Federal Register Notice 86 FR 56300, https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies, January 15, 2022.

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.

RFI Response: Biometric Technologies

Respondents:

- Kavya Pearlman - Founder and CEO XR Safety Initiative, XR Safety Initiative (XRSI)
- Marco Magnano - Cofounder and Executive Director of Communications, XR Safety Initiative (XRSI)
- Rachel Michelon - Medical XR Advisory Council Lead, XR Safety Initiative (XRSI)
- Ryan Cameron - Medical XR Adviser and Co-chair Medical XR Privacy & Safety Framework, XR Safety Initiative (XRSI)

Respondent Type: Non-Profit Research Organization registered in California, USA

About XR Safety Initiative (XRSI)

XR Safety Initiative (XRSI) is a 501(c)(3) worldwide not-for-profit Standards Developing Organization(SDO) that promotes privacy, security, and ethics in immersive environments. XRSI's mission is to help build safe and inclusive experiences so that XR stakeholders can make informed and pragmatic decisions. XRSI does this by discovering novel cybersecurity, privacy, and ethical risks and proposing potential new solutions to mitigate them. XRSI, being the first such global effort, is uniquely positioned to provide impartial, practical information about XR and Spatial Computing-related risks and opportunities to individuals, corporations, universities, government agencies, and other organizations worldwide. XRSI launched the first novel XRSI Privacy Framework for the XR and SpatialComputing domain to address the impact of Biometric Inferences via Special Data Type consideration. The framework has been well received and has been a point of discussion among XR stakeholders and many regulatory entities worldwide.

SUMMARY

Even though XRSI specifically focuses on Immersive Technologies and Metaverse-related use cases, we have discovered that Biometric Inferences impact most of the technology landscape and, in turn, humans. With the significant focus on the Metaverse globally, amplified by the pandemic, the use of Immersive Technologies such as XR[1] and its intersections that utilize Biometric data and inferences must not be ignored. If anything, XR use cases are the perfect testing ground for classifying and handling the potential risks and opportunities stemming from Biometric inferences.

The domains in which these technologies are being used: XR and Metaverse related Technologies and their intersections, e.g., Artificial Intelligence, Robotics, Decentralized Ledger Technologies, Brain-Computer Interfaces, etc.

The entities making use of them: Big tech companies like Meta, Microsoft, Google, Niantic, Snap, Netflix, Amazon, Neuralink, and a large number of Metaverse-focused organizations.

Current principles, practices, or policies governing their use are lacking when it comes to inferences. From a policy perspective, most companies can only address Biometric Data per state laws or European specific General Data Protection Regulation (GDPR) within the context of Privacy laws. None of the laws, including GDPR, currently address inferences and their impact. XRSI analyzed these laws within the United States and found no mention, indication, or guidance on the inferences application or use.

[1] Extended Reality (XR) is a fusion of all the realities – including Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR) – which consists of technology-mediated experiences enabled via a wide spectrum of hardware and software, including sensory interfaces, applications, and infrastructures. Source: https://xrsi.org/definition/extended-reality-xr

Topic 1. Descriptions of use of biometric information for recognition and inference

Information about planned, developed, or deployed uses of biometric data, 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.

XR Safety Initiative (XRSI) is serving as a subcontractor to Cyber Bytes Foundation (CBF) to create natural authentication methods for First Responders using Augmented Reality (AR) Systems in the context of a NIST Grant award. XR technologies can be valuable tools to Public Safety Organizations (PSOs) in doing their jobs and accomplishing their missions.

First Responders often have to utilize multiple disconnected databases in the line of duty to gain critical information such as juvenile status or identification verification.

AR can provide a means to have this information directly in the line of sight, but the AR device must be authenticated due to the sensitive nature of the data it would be displaying. This prevents equipment and sensitive data from falling into the wrong hands in often chaotic situations.

The issue is further amplified when PSOs operate in limited settings such as unreliable network coverage, sensitive situations like an active shooter, etc.

By using Biometric Inferences (Natural Authentication) to reduce or eliminate cognitive load during authentication to the AR device at hand, first responders can remain focused on their duty.

The research work focuses on identifying PSOs' requirements such as form factor, usability, and other pertinent factors to identify and validate authentication methods as probable.

These methods are tested and validated further to develop secure and safe authentication methods through actual PSOs participation.

During the research, companies are identified as using AR, and existing authentication methods that authenticate users to AR devices are identified. Existing AR devices and sensors that provide Biometric Inferences are also identified.

Topic 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 in 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.

