ITI Promoting Innovation Worldwide

January 14, 2022

Via email to: biometricRFI@ostp.gov

RE: ITI Response to Office of Science and Technology Policy (NIST) Request for Information on AI-Enabled Biometric Technologies [Docket Number 2021-21975]

The Information Technology Industry Council (ITI) appreciates the opportunity to provide feedback in response to the Office of Science and Technology Policy's (OSTP) *request for information on AI-enabled biometric technologies.* One of the specific uses of Artificial Intelligence (AI) that has garnered attention not only in the U.S. but around the world is AI-enabled biometric technologies, with a particular emphasis on facial recognition technology. However, ITI recognizes the need to broaden the discussion around AI-enabled technologies beyond facial recognition, including, but not limited to, voice analysis, key stroke analysis, and various health indicators. As such, OSTP's RFI is timely and important.

ITI represents the world's leading information and communications technology (ICT) companies. We promote innovation worldwide, serving as the ICT industry's premier advocate and thought leader in the United States and around the globe. ITI's membership comprises leading innovative companies from all corners of the technology sector, including hardware, software, digital services, semiconductor, network equipment, and other internet and technology-enabled companies that rely on ICT to evolve their businesses. AI is a priority technology area for many of our members, who develop and use AI systems to improve technology, facilitate business, and solve problems big and small.

ITI is actively engaged on AI policy around the world and issued a set of *Global AI Policy Recommendations* in 2021, aimed at helping governments facilitate an environment that supports the development of AI while simultaneously recognizing there are challenges that need to be addressed as the uptake of AI grows around the world.[1] We have actively engaged with the USG on its AI-related workstreams, most recently providing feedback on NIST's efforts to develop an *AI Risk Management Framework* and the *National AI Research Resource.*[2]

ITI and our members share the firm belief that building trust in the era of digital transformation is essential and agree that there are important questions that need to be addressed regarding the responsible development and use of AI technology. As this

[1] Our complete *Global AI Policy Recommendations* are available here: https://www.itic.org/documents/artificial-intelligence/ITI_GlobalAIPrinciples_032321_v3.pdf

[2] See ITI comments responding to RFI on Developing an AI Risk Management Framework here: https://www.itic.org/documents/artificial-intelligence/NISTRFIonAIRMFITICommentsFINAL.pdf; see ITI comments on National AI Research Resource here: https://www.itic.org/documents/artificial-intelligence/2021-9-30_ITICommentsNAIRRRFIFINAL(1).pdf

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

technology evolves, we take seriously our responsibility as enablers of a world with AI, including seeking solutions to address potential negative externalities. To be sure, the tech industry is aware of and is already taking steps to understand, identify and mitigate the potential for negative outcomes that may be associated with the use of AI and AI-enabled systems. Companies are developing technical toolkits to help increase understanding of how AI models perform across different demographic groups and are leveraging ethics frameworks to ensure they are developing AI in a responsible manner. We therefore welcome the opportunity to provide comments on AI-enabled biometrics technologies, with a specific focus on existing governance frameworks and best practices that may be useful to consider moving forward.

General Thoughts

In considering any future policy action, OSTP should focus on specific, high-risk uses of AI-enabled biometrics technologies, rather than on the technologies themselves. It is important to highlight at the outset that AI-enabled biometric technologies only represent one use-case of AI technology. We emphasize this because although there are a discrete set of risks that may be associated with particular types of AI-enabled biometric technologies, such risks are not uniform across all AI technologies, nor are they uniform across biometric technologies as a whole. As with AI more broadly, context and use are critical. In considering any future policy action related to biometric technologies, the USG needs to be careful to draw clear distinctions between different uses of biometric technologies and to focus its policies on specific uses rather than on the technology writ large. For the purposes of any future policymaking activity, we also encourage the USG to clearly define what it considers to be biometric technologies. At present, there seems to be conflation between private sector and public sector uses, and between uses for mass identification or surveillance in public settings and uses in private settings. The RFI – and more broadly, other USG messaging on this subject -- does not distinguish between these uses, though their risk profiles and implications -- especially in the context of privacy, human rights, and access to services and benefits -- can be vastly different. We encourage OSTP, and the USG more broadly, to keep this need for a use-based focus in mind if and when devising policy, which should be carefully tailored to address specific, problematic use cases and mitigate the associated risks, as opposed to horizontally applying one risk profile and one set of policy measures across all biometric technologies.

