Comments of the Software & Information Industry Association
RFI on Privacy, Equity, and Civil Rights
Department of Commerce, NTIA

March 6, 2023

Introduction

The Software & Information Industry Association (SIIA) thanks the National Telecommunications and Information Administration (NTIA) for the opportunity to provide this written comment in response to the NTIA's request for information (RFI) on privacy, equity, and civil rights.[1] SIIA is the principal trade association for those in the business of information, representing over 450 companies involved 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. SIIA's mission is to protect the three stages of the information lifecycle: creation, dissemination, and productive use.

Executive Summary

The relationship among privacy, equity, and civil rights is critical to the digital landscape and an area of focus for SIIA's work in privacy and data protection. SIIA supports privacy as a fundamental value, one essential to individual autonomy and a functioning democracy. Data privacy standards that harmonize meaningful consumer safeguards with appropriate business compliance will not only ensure smooth implementation of uniform privacy practices, but provide a stable and robust environment for the information industry to flourish.

We welcome NTIA's continued attention to this topic. The Biden administration has made the topic a core focus as it examines and assesses the existing "discriminatory disparities" in the digital economy, particularly with regard to the risk that data collection could have on marginalized communities. We commend the NTIA on its efforts to organize listening sessions last year, which heightened the call for additional consideration on the topic, as well as NTIA's exemplary past efforts to shape the intersection of these topics, including the 2018 call for comments on developing the administration's approach to consumer privacy; a 2014 report to the White House and its 2012 bill of rights[2]. We also agree with the notion that the United States needs a federal privacy law, and that industry requires uniform rules of the road that will benefit both businesses and consumers, as discussed in the NTIA's comments responding to the Federal Trade Commission (FTC) ANPR on commercial surveillance and data security. It is also valuable to recognize existing guardrails for the industry, with regard to sector-specific data. In addition to the laws with which industry already complies, many companies are playing

[1] NTIA, Privacy, Equity, and Civil Rights,88 FR 3714. (Jan 20, 2022) [hereinafter "RFI"].

[2] White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Economy, (Feb. 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.
White House, Big Data: Seizing Opportunities, Preserving Values, (May 2014), National Telecommunications & Information Administration, Request for Comments on Developing the Administration's Approach to Consumer Privacy, (Sept. 25, 2018).

a role in minimizing harms and supporting the user experience by strengthening the individual data rights of the consumer, which is particularly beneficial for marginalized communities.

As NTIA develops its report on privacy, equity, and civil rights, we urge NTIA to take consideration of rights guaranteed by the U.S. Constitution, how existing laws and industry standards for privacy and data security interact with equity and civil rights concerns, nuances across industries and data processing entities, and current as well as anticipated benefits of the technology and underlying data.

Our responses to specific RFI questions highlight the following core themes:

1. **The United States needs a comprehensive federal privacy law**.

SIIA believes that passing a comprehensive federal privacy law will go a long way towards addressing the privacy concerns suggested by the RFI at both the individual and collective levels. We would note that NTIA appears to share this view, as indicated in public remarks made by NTIA Director Alan Davidson.[3] This is also reflected in NTIA's comments submitted to the FTC earlier this year.[4]

The United States should ensure that a federal privacy law incorporates critical protections for special populations and ensures appropriate First Amendment protections. A federal privacy law can help build a uniform baseline and close gaps that may exist outside of the sectoral approach while encouraging future benefits of the technology. This is particularly true as we consider special populations and marginalized communities. For example, existing sectoral laws such as Family Educational Rights and Privacy Act (FERPA) and Children's Online Privacy Protection Rule (COPPA) provide enhanced privacy protections for students and children.[5] As the United States works toward a federal privacy law, these sectoral laws should remain intact, as they are critical components of schools receiving federal and state funding, support state benchmark exams, and provide a profile of overall achievement.

In lieu of action by Congress, states have been active in passing unique consumer privacy laws that include different rules and requirements. The patchwork of state laws across the nation creates uncertainty for consumers and businesses. In our submission, we share more about Virginia's consumer data privacy law as the "gold standard" for harmonizing business compliance with meaningful consumer protections.

2. **Privacy legislation must protect the use of publicly available information (PAI).**

In the United States, publicly available information (PAI) is protected by the First Amendment. While certain federal bills have proposed to place limits on the collection and use

[3] Georgetown Law Institution for Technology and Policy. Building on the Dream: Privacy, Equity and Civil Rights. January 18, 2023.

[4] FTC. Comments of the NTIA to the FTC. Commercial Surveillance ANPR. FTC-2022-0053.

