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.
Bipartisan Policy Center Response to OSTP's RFI on Public and Private Sector Uses of Biometric Technologies

Introduction

The Bipartisan Policy Center (BPC) is committed to developing viable, consensus-driven solutions to improve public and private sector use of biometric technologies. We appreciate the Office of Science and Technology Policy's (OSTP) invitation to provide information about the use of these technologies and impacted stakeholders and efforts to develop a bill of rights for an automated society. BPC works with a wide range of stakeholders from government, academia, industry, and civil society to develop recommendations on privacy issues encompassing biometric privacy and is pleased to share our expertise and research in the comments below.

Much of our response for this RFI reiterates critical points made in published research papers and fact sheets to supplement our ongoing work in this space. We encourage Congress to provide unique attention to high-stakes privacy issues concerning biometric information. Congress must base decisions on regulating or providing safeguards around sensitive information on a cooperative and multi-stakeholder approach.

We look forward to OSTP's continued undertaking of similar efforts to address these issues.

Overview: The purpose of this RFI is to understand the extent and variety of biometric technologies in past, current, or planned use; the domains in which these technologies are being used; the entities making use of them; current principles, practices, or policies governing their use; and the stakeholders that are, or may be, impacted by their use or regulation. OSTP encourages input on both public and private sector use cases.

Detailed Response

1. Descriptions of use of biometric information for recognition and inference: Information about planned, developed, or deployed uses of biometric information, including where possible any relevant dimensions of the context in which the information is being used or may be used, any stated goals of use, the nature and source of the data used, the deployment status (e.g., past, current, or planned deployment) and, if applicable, the impacted communities.

The collection, storage, and use of biometric information has grown over the years and will continue to grow as IT administrators seek to secure and authenticate users. Biometric information is proliferating workplaces, government agencies, and everyday life. Without regulation or guidance, companies and individuals are almost entirely determining how to deploy new technologies appropriately. We've identified a few of the uses of biometric systems by employers and government agencies.
In the workplace: Biometric authentication and identification technologies have been deployed in workplaces for many years. Many older systems in the workplace include biometric time tracking devices and authentication tools such as fingerprint or face-scanning technology to access secure work devices or clock in for a shift. In many cases, fingerprint readers have replaced the “punch card” for many hourly work environments. These technologies can be scaled up or down according to employers’ surveillance preferences. For example, clocking in and out of a shift in a warehouse using your fingerprint represents a small biometric footprint. At many retailer fulfillment centers, employees are tracked using facial recognition throughout their shift, representing a large biometric footprint. This includes physical tracking to ensure that workers are following safety rules, monitoring their activities on the warehouse floor, and other applications.

More modern biometric uses in the workplace include things like tracking eye movements and facial expressions through a webcam to ensure a workers’ attention is staying on task, and sentiment analysis to gauge the mood of workers. Non-traditional use of biometrics in the workplace includes data collected through health tracking devices that track things such as location, heart rate, gait, or other physical attributes. This type of data collection has only increased as remote work environments become more popular.

Government use: Biometric data collection in the government sector is prolific, and there are many examples of government agencies and law enforcement's collection and use of biometric information. Similarly to the use of biometric identifiers in the workplace, a few departments detect their employees’ identities using biometric technology. The Defense Department and Air Force use biometric recognition technology for entry into secure areas. Several government agencies are expanding their use of biometric data. The U.S. Customs and Border Protection (CBP) Agency Global Entry program, for example, uses biometric identifiers in several ways. Originally used as facial recognition technology upon EXIT, CBP’s biometric scanning procedures have expanded to facial scans to verify passport and VISA images and other technology to expedite clearance for travelers arriving in the United States. Some land borders ports also use biometric devices and algorithms to verify travelers. CBP's responsibility to confirm the identity of international travelers through a facial recognition process is balanced by its commitment to privacy by limiting the amount of personally identifiable information used and the deletion of photos of U.S. citizens and non-citizens. Like any successful implementation of biometric technology, the operation of an efficient commercial travel process will require additional assessment and gradual rollout to wherein early experiences inform further deployment. The NSA deployed technology that can identify people by the sound of their voices as early as 2006. The system takes samples to make a “voiceprint” then compares other recordings to the voiceprint to identify a match. The existence of the system was revealed when Edward Snowden released classified documents to the public.
Federal law enforcement captures individuals’ biometric information through fingerprints, and images and videos that capture a person’s facial features such as mugshot photos and driver’s license photos. According to the FBI’s Privacy Impact Assessment, information collected for the biometric identity and criminal history system is protected through several measures, such as limited retention time and strong security features to lower risks to individuals’ privacy.

