Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
Consumer Technology Association
Comments on
OSTP Request for Information on Biometric Technologies and an AI Bill of Rights

Respondent Name: Consumer Technology Association
Respondent Type: Industry Association

I. Introduction

The Consumer Technology Association® (“CTA”)® respectfully submits these comments in response to the Office of Science Technology and Policy (“OSTP”) request for information (“RFI”) related to Public and Private Sector Uses of Biometric Technologies. CTA supports OSTP’s effort to understand the innovative potential of biometric technologies in considering whether an artificial intelligence (“AI”) Bill of Rights (“AI Bill of Rights”) is necessary.

CTA is pleased to share our members’ perspectives regarding the development, use, and potential of biometric technologies. We believe that these tools present great opportunity to further consumer protection, reduce inequality, and improve quality of life for all Americans.

CTA supports efforts to ensure that biometric technologies and AI are designed, developed, used, and evaluated in a responsible manner. As CTA has previously explained, “these tools should be used carefully, subject to proper guardrails that promote beneficial uses while safeguarding against privacy and civil liberties harms.” Left untethered and in the hands of bad actors, these powerful technologies can pose risks to consumers. These risks are not consistent across technologies or contexts, but in fact vary depending on the use case, developer, and end user. The dual goals of developing responsible AI and enabling innovation are best served through an intentional commitment to develop and implement codes of conduct, voluntary standards, and best practices that complement developing or existing policy initiatives and encourage self-regulation. When based upon clear and targeted frameworks and principles, self-regulation can result in meaningful protection for users and profound innovation while minimizing potential bias and enhancing trustworthiness. OSTP has an opportunity with its AI Bill of Rights to present such a statement of principles, resulting in a flexible tool that adapts to changing technologies, rather than a rigid, quickly outdated set of fixed rules that neither encourages nor adapts to innovation. In addition, educational activities that enhance people’s understanding concerning ethics related to biometric technologies are beneficial for extending an appropriate way of using these technologies.

---

1 CTA® is the tech sector. Our members are the world’s leading innovators—from startups to global brands—helping support millions of jobs. CTA owns and produces CES®—the largest, most influential tech event on the planet.
Respectfully, CTA urges OSTP to consider a risk-based approach to an AI Bill of Rights, one that recognizes the variety of biometric technologies and leverages existing law, regulation, and best practices to match any potential new regulation to the degree of risk (and corresponding benefits) any particular biometric-based AI tool may create. This is necessary to ensure that the public, the economy, and the world can benefit from the tremendous potential of biometric technologies and AI, and to allow regulators to better understand and evaluate the potential costs, and benefits, of implementing a framework that may lead to new rules and restrictions on the development and use of AI.

II. Biometric Technologies Present Real and Potential Benefits to the Public.

The benefit of biometric technologies is incontrovertible. As CTA explained in its June 2020 report on facial recognition and biometric technologies, “biometric technologies are already offering consumers increased convenience, enhanced data security, and improved physical safety.”4 The potential benefits of biometric technologies are limited only by the imagination of entrepreneurs and engineers. We explore below examples of just a few of the many benefits to consumers:

a. Accessibility. Several companies use facial recognition and other biometric technologies to address challenges faced by individuals with a range of disabilities. For example, Aria, which provides tools to assist blind and low-vision individuals, has created specialized glasses to connect individuals with visual impairments with remote agents who can see the user’s surrounding environment through the glasses and describe it to them in real time, increasing accessibility without compromising safety. Among other things, Aria’s technology employs facial recognition tools to identify individuals nearby who are known to the user, allowing the remote agent to help the user interact fluidly with their colleagues, friends, and family. As another example, Intel developed an AI-powered motorized wheelchair allowing severely disabled users to use facial movement to direct the chair’s movement, improving mobility and independence. As automated vehicles develop and expand, integration of biometric technology will allow individuals who otherwise would not be able to operate a vehicle independently to easily run errands, visit family and friends, and enjoy newfound mobility.5

b. Public Safety. Biometric technologies are used throughout public and private life to further personal and collective safety and security. Fingerprint/finger vein scanners, iris identification, and facial recognition tools can determine who is—and who is not—authorized to enter a property, building or room, for instance. Banks and other financial institutions look to facial recognition technology, and some are experimenting with fingerprint/finger vein technology, to prevent fraud and confirm identity6 and prevent or