[5] Family Educational Rights and Privacy Act (FERPA): (20 U.S.C. § 1232g; 34 CFR Part 99); Children's Online Privacy Protection Rule (COPPA): (16 CFR Part 312)

of PAI, these provisions, if enacted, would not comport with the First Amendment. To date, states have had to revise their approach to PAI and ensure the necessary protections for all forms of PAI. In essence, PAI remains PAI regardless of how it is processed and whether it is combined, derived, or otherwise changed from its original form. There are a few important aspects of this, which we share in greater detail.

3. **Privacy policy should balance data minimization with socially-beneficial data uses.**

General purpose data use, in and of itself, has a number of socially beneficial uses including market research, product development, financial analysis, support for national security and law enforcement, protecting against discrimination, and more. Presuming harm in all data practices fails to distinguish between positive and unfair and deceptive data uses. Efforts to enhance data minimization should distinguish between controller and processor obligations toward the data and how data will be used. Further, we recommend any approach toward data minimization is measured, to prevent a chilling effect on the information economy, innovation, and efforts underway to improve data fairness and equity and data-driven solutions to social needs and societal challenges.

4. **Privacy policy should advance "privacy by design" and incentivize use of privacy enhancing technologies.**

One of the most important approaches to advancing privacy is "privacy by design," which now overlaps with the requirements in state consumer laws and has been acknowledged in the GDPR.[6]

Technologists can and should incorporate "privacy by design" into their product roadmaps, with an eye to how product design features, including personal information and related data privacy elements, impact marginalized communities. Companies are often leveraging the principles in GDPR's Privacy by Design framework and then tailoring these concepts to their own product design and deployment process. ISO 31700 is the privacy by design standard adopted by the International Organization for Standardization this year, which complements the work industry is already doing.[7] It features 30 requirements and guidance on privacy-by-design principles for effectuating consumer rights, relevant roles and authorities, privacy control designs and more.

To date, industry has made tremendous strides in shaping best practices and supporting data privacy by design. Examples of these solutions include the development of privacy by design programs, the global privacy control, and recent opportunities for privacy-enhancing technologies, a range of policy solutions that embed data minimization into their approach.

---

[6] Article 25, Data Protection by Design and Default, EU General Data Protection Regulation (GDPR), Regulation (EU), 2016/679 O.J. 2016 L 119/1 (hereinafter "GDPR").

[7] "International Association of Privacy Professionals, ISO Set to Adopt Privacy-by-Design Standard," ISO set to adopt privacy-by-design standard, (January 13, 2023)

Privacy engineering programs are growing and many companies - from the largest household platforms to the newest startups - are using privacy preserving technologies to streamline the responsible sharing of personal information to unlock analytics that require strong privacy protective practices.

NTIA should consider the research and potential of these technologies in limiting data privacy risks and harms to consumers, as current guidelines and research is being shaped by the National Institute of Standards and Technology (NIST) and the Office of Science and Technology Policy (OSTP). NTIA should review to ensure that any approach to data minimization does not handcuff the testbed for these types of privacy protective solutions.[8]

5. Policy on AI and automated decision-making raises equities beyond privacy and should be coordinated across the government.

We recommend that the U.S. government take a more proactive approach to building an AI governance framework to ensure it keeps its global competitiveness and continues to foster a pro-democratic and pro-innovation climate.[9] 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.[10]

It is critical that further guidance and actions by the Executive Branch build on the substantial records developed in the past few years. These include records reflecting public input by NIST,[11] in connection with the AI risk-management framework, and OSTP, in connection with a recent RFI on biometrics and input provided on the AI bill of rights.[12] Ensuring cross-government interoperability will mitigate the unintended consequences of overregulating the digital market economy.

---

[8] *See generally* Comments of the Software & Information Industry Association (SIIA) on the Request for Information: Study to Advance a More Productive Tech Economy, Submitted to the National Institute of Standards and Technology (NIST), (Feb. 14, 2022) (setting forth these principles in more detail); Comments of the Software & Information Industry Association (SIIA) to the California Privacy Protection Agency (Nov. 8, 2021) (same); Comments of the Software & Information Industry Association (SIIA) on the Request for Information on Advancing Privacy - Enhancing Technologies, Submitted to the Office of Science and Technology Policy and the Fast Track Action Committee on Advancing Privacy-Preserving Data Sharing and Analytics of the Subcommittee on Networking and Information Technology Research and Development, SIIA.net (Aug. 2022); Comments of the Software & Information Industry Association (SIIA) on the Request for Information: Study to Advance a More Productive Tech Economy, Submitted to the National Institute of Standards and Technology (NIST), SIIA.net (Feb. 14 2022).