In seeking to use the information gathered via this RFI to develop a Bill of Rights for an Automated Society (hereafter "Bill of Rights"), we encourage OSTP to take a risk-based approach that considers use-cases or applications of the technology. We recognize that the use of AI-enabled biometric technologies can pose a serious risk to human rights when used for specific purposes in both the public and private sectors. In our view, the "Bill of Rights" terminology seems to imply a set of protections for consumers from government use of AI, but OSTP's focus does not seem limited to government uses. In line with the points we made above, risk should be assessed based on use case and context, instead of evaluating an entire set of technologies collectively, which can be used for many different

purposes. OSTP's event series on developing a Bill of Rights, which focused on the use of AI in criminal justice, social welfare, healthcare, etc., was a good first step in discussing the potential implications of using AI in areas where there may be an outsized risk to fundamental human rights. Yet, even within these sectors, there may be applications where the use of AI does not present an outsized risk – or even, in some instances, any risk to individual rights at all – and so it is important that in developing any future policy intended to address concerns stemming from the use of AI in these sectors, USG takes a risk-based approach, in which it seeks to identify specific civic or consumer problems that require remedies.

There are a wide variety of governance frameworks and best practices that focus on privacy, security, human rights, and responsible AI that create safeguards when used in the development and deployment of biometric technologies. We highlight some of these frameworks in response to question 6 below but believe that many of these frameworks and best practices can be leveraged to address concerns related to the development and deployment of biometric technologies. OSTP and other USG stakeholders considering policies to address biometric technologies should take care to disentangle and deconflict such policy measures from existing policy frameworks, focusing any biometric-specific policies on gaps that aren't addressed elsewhere.

OSTP should seek to align its efforts to develop a Bill of Rights with other ongoing federal agency activities. At the moment, it remains somewhat unclear to us what the Bill of Rights will entail and whether it will result in discrete policy action. For example, the National Institute of Standards and Technology (NIST) is currently developing an AI Risk Management Framework, which will ideally address several areas of relevance to a Bill of Rights. We also think it useful for OSTP to refer to the principles contained in the Office of Management and Budget's *Guidance for the Regulation of AI Applications*. The OMB memo provides a useful backdrop to frame broader federal AI efforts, including those being undertaken by OSTP. In particular, principles related to risk assessment and management, flexible approaches to AI risk management, and public trust in AI are all relevant to this RFI as well as the Bill of Rights efforts more broadly. We also encourage OSTP to align its efforts with the work being undertaken by NTIA on Privacy, Equity, and Civil Rights, which we believe will tie into the development of a Bill of Rights. Finally, OSTP should also reference and integrate other frameworks that are currently in use by federal agencies, including those developed by DOD, ODNI, and HHS so as to align guidance to the extent possible.[3]

[3] Ethical Principles for Artificial Intelligence, available here: https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/; Principles of Artificial Intelligence Ethics for the Intelligence Community, available here: https://www.dni.gov/files/ODNI/documents/Principles_of_AI_Ethics_for_the_Intelligence_Community.pdf; Trustworthy AI Playbook, available here: hhs.gov/sites/default/files/hhs-trustworthy-ai-playbook.pdf

In developing any future policy response on AI-enabled biometric technologies and the Bill of Rights more broadly, we strongly encourage continued stakeholder engagement, particularly with the developers, designers and deployers of AI technology. We appreciate that OSTP has sought to engage with potentially impacted communities early in the development of the Bill of Rights process as evidenced by the recently completed event series and listening sessions, as well as this RFI. While civil society and human rights groups were well-represented on the panels during those sessions, and while we appreciate the opportunity to provide written input on AI-enabled biometric technologies, we strongly encourage additional conversation with those stakeholders who are developing, designing, and deploying AI systems. Such conversations will provide a robust, well-rounded understanding of the landscape and allow for exchange between all stakeholders in the AI ecosystem.

