemic risk for the entire information environment.[16] Synthetic media, including deepfakes, provide a special challenge because of how they deliberately distort existing images, video, and audio.[17]

We are encouraged by work underway around **content provenance and authenticity** as one way to combat the scourge of disinformation and deepfakes. The Content Authenticity Initiative[18] is a cross-industry coalition of content creators, technology companies, and others dedicated to using technology to fight the scourge of disinformation through content authenticity. A related project, the Coalition for Content Provenance and Authenticity[19] recently issued a series of technical specifications designed to certify the provenance of media content.[20] This builds on work of several private firms, including one of our member companies, Adobe.[21]

This is a core area where further efforts within the U.S. government and between the government and private firms would be extremely beneficial and we recommend including this as a strategic aim in the Strategic Plan. We support the Deepfake Task Force Act[22] as one important way to achieve this. That Act would create a task force within the Department of Homeland Security and coordinate efforts with the private sector to fight deepfakes.[23] This is exactly the sort of coordination that we believe is critical in addressing one of the most challenging digital threats facing society today.

* * *

Thank you for the opportunity to provide input on the Strategic Framework. We would be pleased to discuss any of these issues in further detail. Please direct any inquiries to **Paul Lekas, SIIA Senior Vice President for Global Public Policy** (plekas@siia.net).

---

[16] Katerina Sedova, et al., AI and the Future of Disinformation Campaigns, Georgetown Center for Security and Emerging Technology (Dec. 2021).

[17] Kartik Hosanagar, Deepfake Technology Is Now a Threat to Everyone. What Do We Do?, Wall Street Journal (Dec. 7, 2021); Tim Hwang, Deepfakes: A Grounded Threat Assessment, Georgetown Center for Security and Emerging Technology (July 2020).

[18] Content Authenticity Initiative, https://contentauthenticity.org/.

[19] Coalition for Content Provenance and Authenticity, https://c2pa.org/.

[20] Coalition for Content Provenance and Authenticity, C2PA Specifications.

[21] Eric Abent, Adobe Expands Content Authenticity Initiative Tools to Fight Misinformation, SlashGear.com (Oct. 26, 2021).

[22] Deepfakes Task Force Act, https://www.congress.gov/bill/117th-congress/senate-bill/2559/text.

[23] U.S. Senate Comm. on Homeland Security & Govt. Affairs, Tech Leaders Support Portman's Bipartisan Deepfake Task Force Act to Create Task Force at DHS to Combat Deepfakes (July 30, 2021).

Annex - Advancing a Democratic Vision of Data Governance

Advancing a model for the responsible development and use of emerging technologies is among the most important components of a U.S. approach to fostering economic and competitiveness. The global nature of data and information means that many U.S.-based companies and the strength of the U.S. innovation climate are directly affected by laws and regulations implemented in foreign jurisdictions. It also means that what the United States does in terms of establishing rules of the road can have a noticeable effect on how other nations develop their own technology policies.

While the U.S. government has made this a priority in its foreign policy,[24] the nation still lacks a fundamental data governance framework, with no general application privacy law and no clear vision for advancing a regulatory framework for AI. Other jurisdictions have stepped up to fill this gap. The European Union's (EU) GDPR has become the benchmark privacy framework for jurisdictions worldwide, and the EU is looking to do the same with AI. The United Kingdom (UK) is among many nations that have advanced a concrete vision of data governance. The UK Data Protection Act 2018 is now entering its fourth year and the UK Information Commissioner's Office is actively exploring measures to update the Act and provide guidance to the public and business around emerging technologies.[25] China, too, has passed a consumer data privacy law along with regulatory frameworks for AI.

As described below, we recommend that the Strategic Plan convey the importance of (1) passing a comprehensive federal privacy law and (2) developing a formal framework to guide AI development and use.

Federal Privacy Legislation as a Necessary First Step to Providing a Baseline for Emerging Tech

SIIA and its members have advocated strongly for federal privacy legislation for years and are active in engaging with members of Congress and administrations of both parties. A federal privacy bill is the number one solution to closing the gaps on the use of personal data and data-driven technologies and driving innovation in the U.S. economy. Currently, the patchwork of state laws across the nation create uncertainty for consumers and businesses, burden companies with duplicative compliance costs (estimated at $1 trillion over 10 years) and have a disproportionate impact on growth and innovation for

[24] As the White House states in its Indo-Pacific Strategy: "We will also work with partners to advance common approaches to critical and emerging technologies, the internet, and cyberspace. We will build support for an open, interoperable, reliable, and secure internet; coordinate with partners to maintain the integrity of international standard bodies and promote consensus based, values-aligned technology standards; facilitate the movement of researchers and open access to scientific data for cutting-edge collaboration; and work to implement the framework of responsible behavior in cyberspace and its associated norms." White House, Indo-Pacific Strategy of the United States (Feb. 2022).