[9] *See generally* Comments of the Software & Information Industry Association (SIIA) on the Request for Information: Study to Advance a More Productive Tech Economy, Submitted to the National Institute of Standards and Technology (NIST), (Feb. 14, 2022) (setting forth these principles in more detail); Comments of the Software & Information Industry Association (SIIA) to the California Privacy Protection Agency (Nov. 8, 2021) (same).

[10] National Institute of Standards and Technology (NIST). AI Risk Management Framework. January 2023.

[11] Id.

[12] See OSTP, Notice of Request for Information (RFI) on Public and Private Uses of Biometric Technologies, 86 FR 56,300 et seq. (Oct. 08, 2021); OSTP Blueprint for an AI Bill of Rights (Oct. 2022).

Responses to Specific Questions

1. How should regulators, legislators, and other stakeholders approach the civil rights and equity implications of commercial data collection and processing?

a. Is "privacy" the right term for discussing these issues? Is it under-inclusive? Are there more comprehensive terms or conceptual frameworks to consider?

Examining the full set of the issues covered in the RFI solely through the lens of "privacy" can be over-inclusive in addressing the potential questions that may warrant attention by policymakers. Generalizing "privacy" as a catch-all for matters that do not have a direct privacy interest may divert attention from more pressing and impactful actions on privacy - leading to unintentional duplication in the regulation of existing laws. This is raised in a recent paper by privacy scholar Woodrow Hartzog. In "*What is Privacy? That's the Wrong Question"*, Hartzog warns that a broad and singular conceptualization of privacy is not beneficial as it guides lawmakers towards vague, overinclusive, and potentially underinclusive rules that often disproportionately harm marginalized groups.[13]

We agree. There is a difference between the informational injury caused by the mere publication of information (such as a defamatory statement about a private person, or the contents of a visit to a consumer's doctor) versus those injuries in which biased information can taint an otherwise lawful and appropriate decision. Although we recommend that NTIA ensure that its assessment focuses on core privacy and security practices that lead to harm or injury related to civil rights and equity, we believe that it is important to keep these two categories of injury distinct. Otherwise privacy means everything, and nothing. By focusing on privacy and outcomes – will help lead to a report and recommendations with a direct relationship to the development of privacy policies that address NTIA's concerns.

b. To what degree are individuals sufficiently capable of assessing and mitigating the potential harms that can arise from commercial data practices, given current information and privacy tools? What value could additional transparency requirements or additional privacy controls provide; what are examples of such requirements or controls; and what are some examples of their limitations?

As NTIA is aware, the United States currently has no comprehensive federal privacy law[14] although several states – at the date of writing, those include California, Colorado, Connecticut, Virginia, and Utah – have enacted comprehensive privacy laws. While the state laws differ, they align in offering individual consumers the rights to access, correct, delete, and limit the use of their personal information. These additional consumer rights are one aspect of consumer privacy law that provide additional transparency and accountability for consumers in

[13] Hartzog, Woodrow, What is Privacy? That's the Wrong Question (November 24, 2021). 88 The University of Chicago Law Review 1677 (2021), Available at SSRN: https://ssrn.com/abstract=3970890

[14] For example, sectoral laws such as: Health Insurance Portability and Accountability Act, Pub. L. 104–191; Gramm-Leach-Bliley Act, L. No. 114–94, 129 Stat. 1787, codified at 15 U.S.C. 6803(f)).

ensuring they are able to assess and mitigate harms arising from the use of their personal information.

The vast majority of the state consumer privacy laws also require 1) an opt-out preference signal and mechanism for consumers to be able to opt-out of processing their personal data;[15] and 2) a data protection impact assessment that data controllers and other entities must complete to assess their processing activities and mitigate risks that could arise. Enforcement action is currently handled by the Attorney General's office in each state based on a criteria and an enforcement fine that varies by state. For instance, this year, California's Attorney General has indicated that the state plans to crack down on businesses not complying with its data privacy practices.[16]

If a federal privacy law were to pass, it should incorporate a combination of these individual consumer rights, coupled with the requirement for controllers processing data that has a legal or similarly significant effect[17] to conduct data protection impact assessments. These guardrails will ensure accountability and transparency for consumers.

Because these types of requirements are gaining traction at the state level, many actors within the private sector have incorporated guardrails to curb potential harms of commercial data practices throughout the privacy by design process. As such, companies are currently able to support positive privacy "hygiene" and sufficiently assess and mitigate the potential harms of commercial data practices.

Federal comprehensive consumer privacy law remains the number one policy action that can provide guardrails and safeguards for consumers and will be meaningful for consumers in minimizing harm.

c. How should discussions of privacy and fairness in automated decision-making approach the concepts of "sensitive" information and "non-sensitive" information, and the different kinds of privacy harms made possible by each?