Some local governments have also benefited from the installation of biometric identifiable technology. Cities from Atlanta to Portland installed thousands of cameras that can combine with facial recognition technology particularly for criminal investigations. This technology has come under scrutiny by other cities that have recently restricted the use of facial recognition technology in public spaces. For example, in 2019, San Francisco passed a law to ban the use of facial recognition software by the police and other agencies.

**In health care:** Biometric technology can substantially improve capabilities in the health care industry and improve staff and patient safety. Patients’ personal health identifiers are generally protected under federal health privacy law, HIPAA, as discussed in a later section. For authentication purposes, biometric identifiers can be used to protect patients’ sensitive information and reduce registration times. Biometric technology is also a promising tool for improved accuracy and efficiency of electronic medical records (EMR) and health records (EHR). Biometric technology is poised to grow in one of the largest sectors in the US, however, lawmakers should consider how to streamline transitions in the health care system and how to ensure patients’ safety is protected.

Congress must learn from successful implementation as well as mismanagement and mistakes identified in this response and by other RFI responses to better protect Americans’ sensitive and critical information.

**2. Procedures for and results of data-driven and scientific validation of biometric technologies:** Information about planned or in-use validation procedures and resulting validation outcomes for biometric technologies designed to ensure that the system outcomes are scientifically valid, including specific measures of validity and accuracy, resulting error rates, and descriptions of the specific measurement setup and data used for validation. Information on user experience research, impact assessment, or other evaluation of the efficacy of biometric technologies when deployed in a specific societal context is also welcome.

As part of OSTP’s ongoing research on the validation of biometric technologies, special consideration should be made to review the work of Dr. Anil Jain and his research on relevant sample sizes and processes for authentication. Dr. Maruf Monwar and Marina Gavirlova have also produced research on multimodal biometric systems.
To gain greater expertise, we suggest the National Center for Biotechnology Information at the NIH as a valuable resource on the topic. NIST also has several resources, including a summary of a workshop conducted in 2015 to improve datasets standards for use in biometrics.

3. **Security considerations associated with a particular biometric technology.** Information about validation of the security of a biometric technology, or known vulnerabilities (such as spoofing or access breaches). Information on exhibited or potential leaks of personally identifying information via the exploitation of the biometric technology, its vulnerabilities, or changes to the context in which it is used. Information on security safeguards that have been proven to be efficacious for stakeholders including industry, researchers, end users, and impacted communities.

Federal legal requirements outlined in the Health Insurance Portability and Accountability Act (HIPAA) and Family Educational Rights and Privacy Act (FERPA) under which individuals’ biometric information is broadly protected, help to protect individuals’ information. HIPAA applies safeguards for patients’ sensitive health information and require covered entities to notify individuals in the event of a breach of personal health information, including biometric identifiers. FERPA similarly requires parental consent before a student’s biometric records can be released.

Federal agencies are uniquely required to abide by the Privacy Act of 1974, also known as the “Code of Fair Information Practices,” which intends to “balance the government’s need to maintain information about individuals with the right of individuals to be protected against unwarranted invasion of their privacy and to limit the unnecessary collection of information about individuals.” This is essential in address privacy violations, such as the cybersecurity incident during a 2019 biometric pilot program by CBP where thousands of traveler’s Personally Identifiable Information (PII) was was improperly used.

Some state and local city regulations and corporate policies have added much needed layers of protection against security risks and privacy concerns of biometric technology. Stakeholders' sensitive information or personally identifying information is safeguarded under these laws, and incidences such as data breaches are more likely to be reported and responded to appropriately.