The work from previously mentioned natural authentication methods for First Responders using Augmented Reality (AR) Systems via NIST Grant award[2] is planned to include prototype development that records several biometric data streams to train a Machine Learning algorithm and then the result will be used to identify the subject in an appropriate context. These biometric data streams could be used by themselves or in combination with others and would consist of data such as voice audio samples, EKG, EEG, body movement patterns, gaze patterns, galvanic skin response, bio capacitance, and any others we can include within the scope of the project. As first responders are authenticated, cognitive load, as well as other attention metrics, will be measured and compared to a baseline so it can be determined whether the method truly is Natural Authentication. The end goal is to ensure that the device is authenticated as close to real-time as possible without impacting the awareness of the subject, as well as being resilient against environments and challenges faced by first responders in the line of duty.

Topic No. 3. Security considerations associated with a particular biometric technology.

Information about validation of the security of 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.

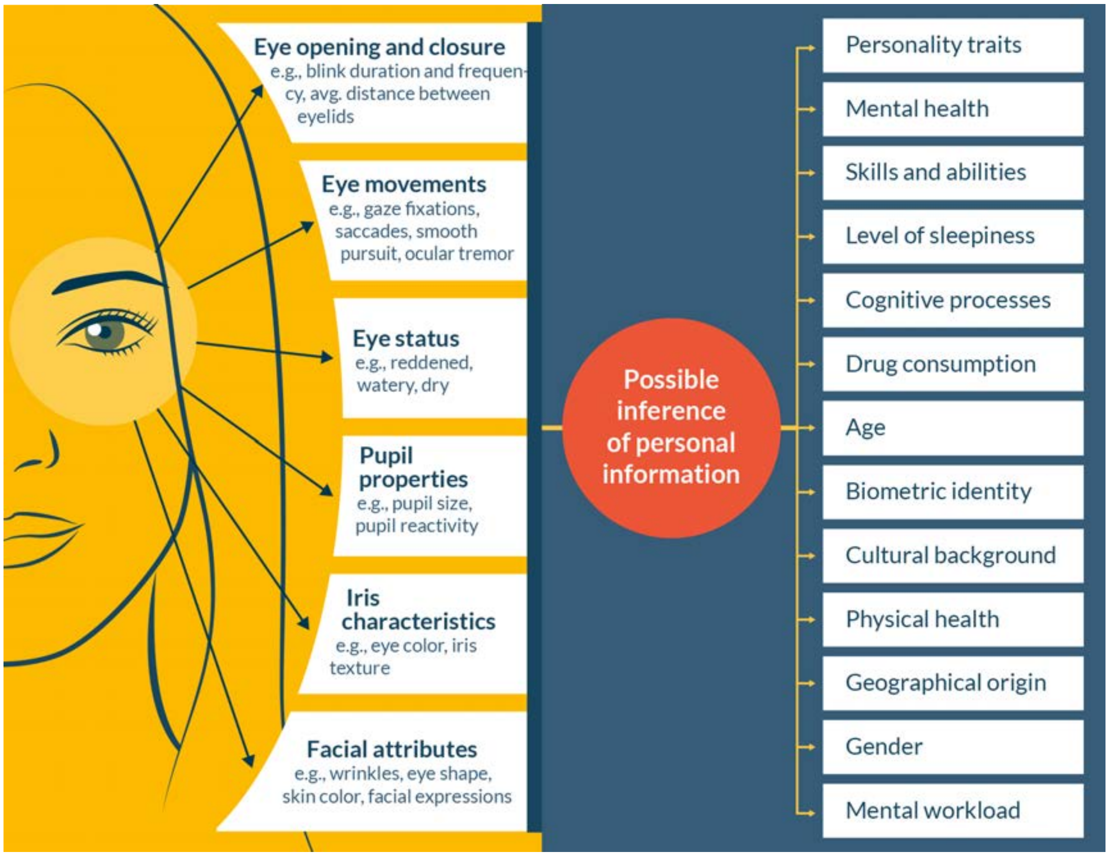
[2] Natural Authentication methods for First Responders using Augmented Reality (AR) SystemsNIST Grant Award
https://xrsi.org/cyber-bytes-foundation-and-xrsi-announce-grant-award-to-create-natural-authentication-methods-for-first-responders-using-augmented-reality-systems

XRSI has developed a Privacy and Safety Framework for XR and Spatial Computing Domain[3] specifically focusing on Biometric Inferences. Many organizations are developing immersive technologies to build all-day wearable glasses that are spatially aware with the goal of delivering AR and VR experiences more immersive and integrated into the physical world serving as the baseline for the Metaverse. In order to achieve this outcome via the use of AI algorithms, a large amount of data collection is necessary. The concerns for excessive data collection are heightened because of a large amount of real-time data collection and the potential inferences that are possibly made. While some inferences are necessary and even welcomed by individuals such as curated and customized shopping preferences many others such as Biometrically-Inferred Data (BID) are not and may cause harm to humans.

