SIIA
POLICY

Comments of the Software & Information Industry Association (SIIA) on the Request for Information on Public and Private Sector Uses of Biometric Technologies

Submitted to the Office of Science and Technology Policy

January 14, 2022

On behalf of the Software & Information Industry Association (SIIA), we appreciate the opportunity to provide input on the Request for Information on Public and Private Sector Uses of Biometric Technologies (the RFI) issued by the Office of Science and Technology Policy (OSTP).[1]

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include over 450 companies reflecting the broad and diverse landscape of 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. As the only association representing a diverse array of technology companies across the information landscape, SIIA believes in consumer privacy protections and responsible use of emerging technologies, including those that utilize biometric information.

We commend OSTP's efforts to develop a Bill of Rights for an Automated Society,[2] and appreciate the steps that OSTP has taken, through this RFI and a series of roundtables and listening sessions, to hear from consumers, businesses, academics, and the American public. Artificial intelligence (AI) is having a profound impact on all aspects of society and the impact will only continue. Leadership in developing policy to ensure that AI technologies are developed and used responsibly and in accordance with societal expectations is critical. We appreciate OSTP's role in ensuring that emerging technologies advance (and do not undermine) efforts to support diversity, equity, and inclusion (DEI) and individual privacy.

This submission is divided into four parts. First, we provide general recommendations on developing policy guidance on biometric information. These recommendations, applicable more generally to AI, are developed with a view towards policymaking, regulatory development, and statutory drafting rather than providing technical background on questions raised in the RFI. Second, we address the definitions of "biometric information" and "biometric technologies" as used in the RFI. Third, we highlight some of the many socially beneficial uses of biometric information that we have gleaned from our member companies. Fourth, we discuss the need for federal privacy legislation as a critical step on the path towards developing guidance on biometrics.

[1] Office of Science and Technology Policy, Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, Fed. Reg. 86, 193, 56300-02 (Oct. 8, 2021).

[2] See Eric Lander and Alondra Nelson, American Need a Bill of Rights for an AI-Powered World, *Wired* (Oct. 8, 2021).

Guiding Principles for Developing Policy on Biometric Information and Biometric Technologies

One of the challenges inherent in developing governance rules for emerging technologies is that the technologies are constantly evolving. Business and consumers alike need predictability and as a society it is important that we develop practical guardrails to ensure responsible collection and use. We are encouraged by OSTP's focus on the *uses* of biometric information. We believe that focusing on uses is a prudent way to approach the development of guiding principles and regulatory and legislative recommendations.

Building on the approach taken in the RFI, we offer for consideration several guiding principles as OSTP continues its work on biometrics and on the broader Bill of Rights for an Automated Society. Overall, we believe the goal should be for a flexible policy and regulatory framework that will promote both innovation and responsible use—including uses of biometric information that benefit marginalized communities—and establish necessary guardrails that reflect societal norms and expectations.

First, we recommend that OSTP adopt a **technology-neutral approach** to developing policy. We believe the focus should be on transparency, information collection, and information use 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. Biometric information may be collected through numerous technologies and a one-size-fits-all approach will not be sufficiently flexible to provide a groundwork as advances occur. In most cases, a piece of software is not inherently good or bad—much like a hammer is neither good nor bad—and the key is to focus on how the software—or hammer—is used in practice.[3]

Second, we recommend that OSTP look to develop a **risk-based approach**. With respect to the field of biometrics, there is a range of risks to individual rights and other values depending on the type of information collected, how that information is stored and used, and what consumers' expectations are. For example, use of a fingerprint for the sole purpose of verifying identity to unlock a smartphone represents a low-risk situation; so, too, is using biometric information for facial authentication to assist educators in comparing a prior image of the individual to themselves to ensure the proper individual is taking an exam. Many companies use biometric tools strictly for identifying and authenticating consumers with strict use and storage restrictions on that information. These circumstances are likely to result in less risk that consumer data will be re-processed or shared for a secondary purpose. On the other hand, a government-run mass surveillance program using facial recognition that compares faces to images in a large database without restriction represents a high-risk situation; this can occur in a less transparent environment, without consent, where there is a potential for information asymmetry and infringement of constitutionally protected rights.

Responsibility, security, and accountability for biometric information 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 biometric information and design contextualized collection and use restrictions to prevent those harms.