4 Id. at 5.
solve ATM thefts.\(^7\) To address vehicle theft, manufacturers are installing biometric recognition tools to determine who is permitted to start and drive a car or truck.\(^8\) Driving on the streets is safer due to some vehicles’ inclusion of face and posture analysis software that identifies inattentiveness, drowsiness, and other potential safety issues, alerting the driver so they can avoid accidents and stay safe.\(^9\) Biometric technologies improve consumer security in their personal technology as well, such as fingerprint/finger vein scanners or face scans to open sensitive phone apps, verify identity, complete a transaction, provide enhanced cybersecurity, or sign into a personal device. Furthermore, consumers increasingly look to biometric technology to enhance their security in the home. Smart locks, security cameras, and other devices identify guests and family members thus giving consumers peace of mind and furthering protection of their homes and families.

c. **Travel Convenience and Safety.** U.S. Customs and Border Protection ("CBP") and the Transportation Security Administration ("TSA") have deployed facial recognition technologies to facilitate screening increasing volumes of travelers.\(^10\) These systems help verify identities, furthering individual and collective security while enabling travelers to proceed quickly to their destination. Similarly, Japanese authorities began using facial recognition technology at Narita Airport in Tokyo in 2019, and announced plans to expand the program to additional airports.\(^11\)

d. **Energy Efficiency.** Biometric technologies can significantly enhance individual and collective energy efficiency. For example, sensors embedded in clothing and furniture will allow for dynamic adjustment of temperatures within a home. Appliances and other facilities in the home could be automated to activate when sensors perceive the need and otherwise hibernate.\(^12\) These efficiencies would be reliant on the use of biometric technology—and the development of the technologies itself requires the expansion and use of such technology.

e. **Healthcare efficiency.** Biometric technologies are in active use in the healthcare setting to improve patient experiences, assist care teams, and create efficiencies in diagnoses with remote patient monitoring. For example, several hospitals and care facilities have integrated in-room devices to enable patients to better communicate with their care teams

---


\(^9\) Id.


and families, and to share post-surgical data between at-home patients and their care teams. Voice biomarkers may also assist in detecting certain conditions or even adverse issues within a patient’s home. Additionally, care teams may leverage voice services for note capture during visits and paired with AI, voice technologies may help care teams with condition diagnosis and medical claims. Biometric technologies also expedited secure, authenticated, and efficient mechanisms for providers and patients to access appropriate records through proof of identity.

As noted above, biometric technology is not only used in the commercial sector but also used by public sector actors, including numerous federal agencies to help keep the public safe, enhance cybersecurity and national security, secure borders and improve the delivery of medical services. These and many other use cases were outlined in a recent GAO Report summarizing the many federal agencies that currently use this technology to fulfill their missions. Thus, any accounting of the benefits of biometric technologies must also consider the increasingly important role of this technology to help government agencies fulfill critical missions and mandates.

III. Existing Law and Standards Protect Consumers.

A range of existing laws at the state, federal, and international level and robust industry and global standards help manage the risks of biometric technologies. We outline below just a few of the many ways the development and use of biometric technologies and AI are currently regulated and consumer harm alleviated:

a. The FTC Act and State UDAP Statutes: Section 5 of the Federal Trade Commission (FTC) Act prohibits “[u]nfair methods of competition” and “unfair or deceptive acts or practices in affecting commerce.” Similarly, each state has its own corollary law or laws, referred to as “Unfair or Deceptive Acts or Practices” (“UDAP”) statutes. The FTC, state attorneys general, and, in many states, private citizens can act against deceptive or unfair uses of information from biometric technologies and AI. Indeed, the FTC has already articulated its intention to use existing authority to ensure that AI tools, including those enabled by biometric technology are transparent, truthful and representative.