Academics have done important research on sensitive data. In a recent article titled *"Data is What Data Does: Regulating Use, Harm and Risk, Instead of Sensitive Data*[18]," renowned legal scholar and professor Daniel Solove addresses the impact of regulating sensitive data as well as proxy data and algorithms supporting automated decision-making. He notes the clear limitations with trying to regulate the space and that such an approach will result in severe overbreadth. Additional regulations will only create an unenforceable standard where

---

[15] Wheeler et al., "State Level Comparison Charts of Data Privacy Laws in the U.S" Bloomberg Law, (February 2, 2022)

[16] Attorney General Rob Bonta, State of California Department of Justice.. Ahead of Data Privacy Day, Attorney General Bonta Focuses on Mobile Applications' Compliance with the California Consumer Privacy Act,(January 27, 2023)

[17] Article 22, Automated Individual Decision-Making, Including Profiling, EU General Data Protection Regulation (GDPR), Regulation (EU), 2016/679 O.J. 2016 L 119/1 (hereinafter "GDPR").

[18] Solove, Daniel J., Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data (January 11, 2023). 118 Northwestern University Law Review (Forthcoming), Available at SSRN: https://ssrn.com/abstract=4322198 or http://dx.doi.org/10.2139/ssrn.4322198

all data is viewed as harmful, and such an approach will be met with First Amendment challenges. He writes: “The particular type of personal data does not indicate anything important when it comes to determining how to protect it. What matters is use.” We agree with this approach.

What we can expect is timely action through a federal privacy law that sets out the basic parameters on how privacy and data cannot be used or processed to unlawfully discriminate or segregate, as noted in the first point. Such a policy will keep pace with technology and leaves room for AI policy to develop with more robust parameters on bias and risk mitigation, particularly as it relates to technological harms that disproportionately impact marginalized communities.

We recommend that any regulation of automated systems should be both risk-based and technology-neutral.[19] Guiding principles for this approach include distinguishing between automated systems and automated decision-making technology for future regulation, evaluating decisions based on their impact on a natural person’s rights, balancing the context-specific risks of harm to the consumer as a result of an automated decision against the benefits to the public of permitting that use, and preserving the intellectual property and innovation landscapes.

Furthermore, any risk-based framework should avoid treating all automated systems the same. Article 22 of the GDPR takes a beneficial approach by requiring only impact assessments of high-risk systems that have a legal or similarly significant impact.[20] Specifically, data controllers must implement suitable measures to safeguard data subjects’ rights, freedoms, and legitimate interests. Implementing a similar process in the United States would allow interoperability between U.S. privacy regimes and other countries without stifling innovation or R&D. Consent fatigue notwithstanding, policymakers should incorporate the GDPR’s risk-based focus into its regulatory scheme for specific harms from automated systems. New policy should focus on identifying the reasonable and unreasonable sources of impacts from high-risk AI systems and clarify what empirical evidence is required and by whom to make or defend against allegations of discrimination, data misuse, and other harms.

In sum, automated decision-making, automated systems, and AI should not be seen as inherently harmful; these are tools, and we recommend policymakers focus on the harms caused by these tools and focus regulation on those harms rather than wholesale on the tools themselves. AI can produce robust societal benefits: whether it is by helping consumers find helpful or personalized products and services to improve their quality of life, detecting and preventing financial crimes, or equipping our schools with the best tools to teach students. Creating a risk-based framework to AI regulation is key to ensuring that the appropriate guardrails can exist while still reaping the technology’s expansive benefits.

---

[19] See generally Comments of the Software & Information Industry Association (SIIA) on the Request for Information: Study to Advance a More Productive Tech Economy, Submitted to the National Institute of Standards and Technology (NIST), (Feb. 14, 2022) (setting forth these principles in more detail); Comments of the Software & Information Industry Association (SIIA) to the California Privacy Protection Agency (Nov. 8, 2021) (same).

[20] Article 22, Automated Individual Decision-Making, Including Profiling, EU General Data Protection Regulation (GDPR), Regulation (EU), 2016/679 O.J. 2016 L 119/1 (hereinafter “GDPR”).

d. Some privacy experts have argued that the collective implications of privacy protections and invasions are under-appreciated. Strong privacy protections for individuals benefit communities by enabling a creative and innovative democratic society, and privacy invasions can damage communities as well as individuals. What's more, many categories of extractive and profitable processing rely on inferences about populations and demographic groups, making a collective understanding of privacy highly relevant. How should the individual and collective natures of privacy be understood, both in terms of the value of privacy protections; the harms of privacy invasions; and the implications of those values and harms for underserved or marginalized communities?