[3]

The harms should be measured based on injury-in-fact to the consumer and consumer expectations. 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.

Third, we recommend that OSTP support 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 biometric information. The work of the National Institute of Standards and Technology (NIST) in developing a risk management framework and establishing guidelines to address algorithmic bias is especially encouraging.[4] NIST has also led many efforts to shape the very first, overarching technical standards and testing for biometrics, starting decades prior to the widespread use of biometrics in routine consumer transactions that we see today. [5,] 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 biometric information is collected and used.

Fourth, we recommend that OSTP **distinguish between public and private** collection and use of biometric information.

In the private context, we note that many companies have built robust frameworks for assessing how they collect and use biometric information. Our members are using biometrics in a wide variety of safe, effective, and efficient applications and contexts that present many benefits to stakeholders and the public, are done in a transparent manner and in accord with consumer expectations. Our members adhere to industry standards and many have established self-regulatory frameworks and principles[6] to ensure pre- and post- deployment impact assessments are conducted both prior to collection of biometric information and upon use of that information for various purposes.

In addition, some companies have proactively chosen to curb some forms of biometrics, including the use of facial recognition technologies, by placing moratoriums on public sector sales, or determining it would be best not to offer the technology at all, due to findings about inappropriate use in public settings.[7] We would encourage OSTP to foster these efforts and focus efforts towards policy that would promote these frameworks and provide appropriate checks on the highest risk situations.[8]

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

[5] See NIST, Biometrics.

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

[7] See Taylor Kay Lively, Facial Recognition in the US: Privacy Concerns and Legal Developments, *Security Technology* (Dec. 2021).

[8] With respect to personal consumer devices (laptops, cell phones, etc.), that use biometric information for facial recognition, many private companies have built-in consumer engagement features that allow consumers to determine the specific uses of the technology, how the technology uses the information and what decisions and outputs are then gathered from that application. This empowers consumers about how their own information is and will be used.

The public sector or government experience with biometric information presents a different situation and we believe that OSTP can play an important role in guiding the government's collection and use of such information.

Governments can make use of biometric 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. Yet there is limited guidance on how the federal government *should* be collecting and using biometric information. Questions abound about what biometric 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.[9] 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.[10] Congress has introduced several bills that would direct the U.S. government on use (or non-use) of facial recognition technologies, [11] yet much can be accomplished through Executive Branch action alone. Many states and local governments are grappling with this issue.[12] It is important that the federal government confront these issues and provide a model for the nation.

Defining Biometric Information and Biometric Technologies

In this part of our submission, we address the definitions of key terms as they appear in the RFI and offer suggestions on how to amend these definitions to support OSTP's policy making efforts.

Biometrics is a category that has been subject to many definitions. As in other areas of advanced technology, including artificial intelligence more generally, it is important to get the definitions right in the first instance. With the Constitution's Bill of Rights as a comparison, we recommend that OSTP

[9] 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*).

[10] Ibid.

[11] 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).

[12] Several states have passed laws governing the public use of facial recognition technology, a subset of biometrics. Virginia and Pennsylvania require prior legislative approval before deploying facial recognition technologies, and states like Massachusetts, Utah, Kentucky, and Louisiana require law enforcement to submit written requests to the state agency that stores the database. Some states, including Massachusetts, Washington, and Maine, have placed additional administrative requirements like obtaining a warrant or court order or meeting a probable cause standard on government entities, while the state of Washington requires public entities and law enforcement to obtain public notice, hold community meetings, and publish an accountability report prior to using facial recognition. California, Mississippi, and Massachusetts have banned local government use of facial recognition. Other states have enacted narrow bans on the use of police body cameras that have facial recognition.

ensure that guiding principles are sufficiently flexible to survive technological advances. At the same time, to the extent OSTP's efforts will ground future regulatory action and lawmaking, there is a risk that definitions with too much flexibility could render enforcement and oversight impractical and have unforeseen, negative consequences.

As OSTP continues in its efforts to assess how biometric information is collected and used and the impacts that biometric technologies have, we recommend that OSTP focus its definitions in the following ways.