b. Federal and State Anti-Discrimination Laws: The Civil Rights Act of 1964 bars employers from discriminating against applicants or employees on the basis of race, religion, sex, and national origin. The Act prohibits not only affirmative and intentional discrimination but also facially neutral practices with a disproportionate impact on

---


protected classes. Many states have similar legislation. The Genetic Information Nondiscrimination Act prevents employers from using an applicant’s or employee’s genetic information as the basis for an employment decision. Other state and federal laws prohibit discrimination on the basis of pregnancy, age, disability, and citizenship. Individually and collectively, these laws help ensure that information collected using biometric technologies is not used inappropriately in employment-related decisions.

c. **Children’s Online Privacy Protection Act (“COPPA”):** COPPA limits the ability of website operators and online service providers to collect personal information from children. This protects children from the online collection of their biometric information, and appropriately puts parents and guardians in the “driver’s seat” around information collected about their children.

d. **California Consumer Privacy Act/California Privacy Rights Act (“CCPA”/“CPRA”) and Other State Privacy Laws:** The CCPA and new, similar state privacy statutes (i.e., Colorado Privacy Act, Virginia Consumer Data Protection Act) impose a variety of obligations on companies that collect, process, and/or retain the personal information of individuals in their respective states. Among other things, companies must provide notice at or before the collection of personal information and allow residents the ability to “opt out” of any “sale” of their personal information, which includes biometric information. Each state considers “biometric information” sensitive personal information, which affords it greater protection. Colorado and Virginia even require that a company receive affirmative, opt-in consent to use biometric information.

e. **Illinois and Other State and Local Biometric Privacy Laws:** Illinois’s Biometric Information Privacy Act (“BIPA”) imposes a range of obligations on companies collecting biometric information, including requirements to: (1) obtain written consent before collecting biometric information; (2) securely store biometric information; (3) destroy biometric information in a timely manner; and (4) disclose their policies on information use and retention. BIPA contains a private right of action and has resulted in significant damage and injunctive relief settlements for consumers. Several other states and localities, including Washington, Texas, New York City, Portland, OR, San Francisco, Oakland, CA, and several cities in Massachusetts have similar laws regulating the use of biometric-based applications, generally, or facial recognition technology, specifically by private sector and public sector actors.

Further, existing laws and norms at the international and multi-national level address data protection and privacy, discrimination, and consumer protection related to biometric information. For example, companies operating in Europe are subject to certain notice, consent, and transparency obligations under the GDPR for any data processing of EU subjects’ data. These laws are successful in protecting consumers, enabling recourse, and setting standards and compliance expectations for companies developing AI systems and using biometric technologies.

Any consideration of laws, standards and existing norms currently protecting consumers should also consider that biometric technologies are shaped and regulated not only by black-letter law,
but also by robust standards and governance practices developed by the industry and leading developers of this technology.

For example, CTA has contributed to and published numerous studies and standards regarding AI development, including CTA-2096 regarding developing trustworthy AI systems,17 CTA-2089 regarding the definitions and characteristics of AI,18 and the published standard CTA-2090 regarding the use of AI in healthcare and trustworthiness.19

The International Organization for Standardization and International Electrotechnical Commission published ISO/IEC JTC1 standards project 23894 regarding AI risk management,20 the National Institute of Standards and Technology is creating an AI Risk Management Framework,21 and the Organisation for Economic Cooperation and Development (OECD) is in the process of developing its own framework for assessing the opportunities and potential risks presented by different types of AI systems.22 Thus, policymakers should recognize that these standards can provide a framework for acceptable uses that enable innovation while mitigating risks. Policymakers should also consider expanding voluntary testing and performance standards, and updating public sector best practices and guidance documents,23 as means of achieving these goals.

IV. A Deliberate Approach that Balances Risks Against Benefits and Current Industry Safeguards and Practices Will Result in a Meaningful AI Bill of Rights that Will be Supported by Consumers and Industry.