Laws in the United States are silent on the treatment of inferential and proxy data. The inclusion would likely be subject to First Amendment concerns. A significant portion of the discussions at Congressional hearings have centered around the negative use of algorithms with proxy data in decision-making and their potential harms to marginalized communities[21]. While the use of algorithms and proxy data (both alone and when embedded in algorithms) can have negative unintended consequences, they may also have positive impacts: from early health prevention and detection services for life threatening conditions like cancer, to personalized advertising, to the development of helpful products, services, and educational resources that have a particularly beneficial impact on marginalized communities. A balanced, risk-based approach to data use, which is technology neutral and takes into account the socially beneficial use cases and general benefits of data processing practices is essential, or else we risk creating an overly restrictive regime that will limit future innovation.

e. How should proposals designed to improve privacy protections and mitigate the disproportionate harms of privacy invasions on marginalized communities address the privacy implications of publicly accessible information?

In the United States, publicly available information (PAI) is protected by the First Amendment. While certain federal bills have proposed to place limits on the collection and use of PAI, these provisions, if enacted, would not comport with the First Amendment. To date, states have had to revise their approach to PAI and ensure the necessary protections for all forms of PAI. In essence, PAI remains PAI regardless of how it is processed and whether it is combined, derived, or otherwise changed from its original form. There are a few important aspects of this.

First, the transfer and use of PAI in the public domain - even when combined with personal data or when the data is used to derive other information or analytics - remains PAI and should remain protected speech. Sweeping inferences and combined data into the scope of a data privacy law could empower bad actors (e.g., criminals) to delete data – when granted with the individual rights to the data – and thus further diminish the quality of the data being processed and the inferences or analytics generated. This could hamper the positive impacts

[21] Algorithmic Accountability Act of 2022. https://www.congress.gov/bill/117th-congress/senate-bill/3572

felt by a broad swath of industries using mathematical data processing approaches, such as statistical analyses and inferences. Examples include finance, healthcare, retail, and other spaces with real-time markets where businesses and end users depend on predictive and inferential statistics.

Second, entities supporting government agencies and law enforcement should receive exemptions to process the data similar to the government personnel, to ensure that they can carry out a range of activities - from anti-money laundering to stopping human trafficking and more.

In this regard, the United States has the opportunity to learn from the GDPR's shortcomings. Research suggests that the GDPR's blanket opt-in consent regime has led to consumer consent fatigue, shrinking markets, and negative repercussions on product development and innovation.[22] When addressing data minimization and purpose limitations, NTIA should ensure that they are consistent with First Amendment guarantees and do not restrict the socially beneficial use cases that are in the public interest. For example, many of our members rely on publicly available information to generate productive and socially beneficial products and services (e.g. finding missing children, performing corporate due diligence, preventing money laundering and fraud, and more). The policy benefits that result from a robust public domain are guaranteed by the First Amendment of the U.S. Constitution. We would recommend that any guidance the NTIA may issue excludes publicly available information from its scope and correctly define that term to encompass information lawfully acquired from the government or contained in widely distributed media.

4. How do existing laws and regulations address the privacy harms experienced by underserved or marginalized groups? How should such laws and regulations address these harms?

a. Legislators around the country and across the globe have enacted or amended a number of laws intended to deter, prevent, and remedy privacy harms. Which, if any, of these laws might serve as useful models, either in whole or in part? Are there approaches to be avoided? How, if at all, do these laws address the privacy needs and vulnerabilities of underserved or marginalized communities?

b. Are there any privacy or civil rights laws, regulations, or guidance documents that demonstrate an exemplary approach to preventing or remedying privacy harms, particularly the harms that disproportionately impact marginalized or underserved communities? What are those laws, regulations, or guidance documents, and how might their approach be emulated more broadly?

[22] Rebecca Jansen et al., GDPR and the Lost Generation of Innovative Apps, National Bureau of Economic Research (May 2022).

Passing a comprehensive, preemptive federal privacy law is the number one solution to addressing actual or perceived harms with regard to privacy generally and to the impact of data practices on underserved or marginalized groups. By leveling the playing field, it ensures that companies appropriately shape their privacy practices. A federal law of this nature will emphasize the importance of streamlined beneficial data practices to mitigate harmful, unjust, inequitable, and discriminatory practices.

