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.
January 15, 2022

Dr. Eric S. Lander  
Director  
Office of Science & Technology Policy  
Executive Office of the President  
Eisenhower Executive Office Building  
1650 Pennsylvania Avenue, NW  
Washington, D.C. 20504

RE: RFI Response: Biometric Technologies

Dr. Lander,

We at CLEAR are grateful to the Office of Science and Technology Policy (OSTP) for initiating this important conversation around biometric technology, and appreciate the opportunity to share our unique perspective based on our decade of experience using biometrics to create safe and easy experiences for our members.

Our extensive work with this technology drives our firm belief that biometrics are best utilized by private-sector companies on an opt-in basis. Empowering individuals to choose whether or not to utilize biometric technologies is the best way to build trust with individuals and communities, and to ensure these solutions are developed in a responsible, equitable, and reliable way. Every solution powered by CLEAR is fully opt-in, and designed to maintain the trust that we have built with our members and users. As a user, you provide the biometrics we use, and you always know when you're interacting with our services.

While we will speak broadly below about our perspective using opt-in biometrics to power frictionless experiences for our members, we intend to be primarily responsive to the following topics from the RFI:

1. Descriptions of use of biometric information for recognition and inference
6. Governance programs, practices or procedures applicable to the context, scope, and data use of a specific use case
I. Introduction

CLEAR Secure, Inc. is a secure biometric identity company, whose mission is to enable frictionless and safe experiences. With more than 8 million members and 130+ partners, CLEAR's identity platform connects you to all the things that make you, you - transforming the way people live, work and travel.

We believe that when users are in control and empowered to choose to use biometric technology, these solutions can provide safer and easier experiences that protect and improve personal privacy while removing friction from everyday life.

Demand for convenience has grown while tolerance for friction has all but disappeared – creating the need for innovative experiences that are easy for consumers. According to a survey by Whyline Inc. - a CLEAR company - 64% of people would rather abandon certain experiences than wait for them, while another survey from Talkdesk Research reports that 68% of customers state that a single negative customer service experience will reduce their loyalty to a brand. This new convenience economy has made us feel like anything and everything is just a click away, while reducing our tolerance for friction in everyday experiences.

COVID-19 has been a great accelerator of this trend, and there has never been a more critical time for both physical and digital experiences to embrace innovation. According to a July study by Deloitte and the National Retail Federation, 78% of consumers value convenience more now than before COVID-19. And a McKinsey survey of executives in fall 2020 found 63% of companies have had to change to meet shifting customer expectations due to the pandemic, and of those, 62% say they expect those changes to become permanent.

In the wake of the pandemic and our heightened awareness around public health, the new customer expectation will be experiences that are safe, but also frictionless. People will demand solutions that help them cut down on crowds, waiting shoulder-to-shoulder in lines, needlessly touching high-traffic surfaces, and constantly having to hand over the cards in their wallet to prove who they are. They want personalized experiences that value their time and their business, and help them get the most out of their day.

Biometric technologies can help to drive this evolution in experiences, but the foundation has to be built on trust. Americans must be able to trust that they will stay in control of their personal information, trust that their information is being kept secure, and trust that everyone who interacts with a technology solution is being treated equitably. A critical building block of that trust is empowering users to choose whether to engage with such novel and evolving technology. People are more apt to trust technology solutions they view as voluntary, inclusive, and...
transparent. People are more apt to trust technology solutions they view as voluntary, inclusive, and transparent. At CLEAR, building and maintaining trust has been at the heart of everything we do, which is why our solutions are always opt-in.

II. Creating Safe And Frictionless Experiences

CLEAR got our start in a place where trust is paramount, and friction is high - the airport. For over 10 years, we have been partners with the Transportation Security Administration (TSA) and the Department of Homeland Security (DHS) as part of the Registered Traveler program (RT). In the wake of 9/11 and the creation of TSA, the RT program was established as a public-private partnership to leverage private-sector innovation to help maximize security and minimize stress for travelers. With the oversight of our government partners, we use biometrics to create a more frictionless experience at the security checkpoint for travelers, while meeting the highest security standards.

Today, CLEAR’s opt-in travel subscription service, CLEAR+, has 115 lanes located in 40 of the largest and busiest airports across the country. Our members utilize iris or fingerprint scans to quickly verify their identity and move on to physical security screening. We have successfully used biometrics to verify identity and direct passengers to appropriate physical screening over 50 million times since 2010. We have a Net Promoter Score (NPS) of 77 providing world class service to our members, while at the same time maintaining the highest government standards for security.