Specific Responses

Before providing specific responses to several of the prompts under question 6, we think it prudent to raise one foundational issue, which is that in the United States, there is not currently a set of criteria or a methodology that can help stakeholders determine whether a particular application of AI technology is high-risk. We view high-risk applications as applications in which a negative outcome could have a significant impact on people, especially as it pertains to human rights, safety, discrimination, or freedom. A set of criteria developed in conjunction with stakeholders would be useful in further devising policy approaches or risk mitigation techniques for high-risk applications. In light of this, we have encouraged NIST, in its work to develop an AI RMF, to develop a methodology or categorization that can help stakeholders determine the risk level of a specific AI use case and then take steps based on that identification to mitigate that risk. This is something that we have advocated for more broadly, encouraging stakeholders to work together to characterize "high-risk" applications of AI, including by identifying the appropriate roles for AI developers and users in making risk determinations.

The balance of our response is focused on question 6, which asks about existing governance programs, practices, and procedures that may be applicable to the use of AI-enabled biometric technologies. We do not focus on a particular use case, but instead offer general thoughts on existing practices that may be widely applicable.

6) Governance programs, practices, or procedures applicable to the context, scope, and data of a specific use case, including information related to:

As a general matter, the USG should encourage an approach to the development of AI systems that promotes fairness and non-discrimination. Such an approach is relevant to AI systems across the board, not just for AI-enabled biometric technologies. In taking an ethical design approach, one perspective worth considering is espoused in the Guidelines set forth by the European High-Level Experts Group, which propose seven foundational principles that characterize a trustworthy AI system, including human agency and oversight, transparency, privacy and data governance, robustness and safety, diversity,

non-discrimination and fairness, societal and economic well-being, and accountability.[4] Although these principles are applicable to AI systems generally, some may be specifically worth focusing on in the context of a high-risk application of AI-enabled biometric technologies.

When considering best practices to address many of the below areas, we encourage the USG in the first instance to look to voluntary, consensus-based international standards and best practices. For example, ISO/IEC JTC 1 SC 42 is undertaking work on developing standards for aspects of AI, including an AI systems process management standard, which demonstrates that a company is undertaking practices that address risks related to bias, fairness, inclusiveness, safety, security, privacy, accountability, and explainability (the "Artificial Intelligence Management System (AIMS) standard").[5]

There are also a variety of frameworks that have been developed which may be useful in managing risks associated with the use of biometric technologies, including the NIST Privacy Framework and NIST Cybersecurity Framework, along with other AI-specific frameworks. Other domestic frameworks include the DOD's Ethics Principles for AI[6], the Intelligence Community's Principles of AI Ethics[7] and the OMB's AI Regulatory Guidance[8].

Additionally, countries and organizations around the world have developed frameworks to help guide the development and use of AI. We highlight the OECD AI observatory which serves as a repository that references various national and global efforts on AI- specific frameworks.[9] We also recommend that OSTP consider the following frameworks as it develops a Bill of Rights for an Automated Society or other policy measures: JTC 1 SC 42 Standards Work[10], IEEE Position Statement on AI[11], IEEE 7010-2020: Assessing the Impact of AI on Human Well-Being[12], the European Commission High Level Experts Group Ethics Guidelines for Trustworthy AI & AI Assessment List for Trustworthy AI[13], the Considerati