First, we recommend that OSTP limit the definition of "biometric information" to measurements of immutable physical characteristics. The definition used in the RFI – "any measurements or derived data of an individual's physical (e.g., DNA, fingerprints, face or retina scans) and behavioral (e.g., gestures, gait, voice) characteristics" – goes beyond this by including "derived data" in the definition.

We are aware of no existing legal precedent that defines biometric information to include information *derived from* physical characteristics. We are concerned that including "derived data" in the definition could lead to policy that does not sufficiently target the core issues around biometric information and, potentially, is used to ground formal guidance or rules that would be virtually impossible to comply with. This, in turn, will make it more challenging to ensure that public and private actors are meeting whatever obligations they may have to treat biometric information with special care and generate unpredictability among the public about what is and is not allowable.

We consider biometric information to refer to immutable physical characteristics – such as fingerprints, retinas, DNA, and facial features – that can be used for authentication or recognition, which OSTP defines to include both "verification" and "identification". This accords with definitions that are used by the Department of Homeland Security (DHS) and NIST. DHS, for example, describes biometrics as "unique physical characteristics, such as fingerprints, that can be used for automated recognition."[13] NIST offers several definitions, each referring to physical and/or behavioral characteristics, rather than derivations from these characteristics.[14] The Code of Federal Regulations and the U.S. Code use definitions that are generally aligned with these.[15]

[13] See Dept. of Homeland Security, Biometrics.

[14] See NIST Computer Security Resource Center, Biometrics.

[15] See 5 CFR 850.103 ("Biometrics means the technology that converts a unique characteristic of an individual into a digital form, which is then interpreted by a computer and compared with a digital exemplar copy of the characteristic stored in the computer. Among the unique characteristics of an individual that can be converted into a digital form are voice patterns, fingerprints, and the blood vessel patterns present on the retina of one or both eyes."); 21 CFR 1300.03 ("Biometric authentication means authentication based on measurement of the individual's physical features or repeatable actions where those features or actions are both distinctive to the individual and measurable."); 27 CFR 73.3 ("Biometrics. A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable."); 34 CFR 99.3 ("Biometric record as used in the definition of *personally identifiable information,* means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting."); see also 46 USC 70123 ("For the purposes of this section, the term 'biometric identification' means use of fingerprint and digital photography

Likewise, jurisdictions that have enacted laws on biometric information have not expanded it to include derivations of physical or behavioral characteristics. The Illinois Biometric Information Privacy Act (BIPA), one of the most extensive biometrics-related legislation enacted at the state level, "does not include information derived from items or procedures excluded under the definition of biometric identifiers."[16]

Second, we have concerns that including "behavioral characteristics" in the definition will present challenges for policy guidance on the collection and use of information based on immutable physical characteristics. Information based on gestures, gait, signature, keystrokes, and so on are often highly situation dependent and subject to environment-based stressors or emotional reactions like fatigue, happiness, and so on. While there may be value in developing guidelines for how public and private actors collect and use such information, we believe this should be done outside the context of biometrics. These types of information are less reliable for verification and identification purposes as they are not immutable. We would also exclude voice recordings, digital photographs, and speech-to-text services for similar reasons. Expanding the category of biometric information to include personal information or personally identifiable information is a form of mission creep that will have unknown consequences. In this regard, we recommend that approach taken by Illinois in BIPA, which excludes "writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color."[17]

Third, we urge OSTP to focus the term "biometric technologies" to those uses of biometric information for recognition – identification and authentication – and not include those technologies that draw inferences based on biometric information. We believe that a focus on identification and authentication will provide a strong groundwork for setting policy around biometrics without introducing a significant amount of uncertainty introduced by extending policy to those technologies that may use biometric information to draw inferences.

Identification and authentication are related but distinct uses of biometric information. While subtle, the difference between the two is that biometric identification is a process that captures biometric information and then compares it to a large database of stored biometric information in order

images and facial and iris scan technology and any other technology considered applicable by the Department of Homeland Security.").

[16] 740 ILCS 14, sec. 10, Illinois Biometric Information Privacy Act of 2008. BIPA excludes photographs from its definitions of biometric information and identifiers, although we would urge clarity in exempting photographs as this issue has been subject to conflicting judicial interpretations in Illinois. See, e.g., Data Extracted from Photographs: Covered Under BIPA?, *The National Law Review* (Mar. 25, 2021). Similar language has been proposed in federal bills, including the National Biometric Information Privacy Act of 2020 (S. 4400, 116th Cong., Aug. 2020).