In establishing and implementing the RT program, Congress and the TSA recognized how biometric technology could be leveraged to improve security and act as a force multiplier for the TSA’s frontline officers. As the TSA stated in codifying the RT program, the goal of establishing such trusted traveler programs was to “use available technologies to expedite security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening.”

And as TSA looks towards the future of the security checkpoint, they have continued to emphasize the potential of biometrics technology. In laying out their 2019 Biometrics Roadmap, the TSA recognized the opportunity to develop “a biometrics capability, built with strategic partners, that enhances aviation security, streamlines operations, and simplifies the user experience.”

Greater use of biometrics will also help the TSA meet the objectives of President Biden’s recent “Executive Order on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government.” As Secretary of Homeland
Security Alejandro Mayorkas stated, under the President’s EO the TSA will “test the use of innovative technologies at airport security checkpoints to reduce passenger wait times.”

As one of the TSA’s strategic partners, CLEAR looks forward to building the future checkpoint and improving the customer experience together.

As opt-in solutions such as CLEAR have been adopted at airports across the country, travelers have grown more comfortable with the use of biometrics in air travel. According to the International Air Transport Association’s (IATA) 2021 Global Passenger Survey, 73% of global passengers are comfortable using their biometrics to improve their airport experience. In another poll conducted by the Security Industry Association (SIA), 69% of U.S. adults are comfortable with the use of biometrics at airport security, and 75% are comfortable with its use by airlines.

These trends further demonstrate that when new technology solutions allow users to choose whether to engage with them, building a foundation of trust and security, Americans can grow comfortable with their use and enjoy the frictionless journeys they can create.

Building A Frictionless World

While we got our start at airport security, CLEAR’s mission has always been to create safer and easier experiences throughout your day. Being a secure identity company has always been about using biometrics to allow you to link your identity with your boarding pass at the airport, your rental car account, your ticket to the game, or your credit card and proof of age to buy a beer at the concession stand.

Amid the pandemic, we recognized that there was going to be a new source of friction as businesses and venues began to reopen, and a need to create safer experiences for everyone. We developed Health Pass to allow CLEAR users to confirm they meet COVID-related requirements for entry set by CLEAR’s partners – such as proof of vaccination, negative test results, or health survey answers – just by showing the partner a green or red signal without needing to share detailed health information. We also make it safe and easy for anyone to create a free digital vaccine card that you can carry right on your phone and use wherever you need. Once again, secure opt-in identity could be used to remove friction and improve privacy while making experiences safer for everyone.

As we all grapple with evolving vaccine requirements and the complexity of operating amid COVID-19, CLEAR has been partnering with businesses across the nation to help make coming back – and staying back – easier. More than 130 organizations including major professional sports teams, corporate offices, small
businesses, travel destinations, and restaurants have used CLEAR to help keep their doors open, their workers on the job, and their customers safe.

CLEAR's vision is to empower members to use their verified identity to move frictionlessly through a network of different experiences. You are you, and you shouldn’t be constantly having to hand over the cards in your wallet, or share more information than necessary, to prove who you are. But in order to do this, we know our first priority is to maintain the reputation for trust we’ve spent a decade building. That is why everything that CLEAR does is built on our commitment to the privacy of our members.

III. Our Commitment to Privacy

You are you, and your personal information is yours. As a secure identity company, we firmly believe in keeping users in control of their information. That is why we will never sell or rent personal information, and every solution CLEAR provides is entirely opt-in. We have spent a decade building a brand that stands for trust, and know that our first duty is always to our members.

We believe that our members and users should always know why CLEAR is asking for their information and how it is being used. The only time a member’s personal information is shared with one of our partners is when the member affirmatively consents to the sharing of that information.

We will also honor any request to delete a member’s personal information from our databases, since you don’t truly control your information unless you have the right to have it deleted by any service you no longer wish to utilize. CLEAR has committed to members’ Right to be Forgotten nationally since 2010, well before statutes such as CCPA made it mandatory in California.

Additionally, when a member trusts us with their information, it is protected by CLEAR’s comprehensive security program that meets the highest government standards for data protection and privacy.

Leading With Transparency

We believe in transparency in everything we do, which is why our Privacy Policy is written in a simple, straight-forward manner that clearly provides members with a guide to what information we collect, how it is used, and how our members maintain control.

When members enroll in our CLEAR+ subscription service, they provide CLEAR with biographic, biometric, contact, and payment information, as well as an image of a
government-issued identification. In the course of enrollment, members affirmatively opt-in and agree to CLEAR's Member Terms. As we have begun offering additional services that require lower levels of identity assurance, members are prompted to provide only the information necessary to power their chosen experience.