[25] The U.K. government launched its AI strategy later in 2021 and is piloting an AI technical standards hub through the Alan Turing Institute. See, e.g., UK Office for Artificial Intelligence, Department for Digital, Culture, Media & Sport, and Department for Business, Energy & Industrial Strategy, UK National AI Strategy (September 2021).

small- and medium-sized businesses.[26] This will grow as additional states pass privacy legislation – unless Congress acts first.[27]

The benefits of a federal privacy law for fostering a stronger innovation climate for emerging technologies and U.S. competitiveness are many. Such a law should both protect consumers from harm caused by the unreasonable collection and misuse of their personal data and prevent and remedy data practices that stifle innovation and stagnate data flows and routine business processes. Enactment of that statute would create both international and domestic benefits.

A federal privacy law is essential to digital trade and transatlantic data flows. As you are no doubt aware, those flows are in a state of flux due to the EU's invalidation of the Privacy Shield, and recent developments have threatened the use of foundational technologies by multinational companies. The United States' failure to offer a competing vision of privacy has allowed the GDPR to become the dominant approach to regulating personal data in the world. As the EU acts to restrict the activities of U.S. firms, the United States will lose competitiveness in the production, sale and distribution of data-driven technologies and services. Maintaining U.S. competitiveness requires the development of a U.S.-based common set of definitions and policies that can help build alignment on data flows with the rest of the world.

Domestically, the benefits of a federal privacy regime include creating baseline harmonization of consumer and business expectations surrounding personal information; supporting and fueling further competitive innovation in emerging technologies; and more deeply embedding diversity, equity and inclusion into privacy, emerging tech, and AI policies and practices.

We therefore encourage the Strategic Plan to emphasize the need a comprehensive federal privacy law that will provide strong and meaningful consumer protections (such as individual rights to notice, access, control, correction, deletion, and portability), permit socially beneficial uses of consumer data - particularly publicly available information - and promote innovation and competition in the American economy.

Developing a U.S. Legal Framework for AI

The United States risks missing an opportunity to shape AI regulation in a manner that will promote U.S. innovation and reflect core U.S. values. The EU is open about its goal of establishing the ground rules and guardrails for AI as it has done with privacy. The EU is not alone; indeed, many nations as well as U.S. states and localities are exploring and enacting rules that will have a direct impact on U.S. companies and U.S. innovation.

We recommend that the U.S. government take a more proactive approach to building an AI governance framework to avoid a repeat of what happened with privacy. We offer a few overarching

[26] See Information Technology & Industry Foundation, The Looming Cost of a Patchwork of State Privacy Laws (Jan. 24, 2022).

[27] Three states have comprehensive privacy laws (California, Colorado, and Virginia), and dozens of bills have been introduced in most of the remaining states. See IAPP, State Privacy Legislation Tracker (Feb. 2022).

principles for building a regulatory (or legislative) framework that would advance responsible AI and fairness, promote U.S. innovation, and provide necessary guardrails around both public and private use.[28]

First, we encourage efforts currently underway in the U.S. government to develop **guidelines for responsible and ethical use** of AI technologies – which should include those technologies that collect and use data embedded in emerging technologies. NIST's work in developing a risk management framework and establishing guidelines to address algorithmic bias is especially encouraging.[29] Alignment of key stakeholders, including industry groups, government stakeholders, private companies, and consumer advocacy groups to existing principles and standards like those adopted by NIST will lead to further harmonization of policy and technical foundations for how information is collected and used.

We also recommend that the government endorse a **technology-neutral approach** to regulating AI. We believe the focus should be on the type of data being collected, building transparency around notice and consent of data collection, and clear basis for the use and processing of information, rather than the technological tools— and the underlying algorithms—that facilitate that collection and use. The distinction may be subtle, but it is an important one. As noted, there are a wide variety of emerging technologies (and nuances within each); overarching rules must be sufficiently flexible to provide a groundwork as advances occur, with detail to be worked out through standards and regulations.

This approach also recognizes that technologies are tools that in most cases are not inherently good or bad. Because of this, we recommend that the focus be on how the models are used in practice. We believe the **risk-based approach**, now widely endorsed, provides the right lens. With respect to emerging technologies, there is a range of risks associated with the type of information collected, how that information is stored and used, and what consumers' expectations are. Responsibility, security, and accountability for data-driven technologies should be commensurate with risk.