An AI Bill of Rights could be a reliable tool for cultivating and protecting innovation while establishing common principles to address potential risks and harm. As OSTP develops its AI Bill of Rights, CTA recommends that OSTP leverage the protections afforded under existing law and industry safeguards, while also embracing the many benefits of biometric technology and AI tools already in the marketplace.

CTA suggests the following be considered as part of any AI Bill of Rights:

23 See, e.g., Dep’t of Justice, Bureau of Justice Assistance, FACE RECOGNITION POLICY DEVELOPMENT TEMPLATE FOR USE IN CRIMINAL INTELLIGENCE AND INVESTIGATIVE ACTIVITIES (Dec. 2017); F.T.C., FACING FACTS, BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES (Oct. 2012).
a. **Risk-Attentive.** Not all biometric technologies and AI systems present equivalent potential risk to all consumers; risk is context-specific, implementation dependent, and potential harm may significantly vary from user to user. CTA urges OSTP to recognize that the diversity and variety in biometric technologies and AI demands a flexible approach to evaluate risk associated with specific uses. A risk-benefit analysis may be more meaningful in this context than hardline standards.

b. **Incorporation of Existing Laws and Standards.** The AI Bill of Rights should leverage existing and proven laws and standards by: (a) incorporating a focus on compliance with existing applicable law; and (b) emphasizing that industry groups, jurisdictions, or other actors should be encouraged to self-regulate; and (3) acknowledging that existing laws already establish important ground rules when developing self-regulatory standards or any potential new regulation. Leveraging existing law not only ensures that the public and businesses understand their rights and responsibilities but also furthers the efficient implementation of any AI Bill of Rights. Businesses can utilize their existing governance processes to ensure compliance with existing laws, resulting in further efficiency and cost reduction as they ensure their practices are aligned with an AI Bill of Rights and aligned with perceived and actual risk that will enhance the deployment, adoption, and use of biometric technologies and AI systems.

c. **Nuanced.** The AI Bill of Rights should recognize the benefits of technological innovation and broad data collection, including of biometric information, where such collection is consistent with existing legal requirements. Appropriate collection and incorporation of additional and varied data inputs will improve AI systems and help address and mitigate potential and harmful bias over time. Better functioning AI (i.e., AI trained on greater amounts and more diverse data, and deployed with appropriate considerations and mitigations) can provide further benefits to the public, such that the AI systems produce more accurate, trustworthy, and ethical outputs. Without sufficient and varied data inputs, desirable outputs may remain unattainable and consumer distrust of the technologies may thwart further development and deployment.

d. **Flexible.** The AI Bill of Rights must be flexible. An extensive, costly (double-digit) compliance process before biometric technology or an AI system can be developed or used may not be appropriate across applications and instances without regard to inherent or perceived risk, including lack of risk. Overly prescriptive rules may stifle innovation and foreclose use of this technology, especially for those applications where possible harm is minimal.

e. **Iterative.** References to a “Bill of Rights” connote fixed, “Constitutional” standards in the American imagination. Such an approach for an AI Bill of Rights would be significantly and harmfully out-of-step with the reality of technological development, innovation, and the actual and potential benefit of biometric technology and AI. CTA emphasizes that, as technology develops, policies and regulations must be able to change. While a Bill of Rights could be a statement of principles regarding biometric technology and AI development, OSTP should emphasize that it is only the start of a process that
will require additional data, evidence, and robust risk-benefit analyses. Further iterations of a Bill of Rights and any resulting recommendations should recognize these complexities. OSTP might consider an incremental and iterative process for a Bill of Rights development: a series of drafts leading to an initial Bill of Rights, with a clear statement that the Bill of Rights is intended to evolve as technology changes.

V. Conclusion

The development and deployment of biometric technologies present immense and transformative benefits for society. CTA is a proud, active participant in the global conversation regarding the regulation of these technologies. We commend OSTP’s efforts to join this dialogue and believe an AI Bill of Rights can serve as a helpful synthesis of principles enshrined in law and recognized by industry. The United States is a hub for the development of biometric technology and AI; we must preserve our leadership and culture of innovation, while ensuring that we protect consumers as AI systems become increasingly interwoven in all aspects of our everyday professional and personal lives.