Once enrolled, our CLEAR kiosks in airports use iris and fingerprint scans, in line with TSA guidelines, to verify members' identities, while our smartphone-based app uses selfies and facial recognition technology. Smartphone users have the option to securely link their identity to verified credentials. For example, Health Pass users can securely link their verified identity to their proof of vaccination or negative COVID-19 test results. All of CLEAR's solutions are fully opt-in and linking information is at the member’s discretion.

The information we obtain about our members is used to administer CLEAR's experiences, such as managing the enrollment process, verifying members' identities, and providing better experiences for our members. We do not and will never sell user information. And our robust privacy policy ensures that member data is not shared with any third party inappropriately. Service providers retained by CLEAR are limited, and are contractually prohibited from using or disclosing any member information they access other than to perform services on behalf of CLEAR and our members.

IV. Using Biometrics To Empower

We understand that biometrics such as facial recognition, iris scans, and fingerprints are especially sensitive data, and that some products powered by this technology raise concerns about the potential for bias or abuse. As OSTP initiates this important conversation around biometric technology, it is crucial to distinguish opt-in solutions that empower users to access more frictionless experiences, while maintaining control of their information, from those that collect biometric information without a person's consent.

Unlike many of the facial recognition applications that have recently received notoriety, all of CLEAR's solutions rely on user-provided images and biometrics, and we do not capture images of non-users. We do not conduct passive monitoring, surveillance, or scanning of crowds, and our members and users always know when they are interacting with our services. We are comparing a user-provided photo against a government-issued ID that the users themselves have chosen to provide us, and we are empowering members to use their biometrics to confirm their identity.
Addressing Bias

As part of our commitment to building solutions that empower our members and users, we take the issue of bias very seriously and we proactively work to mitigate any racial and gender differentials in the algorithms that power our solutions.

All CLEAR members opt-in and provide their own images — and our processes are designed to ensure that a high-quality image is captured. Relying on high-quality, user-provided images as CLEAR does helps to significantly mitigate the risk of racial disparities in facial recognition, which depend greatly on the quality of the photo. Since all CLEAR members have opted in to our service, we can obtain higher quality photos for comparison since each member is aware their photo is being taken during the enrollment and verification process.

We are also not using biometrics to make demographic determinations such as gender, ethnicity, or age. Our only goal is to match identity based on your opt-in enrollment information.

V. Keeping Information Secure

A final element in building biometric solutions on a foundation of trust is that users must know that when they entrust personal information to a company, that company will act responsibly to protect their data, and keep it secure and confidential. CLEAR has implemented a comprehensive information security program that meets the highest government standards of data protection and privacy.

Our security program includes administrative, technical, and physical safeguards to protect against threats to the security, confidentiality, or integrity of our members’ personal data. The tools we use to protect our members’ data include, but are not limited to:

- Data encryption in transit and at rest
- Firewalls
- Multi-factor authentication
- Access-control procedures
- Personnel security controls
- Comprehensive privacy and security training for all team members
- Physical and environmental security procedures
- Intrusion detection and data leakage tools

CLEAR’s commitment to guarding our users’ data is reflected in meeting the highest industry standards for data protection and privacy:

- TSA designated CLEAR’s biometric identity platform at FISMA-High – the
highest government cyber compliance rating available for protecting sensitive data.
- TSA regularly conducts audits and inspections of CLEAR's technology infrastructure.
- CLEAR's biometric enrollment and verification platform have been SAFETY Act Certified as a Qualified Anti-Terrorism Technology by the Department of Homeland Security (DHS).
- CLEAR is compliant with the Payment Card Industry Data Security Standard, an information security standard for organizations that handle credit card information.
- CLEAR's security program was implemented in accordance with the National Institute of Standards and Technology's (NIST) security control framework.

VI. Conclusion

We would like to once again thank your office for initiating this important conversation and soliciting input from companies like CLEAR. Solutions powered by biometrics offer a remarkable technological evolution with a wide range of applications, but we believe are best utilized on an opt-in basis that empowers individuals and builds trust.

Secure identity can enable frictionless experiences, meeting consumers' new expectations for solutions that are safe and easy. And Americans are ready to embrace these solutions, provided they can trust that they will maintain control of their personal information, and that the companies they entrust with their information will keep it secure. Furthermore, Americans expect providers to build and administer these technologies responsibly and equitably. Everything CLEAR does keeps this duty front of mind.

While we know you will be hearing from a range of perspectives, from the private sector, government agencies, advocacy groups, and the public, we hope this will be only the beginning of the conversation. We hope CLEAR can continue to be a resource for you as you examine the promise and responsible use of this technology.