[4] See HLEG Ethics Guidelines here: https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html
[5] See progress of the standard here: https://www.iso.org/standard/81230.html
[6] Ethical Principles for Artificial Intelligence, available here: https://www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/
[7] Principles of Artificial Intelligence Ethics for the Intelligence Community, available here: https://www.dni.gov/files/ODNI/documents/Principles_of_AI_Ethics_for_the_Intelligence_Community.pdf
[8] Guidance for the Regulation of Artificial Intelligence Applications, available here: https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf
[9] See OECD AI Observatory here: https://oecd.ai/en/.
[10] [Link to JTC 1 SC 42 Standards Work]
[11] IEEE Position Statement on Artificial Intelligence, available here: https://globalpolicy.ieee.org/wp-content/uploads/2019/06/IEEE18029.pdf
[12] IEEE 7010-2020 - IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being, available here: https://standards.ieee.org/standard/7010-2020.html
[13] Ethical Guidelines for Trustworthy AI, available here: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai; Assessment List for Trustworthy Artificial Intelligence, available here: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

Artificial Intelligence Impact Assessment (AIIA)[14], Australia's AI Ethics Framework[15] & Actions Plan[16] and Singapore's Model AI Governance Framework.[17] We expand upon these frameworks in our comments responding to NIST's AI Risk Management Framework and would encourage OSTP to review those comments for a fuller understanding of each framework.[18]

However, if there is concern that existing frameworks and best practices are not sufficient to mitigate the risks identified for specific uses of AI-enabled biometric technologies applications, we encourage the USG to undertake an extensive analysis of the current landscape, mapping different standards and frameworks to existing risks so as to better understand where there may be gaps that need to be filled.

- *Stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, assessments, strategies, etc. to mitigate potential harm/risk of biometric technologies*
- *Best practices or insights re: design and execution of pilots or trials to inform further policy developments*

In the response we provided to NIST on the AI RMF, we recommended that the development of the AI RMF be grounded in experience and evidence gathered via policy prototyping.[19] We believe such an approach could be useful to address concerns related to biometric technologies as well, where a variety of stakeholders can come together to co-create governance frameworks, including regulation and voluntary standards. Developing and testing governance frameworks in a collaborative fashion allows policymakers to see how such frameworks can integrate with other co-regulatory tools such as corporate ethical frameworks, voluntary standards, conformance programs such as those for testing and certification, ethical codes of conduct, and best practices. This method has been successfully used in Europe to test an AI Risk Assessment framework, leading to several concrete recommendations for improving self-assessments of AI.[20]

---

[14] The Artificial Intelligence Impact Assessment, available here: https://www.considerati.com/static/default/files/documents/pdf/Artificial%20Intelligence%20Impact%20Assessment%20-%20English[2].pdf

[15] Australia's Artificial Intelligence Ethics Framework, available here: https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-ethics-framework

[16] Australia's AI Action Plan, available here: https://www.industry.gov.au/sites/default/files/June%202021/document/australias-ai-action-plan.pdf

[17] Singapore Model AI Governance Framework, available here: https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf

[18] ITI Response to AI Risk Management Framework, available here: https://www.nist.gov/system/files/documents/2021/09/14/ai-rmf-rfi-0058.pdf

[19] Ibid.

[20] See OpenLoop *AI Impact Assessment: A Policy Prototyping Experiment*, available here: https://openloop.org/wp-content/uploads/2021/01/AI_Impact_Assessment_A_Policy_Prototyping_Experiment.pdf

- *Practices regarding data collection (including disclosure and consent), management (including data security and sharing), storage (including timeframes for holding data), review, and monitoring*

In general, companies may use techniques such as anonymization, pseudonymization, deidentification and other privacy enhancing technologies (PETs) as well as Privacy Preserving Machine Learning (PPML), which ensures that data can be used to train algorithms and perform AI tasks without breaching privacy. Industry is also exploring the use of "federated learning," which aggregates data in ways so that the individual data points are kept private, but AI can be performed on the aggregate with minimal loss of accuracy.