Furthermore, a federal privacy law should complement existing efforts and requirements in the Title VI of the Civil Rights Act[23] and various sectoral laws impacting data privacy. Title VI "prohibits discrimination on the basis of race, color, or national origin in any program or activity that receives Federal funds or other Federal financial assistance." SIIA member companies are already subject to the various sectoral data privacy laws (e.g., HIPAA, GLBA, FERPA) and potential enforcement by the FTC with regard to Section 5 of the Unfair and Deceptive Practices Act. SIIA member companies are in support of the passage of a comprehensive privacy law that works in conjunction with existing federal laws to strengthen consumer protections. A federal privacy law should build a uniform baseline for anti-discrimination in consumer data and continue to utilize sectoral laws that cover sector-specific data.

As we consider our most vulnerable populations, such as children and teenagers, we support efforts at the state, federal, and international level to balance safeguards for these populations while preserving the right for minors to be online, access information, communicate, and freely express themselves.

At the state level, Virginia has demonstrated leadership by serving as an example of what a meaningful consumer privacy law looks like, balancing consumer protections and reasonable business compliance. The Virginia Consumer Data Protection Act (VCDPA) establishes necessary guardrails and offers considerable protections to consumers through requiring businesses to provide disclosures, respond to consumer data subject requests, and comply with certain data processing obligations. Simultaneously, it carries a chiseled definition of "personal data," defining it as any information that is linked or reasonably linkable to an identified or identifiable natural person. 'Personal data' does not include de-identified data or publicly available information."[24] The VCDPA also provides protections against discrimination if or when consumers elect to exercise their rights and gives consumers the ability to opt-out of the sale of their personal data, targeted advertising, and certain profiling.[25]

Furthermore, privacy enhancing technologies (PETs) can play an important role in responsible data sharing, which can benefit marginalized communities. PETs is a catch-all term that refers to a group of technologies that use advanced statistical techniques to protect the privacy and security of shared data, between and across platforms, companies, and data sharing entities. NIST, a long-time champion of PETs, recognizes a host of what were once

---

[23] Office for Civil Rights (OCR), "Civil Rights Requirements Title VI of the Civil Rights Act," HHS.gov, (August 2021)

[24] Title 59.1, Chapter 53, Section 59.1-575 of the Virginia Code. https://law.lis.virginia.gov/vacode/title59.1/chapter53/section59.1-575/

[25] Microsoft Learn: "VCPDA FAQ"

"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.[26] 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. [27] 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.[28] PETs can reduce challenges with anonymizing data and increase the safeguards present.

We therefore recommend that Congress, the executive branch, and states take steps to incentivize PET adoption by public and private entities. The GDPR and other new privacy regimes, including the UK Information Commissioner's Office, have helped to foster increased attention in PET capabilities abroad[29]. Official action by the U.S. government (as well as activity at the state level) 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.

5. What are the principles that should guide the Administration in addressing disproportionate harms experienced by underserved or marginalized groups due to commercial data collection, processing, and sharing?

a. Are these principles reflected in any legislative proposals? If so, what are those proposals, and how might they be improved?

As mentioned above, passing a federal privacy law is key. Last year, the House Energy & Commerce Committee passed the American Data Privacy and Protection Act (ADPPA) – but fell short of bringing the bill to the House floor for a vote. The ADPPA provides one framework for a federal privacy law although aspects of the ADPPA we believe would not advance the interests of underserved or marginalized groups. For example, we believe the ADPPA's treatment of PAI and related exemptions would hinder data practices in a way that limits certain socially beneficial uses of data and would make it more challenging to ensure that practices

---

[26] Luis T.A.N. Brandao and Rene Peralta, 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); NIST Differential Privacy Blog Series, Privacy-Enhancing Cryptography to Complement Differential Privacy (Nov. 3, 2021).

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

[28] Our resource detailing positive use cases of PETs can be found here. Additionally, 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.

[29] UK ICO, Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance. Information Commissioner's Office. October 2021.

around housing, employment, financial services, and other key areas are not having a disproportionate effect on those communities. We also believe that revisions to the ADPPA are needed around protections for children's data as well as provisions around preemption and the private right of action that will likely lead to increased costs and a decrease in services to the general public, including marginalized communities. With additional improvements and support, we believe that a stronger draft of federal privacy legislation is attainable.

b. What kinds of protections might be appropriate to protect children and teens from data abuses? How might such protections appropriately address the differing developmental and informational needs of younger and older children? Are there any existing proposals that merit particular attention?

Existing policies created through Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy Protection Rule (COPPA), and various state-specific regulations currently offer protection to children and teens against data abuses. Federal policy should take into consideration these existing approaches to ensure appropriate protections for children's and students' data.

FERPA, for example, restricts how schools may share student education records and student personally identifiable information as a condition of receiving federal funds.[30] FERPA therefore governs most public K-12 schools, some private K-12 schools, and most public and private institutions of higher education. Substantively, FERPA generally requires affirmative parental or eligible student consent before any release of a student's personal information, and provides parents with the right to inspect educational records.[31] Additionally, COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. The requirements on operators include providing notice to parents on the type and purpose of data being collected, obtaining verifiable parental consent before the data collection process, and retaining children's personal information "for only as long as is reasonably necessary."