One way to think about how to build out a risk-based approach is to **identify the potential harms**—such as discrimination and privacy violations—that could arise out of use, misuse, or abuse of the data-driven technologies.[30] This should be done through a sector-by-sector assessment and ead to **targeted, contextual restrictions on collection, storage, and use** to prevent those harms. We believe such restrictions or guardrails are critical, but they should be as narrowly tailored as possible to support innovation and positive use cases that benefit society.

In addition, we recommend that there be **no broad copyright exception** for the use of data in artificial intelligence. Facts, of course, are free for the taking.[31] And fair use permits the analysis of a copying and analysis of protected works for purposes that do not displace the markets for the original,

---

[28] Among the many existing frameworks, we commend those published by Google and, in January 2022, by the Business Roundtable as especially worthy of attention.

[29] See NIST, AI Risk Management Framework Concept Paper (Dec. 13, 2021); NIST, A Proposal for Managing and Identifying Bias in Artificial Intelligence (June 2021).

[30] See, e.g., FTC Staff, Comment to NTIA (Nov. 8, 2018) (identifying four categories of informational injuries: financial, physical, reputational, and unwanted intrusion).

[31] *Feist Pubs. v. Rural Telephone, Inc.*, 499 U.S. 341 (1990).

for example by creating an electronic card catalog that allows the user to search both the title and text of particular works.[32] Fair use and other doctrines (absent from the laws of different countries) similarly permit ordinary internet-based activities.[33] At the same time, however, the fact-based nature of fair use inquiry allows courts to examine and proscribe uses that would result in substitutes for the author's original creation. There is nothing about artificial intelligence that requires recalibration of the copyright law's current balance.

Lastly, we recommend separate frameworks that **distinguish between public and private** collection, storage, and use of information. In the private context, we note that many companies have built robust frameworks for assessing how they collect and use personal data. Many already adhere to industry standards and have established self-regulatory frameworks and principles[34] and conduct pre- and post- deployment impact assessments when collecting and using personal information. .

The public sector or government experience in collecting and using personal information for AI models presents a different situation. Governments can and do make use of personal information to verify access to benefits, for national security, public safety, and law enforcement purposes, to counter fraud, to assist in providing public health services, and so on. Beyond the restrictions of the Privacy Act of 1974, questions abound about what information the government may appropriately collect, how that information is obtained, and how the information is used consistent with the rights guaranteed by the Constitution.[35] Concerns have been raised about whether the Fourth Amendment provides sufficient protection to individuals—and clarity to government actors—about what information may be collected and how it can be used.[36] Congress has introduced several bills that would direct the U.S. government on use (or non-use) of facial recognition technologies, for example,[37] yet much can be accomplished through Executive Branch action alone. Many states and local governments are grappling with this issue. It is important that the federal government confront these issues and provide a model for the nation.

---

[32] *Authors Guild v. HathiTrust*, 755 F.3d 87 (2d Cir. 2014).

[33] E.g., *Field v. Google*, 412 F.Supp.2d 1106 (D. Nev. 2006) (copying of copyright-protected work allowed via implied license and other doctrines).

[34] See, e.g., Adobe, Ethical Approach to AI; Google, AI Principles.

[35] See, e.g., Matthew Doktor, Facial Recognition and the Fourth Amendment in the Wake of *Carpenter v. United States*, *Univ. of Cincinnati L. Rev.*, v.89, issue 2, at 552-74 (2021); Glenn Gerstell, "Failing to Keep Pace: The Cyber Threat and Its Implications for Our Privacy Laws," remarks to Georgetown Cybersecurity Law Institute (May 23, 2018) (reprinted at *Lawfare*).

[36] Ibid.

[37] See, e.g., H.R.3907 (117th Cong.), Facial Recognition and Biometric Technology Moratorium Act of 2021 (June 2021) (proposing to "prohibit federal government use of facial recognition technologies, provide a private right of action, and remove federal aid from agencies using the technology"); S.1265 (117th Cong.), The Fourth Amendment Is Not For Sale Act (Apr. 2021) (proposing to "prohibit law enforcement from purchasing personal data without a warrant and prevent law enforcement and intelligence agencies from buying illegitimately obtained data"); see also S.3035 (117th Cong.), Government Ownership and Oversight of Data in Artificial Intelligence Act of 2021 (Nov. 2021) (proposing interagency working group to develop guidance for the federal government and contractors around the development and use of AI).