Beyond that, because AI operates in an existing policy and regulatory framework, personal data and related privacy concerns must be taken into account. Indeed, there are laws worldwide that govern the ways in which biometric data, in particular, can be stored and processed. For example, the GDPR prohibits the processing of biometric data for the purpose of uniquely identifying natural persons (with some exceptions). In the absence of a comprehensive privacy law in the United States, states like California, Washington, and Virginia have also passed privacy protection laws, which implicate biometric data and govern the ways in which this sensitive data can be used. To enable trust and interoperability and to facilitate research to develop stronger privacy and security guarantees, we continue to advocate for the development of a national privacy law in the United States, consistent with *ITI's Framework to Advance Interoperable Rules on Privacy*.[21] Indeed, such a law may help to provide a concrete mechanism to address some of the underlying concerns signaled by the prompts in this RFI, including around consent, use, and redress.

- *Performance auditing and post-deployment impact assessments*

In certain high-risk settings, performance auditing and post-deployment impact assessments may be appropriate. However, we do not recommend requiring auditing and post-deployment impact assessments for *all* AI-enabled biometric technologies, as this would be out of step with a risk-based approach. Indeed, as we have referenced above on several occasions, not all uses of these technologies inherently present a risk to human rights. At this point, however, we believe there are more questions than answers around such a mechanism, including which standards an impact assessment would test to, how impacts would be judged, whether such an audit would be voluntary, who would undertake the audit, among others. We therefore encourage the USG to further explore these concepts, and questions, in conjunction with relevant stakeholders, including developers and deployers of AI technology. Doing so will help ensure that any policy that is developed strikes an appropriate balance between protecting privacy and civil liberties, while also allowing for innovation.

[21] ITI Framework to Advance Interoperable Rules on Privacy, available here: https://www.itic.org/public-policy/FINALFrameworktoAdvanceInteroperableRules%28FAIR%29onPrivacyFinal_NoWatermark.pdf

- *Practices re: use of biometric technologies in conjunction with surveillance technologies*

It is worth considering the risk-based approach taken in the EU AI Act, which classifies biometric identification and categorization of natural persons as high-risk, and as a result imposes additional obligations on developers seeking to place such systems on the market.[22] However, the way in which biometric technologies is defined matters, as not every use of biometric technologies is inherently high-risk. We believe that the definition should be understood as clearly targeting biometrics-based technologies that (i) involve the processing of biometrics of an indiscriminate number of individuals and require comparing an individual's biometrics to the biometrics of many other individuals stored in a database to identify said individual (i.e., one-to-many matching or identification) as opposed to one-to-one matching or verification which involves comparing two biometric templates usually assumed to belong to the same individual and in which no link with the actual identity is established; and/or (ii) cover situations where biometrics are used to identify individuals without their knowledge, rather than a situation where a well-informed individual deliberately chooses to verify their identity based on their biometrics in order to transact or otherwise interact with a service provider or a government service. We note, though, that in leveraging this definition, it is important to evaluate whether and to what extent a risk is posed by this sort of biometric technology using other criteria as well, including the impact of the decision the AI-enabled biometric technology application might have on an individual or group of people.

The Act also bans the use of real-time biometric identification by law enforcement in publicly accessible spaces, though there are specific exceptions to the ban. As we noted in our response to the consultation on the AI Act, we recognize there are serious risks to fundamental rights that can be posed by government use of AI for surveillance purposes. At the same time, it is also important to recognize that there are public safety and national security benefits that may come from allowing responsible deployment with strict, meaningful safeguards.

Managing risks in these operations is possible through clearly defined processes and controls such as human review, sufficient confidence scoring (for instance by assigning a percentage of accuracy to any output), judiciary supervision, clear use policies, reasonable boundaries around data retention, and transparency measures. Additional transparency requirements on the user of the AI system (for instance related to when, where and how the AI system is used, how the data is processed and stored and for how long) may be a solution to enhance safeguards for the safe and responsible deployment of such systems.