The use of educational and student data gleaned from these education technology tools is critical to a variety of policy decisions. For example, the U.S. education system makes federal funding decisions using education data and education records. Identifying inequities in education is often done through access to student data, including broader federal programs, such as the Free and Reduced Price Lunch program as well as vital state programs. Maintaining access to and use of that data affects a host of different policy interests beyond consumer protection.

---

[30] Letter from Jeff Joseph, former President & CEO of the Software & Information Industry Association (SIIA), to the Hon. Robert Hertzberg Regarding the Conflicts Between the Family Educational Rights and Privacy Act (FERPA), the Student Online Personal Information Protection Act (SOPIPA), Section 49073.1 of California's Education Code (AB 1584), and the California Consumer Privacy Act (CCPA) (Jan. 28, 2019).

[31] Id.

The emergence of new laws to protect children and teens online in the U.S. and around the world have renewed the focus of companies of all sizes working to build age-appropriate experiences for all users. Balancing safeguards within online experiences – while preserving the right of users of all ages to be online and access information – should be a priority of policymakers. Emerging themes to apply the "best interests of the child" standard may be a path forward to align global standards and streamline emerging compliance issues for companies of all sizes.

d. In considering equity-focused approaches to privacy reforms, how should legislators, regulators, and other stakeholders approach purpose limitations, data minimization, and data retention and deletion practices?

Legislators, regulators, and other stakeholders should approach policy related to data minimization and purpose limitation with care and careful consideration. An overly restrictive approach can lead to significant unintended consequences that impede innovation, the provision of services to consumers, and methods to address potential negative effects on marginalized communities. Presuming harm in all data practices fails to distinguish between positive and unfair and deceptive data uses. We recommend focusing narrowly on harms caused by improper data collection, retention, and security. If regulation is made without focusing on data minimization principles that are carefully crafted and with consideration for the unique innovation economy in the United States, we fear it will have a chilling effect on the ecosystem because it will hamper new product development and innovation, limit free speech, and increase the risk that the regulation will be struck down in the courts. These are likely to have disproportionate effects on underserved and marginalized communities.

We recommend that NTIA advocate for a flexible approach toward data minimization and distinguish between controller and processor obligations toward the data. "Data minimization" refers to implementing guardrails to restrict specific data processing and retention measures. We believe that guidance reflecting a risk-based approach to data minimization will create productive guardrails for the collection and processing of data, elevating priority review of the highest risk activities. This type of guidance would be beneficial to stakeholders because it would further support the existing state level policies and industry standards. It would be similar in nature to the guidance on data minimization and purpose limitation issued by the UK Information Commissioner's Office.[32]

Existing consumer privacy laws are working toward this objective, by ensuring appropriate protections, without curtailing future uses of data. Under Virginia's consumer data privacy law, a business may be required to ensure the data it collects is reasonable and proportional to the disclosed purposes for which it is processed (unless the business obtains consent) and the business would be expected to discard the data it processes, subject to a specific retention schedule. General purpose data use, in and of itself, has a number of socially

[32] UK Information Commissioner's Office, Purpose Limitation, Data Minimisation and Storage Limitation

beneficial uses including market research, product development, financial analysis, support for national security and law enforcement, and more.

e. Considering resources, strategic prioritization, legal capacities and constraints, and other factors, what can federal agencies currently do to better address harmful data collection and practices, particularly the impact of those practices on underserved or marginalized groups? What other executive actions might be taken, such as issuing executive orders?

Federal agencies can and should address harmful data collection and practices in a variety of ways. The first approach is expanding digital access and training across rural and underserved areas around the United States. Federal agencies can allocate more support and resources towards bridging the digital divide for at-risk and marginalized communities by building on the momentum created by the passage of the Infrastructure Investment and Jobs Act (Pub.L. 117–58)[33]. The tools for successful technology adoption and use are equally as essential as access to affordable broadband itself.[34] A key element of these programs should be training communities on data privacy best practices in easily accessible ways, which can support the most vulnerable populations with access to resources, guides, and instructions on how to safeguard their data.

Additionally, NTIA should strive to advance interagency coordination. Several federal agencies have embarked on initiatives related to data governance in the United States. These include the FTC, which has issued an ANPRM on commercial surveillance and data security;[35] OSTP, which issued last year its Blueprint for an AI Bill of Rights[36]; and NIST, which has undertaken several efforts including one focused on advancing a more productive digital economy.[37] These are all critical areas of consideration and while handled by separate agencies, the individual work streams across agencies will have a considerable impact on funding and outcomes for underserved and marginalized communities. In other words, we recommend that NTIA not view privacy and equity/civil rights issues as a standalone topic, but rather it should carefully assess the work already taking place across the government and evaluate opportunities to incorporate these principles.