The Illinois Biometric Information Privacy Act (BIPA) is an example of a local state law that aims to protect individuals from potential exploitations or misuse of their biometric information. BIPA requires employers to publish their intended use of biometric information, and how it will be collected and stored and receive written consent from their employees in the state to use and collect biometric information. The law also has guidelines for permanently deleting and destroying data that is no longer in use to protect individuals from potential future data breaches. Further, the law requires businesses to provide notice in the case of a data breach. While this is
not customary, it is vital to ensure people are informed about the security of their biometric identifiers. While law intends to benefit citizens, the cost of implementing BIPA technology standards and the repercussions for non-compliance drives businesses outside of Illinois’ state lines, which could ensue costs on the economy and people’s welfare.

Some systems implement their own security measures such as only storing the data on the device, and never capturing that data outside of the device's operating system.

4. **Exhibited and potential harms of a particular biometric technology:** Consider harms including but not limited to: Harms due to questions about the validity of the science used in the system to generate the biometric data or due to questions about the inference process; harms due to disparities in effectiveness of the system for different demographic groups; harms due to limiting access to equal opportunity, as a pretext for selective profiling, or as a form of harassment; harms due to the technology being built for use in a specific context and then deployed in another context or used contrary to product specifications; or harms due to a lack of privacy and the surveillance infrastructure associated with the use of the system. Information on evidence of harm (in the case of an exhibited harm) or projections, research, or relevant historical evidence (in the case of potential harms) is also welcome.

The negative impacts caused by leaked, stolen, or misused biometric information are far greater than harms caused by the same misuses of other data. Biometric data is unique and cannot be altered in the case of a data breach. High-stakes biometric information must be treated differently than other data, and Congress should make policy decisions particularly to protect users from harms. We’ve identified some of the harms caused by biometric capturing technology below. However, our response summarizes only the most serious harms we have found, and we recommend OSTP consider all harms identified by respondents to this RFI.

Data that is captured by biometric devices and systems are then processed and analyzed using AI or machine learning. The validity of information generated by AI or machine learning systems can be questioned due to cognitive biases from the AI developers that can influence the models and training data sets. This can lead to bias being hardcoded into the algorithm. We applaud NIST’s recent work to provide a framework to address bias and fairness issues, but more work is necessary to specifically address bias in biometric data-enabled technology.

Disparities in effectiveness of the system negatively affect minority stakeholders. Facial recognition systems can fail when encountering individuals with dark skin, causing harm such as false identifications, bias in algorithms, or bias in error rates. Harms can also be caused by a lack of transparency about the use of biometric data. This can happen when consent is granted for use of biometrics for
identification or access; that data is then used in addition or instead for surveillance or tracking of an individual. Other transparency concerns arise when consent is not deliberately granted, for example, when social media platforms use facial recognition technology to identify and make public identification of people in the backgrounds of pictures.

Unfortunately, Americans have also already encountered malicious actors; Russian-owned FaceApp used deceptive terms of service agreements – an application that encouraged users to upload photos of themselves so the app could manipulate an image to make the subject look older. People raised privacy concerns as they discovered the images were uploading to servers where AI algorithms ran against them. Users gave away control or rights over their images, and therefore their biometric information.

5. Exhibited and potential benefits of a particular biometric technology: Consider benefits including, but not limited to: Benefits arising from use in a specific domain (absolute benefit); benefits arising from using a specific modality of biometric technology (or combination thereof) compared to other modalities in a specific domain (relative benefit); and/or benefits arising from cost, consistency, and reliability improvements. Information on evidence of benefit (in the case of an exhibited benefit) or projections, research or relevant historical evidence (in the case of potential benefit) is also welcome.

There are many advantages to deploying biometric devices, such as increased security and privacy and greater efficiency for validation purposes. Voice recognition tools are also adapting to help decipher demands for speech command systems to improve user experiences.