[22] See Proposed Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (AI Act) And Amending Certain Union Legislative Acts here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

- *Practices for public transparency regarding use (including notice of use), impacts, opportunities for contestation and for redress, as appropriate*

Transparency is important in facilitating trust in AI technologies, particularly those that may implicate fundamental human rights. In our *Global AI Policy Recommendations,* we explore the idea of explainability as one way to enable transparency. Our recommendation regarding explainability, however, speaks more broadly to transparency of AI systems, as opposed to public transparency. That being said, meaningfully explainable AI systems can play an important role in providing an opportunity for impacted entities to understand how and why a system may have arrived at a certain outcome. While explainability will not be useful in every instance, we believe that for high-risk use cases, especially, explainability can act as one safeguard. However, explainability may not always be possible. We appreciate that the USG, through NIST, has already started to undertake work to consider appropriate practices around explainability with the publication of its *Four Principles of Explainable AI*.

In the context of privacy, transparency -- whereby the providers of an AI solution are able to declare how data is being used – also matters. Gaining increased visibility into data sets is important in facilitating trust in a system, such as through a better understanding of where the data came from, how it was cleaned, and what features were used to train an algorithm, etc. However, while increasing visibility can provide additional insight into why a model may have behaved in a certain way or resulted in a certain outcome, we need to approach consideration of transparency in a measured and targeted fashion to avoid unintended consequences.

5) Exhibited and potential benefits of a particular biometric technology

Although there has been a significantly negative focus on facial recognition technology, it is worth noting that such technology – when using the best algorithms – is a powerful tool to help users verify their identity and to prevent fraud. With the right privacy and transparency practices, facial recognition can be valuable when the technology operates on a personal device. This method of on-device facial recognition is deployed in systems used to unlock device such as smartphones, as well as for biometric-based authentication more generally. Since 2000, NIST's Face Recognition Vendor Testing Program (FRVT) has assessed capabilities of facial recognition algorithms for one-to-many identification and one-to-one verification. In a 2019 study, NIST found that the most accurate *identification* algorithms have "undetectable" differences between demographic groups.[23] This is encouraging as industry continues to innovate and improve upon this technology.

Additionally, many of our everyday tasks require verifying our identity in the digital world (for example to fill in our tax return online or to sign into our e-banking app). At the same time, malicious actors have been developing new ways to commit fraud and accomplish

[23] See NISTIR 8271: Face Recognition Vendor Test Part 2: Identification, available here: https://www.nist.gov/system/files/documents/2019/09/11/nistir_8271_20190911.pdf#page=49

nefarious purposes. Combinations of data attributes that resemble a "real person" can be purchased or stolen and used to create a false digital identity or a nefarious actor may create multiple identities with different information (name, date of birth, address, etc.). Using biometric-based technologies can prove to be very useful to detect such bad actors, as stealing or altering a biometric identifier is much more difficult.

In the payment authentication space, the financial industry is gradually moving away from knowledge-based authentication tools given their limited security (passwords or PINs can be stolen), and is investigating the possibility of leveraging authentication solutions that rely on biometrics. Biometrics can serve as the basis for a reliable authentication method and have several advantages over knowledge-based authentication, including reduced risk of social engineering, and reduced transaction failure and abandonment rates (and consequently reduced harm to consumers).

Other beneficial use cases of biometric technologies include voice recognition in personal and home devices that fosters convenience, allows consumers to conduct their daily lives more seamlessly, and makes life easier for people with certain disabilities. In the new world of hybrid work, facial recognition also makes working from home easier in online video conferencing systems, where it helps to facilitate background blur and background replacement.

***

Once again, we appreciate the opportunity to provide input on OSTP's RFI on AI-enabled biometric technologies. To the extent this information is used to inform the development of a Bill of Rights for an Automated Society, we encourage OSTP to focus on high-risk uses of AI-enabled biometric technologies, leverage existing standards and frameworks, align its efforts with other ongoing federal agency activities, and continue robust, diverse stakeholder engagement. We agree that facilitating trust in an era of digital transformation is essential and that important questions related to AI need to be addressed to help foster that trust. At the same time, it is important to keep in mind that there are beneficial uses of biometric technologies and encourage OSTP to consider how to support continued innovation should it seek to devise policy in this arena. Please view ITI as a resource on this matter; we are always happy to provide our perspectives.

Sincerely,

John S. Miller
Senior Vice President of Policy
and General Counsel

Courtney Lang
Senior Director of Policy