[17] 740 ILCS 14, sec. 10, Illinois Biometric Information Privacy Act of 2008. Nevertheless, we do not recommend BIPA as a model for liability. BIPA's statutory violation provisions have led to an avalanche of lawsuits for statutory damages without a showing of injury or harm or improper use of biometric information, including lawsuits based on routine employer practices, cybersecurity breaches, and other topics. See, e.g., Illinois Policy Institute, Illinois employers flooded with class-action lawsuits stemming from biometric privacy law (October 2017); Roy Maurer, SHRM, TopGolf Settles Biometric Privacy Lawsuit (July 19, 2021); BlankRome, Analyzing BIPAs Newest Class Action Trend: Targeting the Use of Voice-Powered Technologies (Aug. 30, 2021); Buchanan Ingersoll Rooney, Biometric Privacy Laws Create New Avenue for Data Breach Class Actions (Nov. 17, 2020).

to identify an individual. Law enforcement typically use this type of facial recognition. Contrary to this, biometric authentication involves verifying an individual's identity by comparing it to the same individual's previously provided biometric information. An iPhone uses this type of technology when Face ID is enabled; it is also used, in the education context, for example, to verify that the proper individual is taking an exam. We would urge OSTP to make this distinction clear in any policy guidance arising out of the RFI.

While biometrics may be used, as the RFI states, "for inference of cognitive and/or emotional states," we believe this category of uses should be treated differently. We are concerned that extending any guidance on biometrics to inferential uses could undermine efforts to set clear guardrails and ensure predictability for consumers and businesses alike. Inferential uses, or "soft biometrics," cannot be depended upon, with high accuracy, to identify a person or enable verification of identity.[18] Thus, technologies using biometric information in this manner present a very different risk profile for individual rights and values. We recommend further fact finding on this category of use cases with a focus on the particular risks (and harms) that such technologies may generate.

Positive Use Cases of Biometrics

We listened closely to the comments shared during OSTP's three listening sessions and while we respect the opinions shared, believe it important to highlight some of the beneficial uses of biometric tools. Indeed, despite attention around abuses of biometric information,[19] we believe it is important to recognize the ways in which biometric information can be used to generate socially beneficial uses – including uses that help to remove barriers and provide access to services for marginalized communities. In addition, technologies can use biometric information to create more secure means to authenticate users, contributing to cybersecurity; streamline processes in public health settings; facilitate increased and more efficient access to social benefits; improve public safety; and assist educators across the learning environment.

Tools that gather and use biometric information have the potential to address concerns around diversity, equity, and inclusion and provide services that improve the lives of people from marginalized communities. One example is the biometrics for individuals with disabilities, particularly in instances when these individuals are surfing the web and are required to authenticate their online presence. Features like voice recognition to authenticate web presence could support individuals with physical disabilities. Individuals with sight loss may benefit from a variety of biometric logins, such as fingerprint, face, or iris authentication, which can simplify authentication, for example, when asked to authenticate sight-based CAPTCHA images. Those with dyslexia may also stand to benefit from biometrics, as opposed to strictly memory-based authentication log-in information, like passwords.[20]

[18] See, e.g., Abdelgader Abdelwhab and Serestina Viriri, A Survey on Soft Biometrics for Human Identification, in *Machine Learning and Biometrics*, Jucheng Yang et al., eds. (London: IntechOpen, 2018); U. Park and A. K. Jain, Face Matching and Retrieval Using Soft Biometrics, *IEEE Transactions on Information Forensics and Security*, v.5, issue 3, at 406-15 (Sept. 2010); A. Dantcheva, What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics, 11 *IEEE Transactions on Information Forensics and Security*, v.11, issue 3, at 441-67 (Mar. 2016).

[19] See Office of the Privacy Commissioner of Canada, Clearview AI ordered to comply with recommendations to stop collecting, sharing images (Dec. 14, 2021).

[20] See Abby Young-Powell, Ensuring Biometrics Works for Everyone, *Raconteur* (Feb. 2021).