The use of biometric systems in airports has helped to reduce the time it takes for passengers to get checked in. For example, TSA Precheck collects biometric data upon enrollment for background checks. However, biometrics are not regularly thereafter confirmed by members when encountering TSA security at airports. In addition, the U.S. Customs and Border Protection agency uses the Global Entry systems to allow expedited clearance for pre-approved, low-risk travelers upon arrival in the United States. Global Entry is a voluntary program that uses facial recognition and fingerprint data for identification and authentication. In exchange, travelers gain access to an expedited screening process when entering the United States. The TSA and CBP are also testing the use of facial recognition for a joint CBP/TSA Trusted Traveler pilot program.

Companies have deployed biometric time clocks to track employees' hours using a unique biometric identifier such as a fingerprint to allow employees to clock in and out more efficiently. These systems also cut down on employees entering fraudulent time worked information and free the employers from manually tracking and verifying employees' attendance. The use of biometric verification also prohibits coworkers from clocking in or out someone other than themselves.
6. Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case:

After assessing five state privacy laws pertaining to the collection and use of biometric information in Illinois, Texas, Washington, California, and New York, BPC created a white paper to understand sensitive information is collected, used, safeguarded, destroyed, and regulated in each state. We encourage OSTP to consider the benefits as well as the shortcomings of these five state laws when shaping future regulations and recommendations on biometric information. In each of the subsections of this response, we will report findings from this analysis and the application of these practices for different stakeholders.

Information regarding:

a. Stakeholder engagement practices for systems design, procurement, ethical deliberations, approval of use, human or civil rights frameworks, assessments, or strategies, to mitigate the potential harm or risk of biometric technologies;

Some states, including the five mentioned above, have introduced or passed legislation to protect people's biometric data, and many businesses have adopted their own policies to comply. The intention of each policy is to mitigate the risks of biometric technologies on consumers and other stakeholders. As some of the first laws to regulate biometric information in the United States, these laws have great influence over business practices and consumer awareness of the handling of biometric information. Using the infographic made public here on BPC's website, stakeholders can better assess requirements and how they overlap or differ from state to state.

Making this information more accessible will allow stakeholders to comply with laws and regulations more easily across the country. It will also improve informed consent of the use of biometric technologies, give consumers access to information about their rights, and facilitate the appropriate use of biometric technology.

b. Best practices or insights regarding the design and execution of pilots or trials to inform further policy developments;

The lack of federal guidance on policies surrounding issues raised in this RFI has left citizens inadequately protected, and corporations forced to navigate state-by-state regulations. As referenced in our papers, a good first step may be establishing a biometric data privacy framework using the NIST Privacy Framework as a guide to building standards.

c. Practices regarding data collection (including disclosure and consent), review, management (including data security and sharing), storage (including timeframes for holding data), and monitoring practices;
The five laws we reviewed reveal distinct practices regarding biometric data collection, use, and storage. Four of the five states require businesses or other entities to inform people of the use of biometric identifying technology. Two states even require affirmative consent prior to the collection, storage, or use of someone's biometric information. This informed use is important so consumers can make informed decisions about their sensitive data.

Despite varied practices regarding data collection, all five states oblige businesses or people to destroy or delete biometric data within a certain time frame. Restricting the retention of sensitive data limits its vulnerability to data breaches and other misuses.

**d. Safeguards or limitations regarding approved use (including policy and technical safeguards), and mechanisms for preventing unapproved use;**

These state laws have implemented safeguards for unapproved use beyond requirements to delete or destroy data. All five laws we reviewed require entities capturing biometric information to protect biometric information in a more protective manner than other, less sensitive data.

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

In general, transparency of information is essential to further inform individuals' decisions regarding the utilization of biometric technology. In some instances, entities collecting biometric information are required by law to notify users in case of a data breach, sometimes requiring the details of the data that was breached. Some state laws we reviewed also allow a private right of action so people harmed by violations of the law have an opportunity to collect for their damages. Damages may result in anywhere from $100 to $25,000.

**Conclusion**

OSTP will play a vital role in defining the future of AI-enabled biometric technologies. BPC's response to the RFI provides recommendations developed from collaboration with industry, academia, government, and civil society on these topics and should be considered in combination with the other responses that have been submitted. We strongly recommend that policy considerations constantly be reviewed and modernized as the technology continues to develop. BPC looks forward to continued work with OSTP to collaborate on these concepts.