6. What other actions could be taken in response to the problems outlined in this Request for Comment include?

b.What role could design choices concerning the function, accessibility, description, and other components of consumer technologies play in creating or

---

[33] Infrastructure Investment and Jobs Act. Pub. L. 117–58.

[34] Comments of the Software & Information Industry Association (SIIA) on the Request for Information: Study to Advance a More Productive Tech Economy (February 2022)

[35] NTIA, Comments of the NTIA to the FTC. Commercial Surveillance ANPR. FTC-2022-0053

[36] Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People, Office White House Office of Science and Technology Policy (OSTP), whitehouse.gov (Oct. 2022); The Biden Administration Launches the National Artificial Intelligence Research Resource Task Force, whitehouse.gov (June 10, 2021).

[37] NIST, "Study To Advance a More Productive Tech Economy." Federal Register. (1/28/2022)

enabling privacy harms, particularly as disproportionately experienced by marginalized communities? What role might design play in alleviating harms caused by discriminatory or privacy-invasive data practices?

c.How can Congress and federal agencies that legislate, regulate, adjudicate, advise on, or enforce requirements regarding matters involving privacy, equity, and civil rights better attract, empower, and retain technological experts, particularly experts belonging to marginalized communities? Are there any best practices that should be emulated?

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 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 U.S. economic competitiveness and how other nations develop their own technology policies.

Congress and federal agencies should encourage technologists to incorporate "privacy by design" into their roadmaps. This should happen with a unique focus on how product design features impact the privacy of marginalized communities. Incorporating a "privacy by design" approach will have success on many fronts: at minimum, 1) companies will be playing a more thoughtful role in shaping their product design early in the process to build a more culturally competent and equitable design, and 2) companies will be able to use this design to better attract, empower, and retain technology experts belonging to marginalized communities, specifically in the space of privacy. As explained in a recent paper titled "*Privacy Research with Marginalized Groups: What We Know, What's Needed, and What's Next,"* poor design choices can lead to an exacerbated experience for marginalized groups - and in some instances, can lead to their exclusion from use. Poor design and loose data security practices can lead to non-use, resistance, and/or apathy towards technology.[38]

At the moment, laws, and guidelines to support the digital accessibility needs for disabled and visually impaired populations (e.g. Web Content Accessibility Guidelines (WCAG) compliance). As a result, many joint initiatives have been launched to promote accessibility within the design process. For example, last year companies like Amazon, Apple, the Davis Phinney Foundation, Google, Meta, Microsoft, and Team Gleason launched the Speech Accessibility Project to make voice recognition technology more useful for people with a range of diverse speech patterns and disabilities. Many of these same companies are also members of TeachAccess, a collaboration between industry, academia, and advocacy stakeholders together to create models for teaching and training students of technology to create accessible experiences. The industry can replicate these processes in the privacy space as well.

[38] Shruti Sannon and Andrea Forte. 2022. Privacy Research with Marginalized Groups: What We Know, What's Needed, and What's Next. Proc. ACM Hum.-Comput. Interact, CSCW 33 pages. (July 2022)

The government can benefit from considering the existing and emerging array of solutions and technologies that are permeating the ecosystem to ensure appropriate safeguards on the processing and sharing of consumer data for marginalized communities. Examples of these solutions include the development of privacy by design programs, the global privacy control, and recent opportunities for privacy-enhancing technologies, a range of policy solutions that embed data minimization into their approach. To date, the industry has made tremendous strides in shaping best practices on privacy and support for data privacy by design, which is the notion that technology should be carefully designed prior to being deployed. Privacy engineering programs are also growing and many companies - from the largest household platforms to the newest startups - are using privacy preserving technologies to streamline the responsible sharing of personal information to unlock analytics that require strong privacy protective practices.[39]

As an existing framework, companies are leveraging the principles in GDPR's Privacy by Design framework and then tailoring these concepts to their own product design and deployment process.[40] Companies should, and are, thinking about data privacy by design by baking this process early into the product design phase, to benefit the needs of a range of groups and protected classes.

We thank you for considering our views on the subject. Please do not hesitate to reach out to discuss this topic further.

SIIA Policy Team

[39] Bosso, Joe. "The Rise of the Privacy Industry." Avast, (February 2022)

[40] "Privacy by Design and Default" General Data Protection Regulation (GDPR). (October 2021)