Research suggests that the algorithms and underlying data fueling some biometric technologies like facial recognition technologies need to be further optimized to support all individuals. To date, bias in facial recognition technologies has led to instances of unethical, biased, and/or discriminatory uses for marginalized communities. But biometrics has the potential, once it is fully optimized for use by diverse populations, to decrease inequity and support people of color and people in marginalized communities, particularly if it helps these very communities who are most at-risk for security hacks, credit fraud, and other negative repercussions to accessing their social benefits.

And the facts are compelling that the future of biometrics is bright. Research by the Center for Strategic and International Studies demonstrates that some of the most accurate facial recognition technologies have an error rate of 0.08% in April 2020, down from an error rate of 4.1% in 2014, according to tests conducted by NIST.[21]

We want to highlight a few of the many case studies from our members that reflect socially beneficial uses of biometric information.

- Google built a machine learning system using open-sourced models to expand the database of forms, expressions and physical characteristics of sign language. This gives individuals with disabilities and their caregivers a better understanding of the types of expressions of sign language that exist and creates a continuously updated database of examples.[22]
- TurnitIn, through ExamSoft, provides access to authentication software that education and professional credentialing institutions can use to validate the identity of the test taker. This provides institutions with a means to preserve the integrity of the test-taking experience while also providing easier access to exams and learning environments.
- Adobe has launched a suite of biometric features, including a forward-thinking facial verification (through a selfie) and government ID authentication, as part of its Document Cloud, which can be used to authenticate remote documents and workstreams. The Government ID Authentication tool compares the selfie to the Government ID to authenticate the user, which provides time and cost savings and creates seamless regulatory compliance for banks, private companies and governments alike. Nearly 8 billion signature transactions have taken place in a one-year period, and nearly half of all Fortune 100 companies are using AdobeSign. This is yet another mechanism that will eliminate the cumbersome nature of paper signatures, create efficiencies for consumers and businesses, and can lead to significant gains for marginalized communities, especially communities with disabilities.

Federal Privacy Legislation is a Necessary First Step

Lastly, we encourage OSTP to play a proactive role in supporting efforts underway to advance a general federal privacy bill. Many of the concerns that the public has raised around the uses of biometric technologies dovetail with concerns around privacy. Yet, the United States has no general application privacy law. We strongly endorse the bicameral efforts underway to advance a comprehensive federal privacy law that will provide strong and meaningful consumer protections (such as individual rights to

[21] See William Crumpler, "How Accurate are Facial Recognition Systems – and Why Does It Matter?," Center for Strategic & Intl. Studies (Apr. 2020).
[22] Kemal El Moujahid, Machine learning to make sign language more accessible, Google - The Keyword (Dec. 2021).

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. The legislation 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.

We are at a unique moment politically when, after years of debate, there appears to be bipartisan support for comprehensive federal privacy legislation. SIIA is working actively with the Senate Committee on Commerce, Science and Transportation and the House Committee on Energy and Commerce to support their efforts to craft a comprehensive federal privacy law that reflects these core elements.

Although some federal privacy legislation proposals address the collection and use of biometric information and others do not, establishing a nationwide, harmonized framework for personal information would, at a minimum, establish a foundation on which to develop targeted guidance on how biometric information is collected and used.[23] A federal privacy law could help to close the gaps that exist across other civil rights and sectoral laws to ensure that companies use data equitably, fairly, and in non-discriminatory manners. It could also establish high-level guardrails regarding the collection and use of biometric information, harmonizing the needs of consumers with those of businesses to foster a healthier digital ecosystem.

We encourage OSTP—and the Biden-Harris Administration—to lend its voice to advance these efforts.

Contact Information

Please direct any inquiries regarding this submission to Paul Lekas, SIIA Senior Vice President for Global Public Policy (plekas@siia.net) and Divya Sridhar, SIIA Senior Director for Data Protection (dsridhar@siia.net).

[23] At the state level, California and Colorado's consumer privacy laws–the California Privacy Rights Act or CPRA, effective January 2023 and the Colorado Privacy Act, effective July 2023–include language that allows consumers further control over facial recognition data. California provides consumers with rights to access, opt-out of the sale of and delete their facial recognition data; Colorado will require businesses to obtain consent prior to processing consumers' facial recognition data. Another area of debate is whether private entities should be allowed to use facial recognition in public accommodations. To date, only Portland, Oregon and Baltimore have enacted regulations that limit commercial uses of facial recognition technologies.