Biometrically-Inferred Data (BID)[4] is a collection of datasets resulting from information inferred from behavioral, physical, and psychological biometric identification techniques, and other nonverbal communication methods. For example, XR devices can lead to inferences such as biometric and gender identity, mental workload, mental health status, cognitive abilities, religious and cultural background, physical health, geographic origin, and many other skills, abilities, personality traits, and more. Based in different jurisdictions, organizations may be mandated to protect BID and require adopting a data governance framework like XRSI's. This will prevent excessive and unwarranted data collection at the hardware, operating system, API, and software levels, leading to responsible research and innovation in the XR domain. Below are a few examples of the data tracked and collected by and for XR devices.

[3] XRSI Privacy and Safety Framework for XR and SPatial Computing Domain http://www.xrsi.org/psf11

[4] Biometrically Inferred Data https://xrsi.org/definition/biometrically-inferred-data-bid


Eye opening and closure
e.g., blink duration and frequency, avg. distance between eyelids
Eye movements
e.g., gaze fixations, saccades, smooth pursuit, ocular tremor
Eye status
e.g., reddened, watery, dry
Pupil properties
e.g., pupil size, pupil reactivity
Iris characteristics
e.g., eye color, iris texture
Facial attributes
e.g., wrinkles, eye shape, skin color, facial expressions
Possible inference of personal information
Personality traits
Mental health
Skills and abilities
Level of sleepiness
Cognitive processes
Drug consumption
Age
Biometric identity
Cultural background
Physical health
Geographical origin
Gender
Mental workload

The emergence of the Metaverse has led to the convergence of various technologies such as XR, Brain-Computer Interfaces (BCI), Artificial Intelligence (AI), etc. The citizens must be protected from these technologies that are capable of mind control, mind-reading, or any other nefarious interference with human brains. While such concerns used to be relegated to conspiracy-theory chat rooms and science fiction, now they're subject to debate by senators.

At the end of 2021, in fact, a constitutional amendment was passed by the National Congress of Chile and signed by the president, the people of Chile as the first in the world to be granted a new kind of human rights—“neuro-rights”—which are made necessary to protect human agency and autonomy from advances in neurotechnology and the convergences leading up to the Metaverse.

XR Safety Initiative (XRSI) has been investigating these rights and the way to facilitate them via their Medical XR-focused Privacy and Safety Framework. These conversations need to happen at a global regulatory level and more efforts are needed to ensure we do not lose human agency and autonomy as we move fast toward and our dependence on Metaverse focused technologies grows. BID provides a legal foundation to classify and protect health inferences as well facilitate neuro rights policy directives to be discussed at the regulatory level. XRSI conducted additional research (resulting in the Securing the Metaverse Research Paper) and presented it at the Simulation Interoperability Standards Organization - SISO Symposium in 2021.[5]

Topic 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.

XR in healthcare presents unique opportunities for patient harm that otherwise did not exist. When a person is fully immersed in a new reality, simple things like ensuring there is a visual representation of a floor, a horizon, or lighting that we often take for granted can really cause serious harm to a patient if not implemented properly. People can stumble, walk into windows or off a balcony, injure their head if the environment is poorly designed. On top of that, VR can introduce psychological trauma because it is just so immersive. This is seen in experiments carried out at various universities where VR has been shown to be so immersive, it can replace pain medication for pregnant patients, or enhance and replace cognitive behavioral therapy that traditionally utilizes psychedelic drugs. In terms of biometrics, VR cameras that display for the user can be moved/angled by software to accommodate vision alignment issues, but bad actors could use this to cause severe eye strain or double/blurred vision to injure subjects.

Given these unique harms, it is simply critical that regulatory oversight that is steeped in research is applied not only in the medical device space but wherever XR is utilized for any purpose. This regulatory oversight needs to address these unique concerns and XRSI Medical Privacy and Safety Framework[6] is being developed to address these issues. See medical.xrsi.org for more information.

[5] Securitng the Metaverse Research by https://www.sisostds.org/DesktopModules/Bring2mind/DMX/API/Entries/Download?Command=Core_Download&EntryId=52969&PortalId=0&TabId=105

[6] XRSI Medical Privacy and Safety Framework https://medical.xrsi.org/

Cyber XR Coalition for advocacy and rights : The mission is to actively address social and technical biases in emerging technologies that foster a sense of belonging while helping to ensure a safe experience for all. The coalition advocates to address the impact resulting from the misuse of biometric inferences and from algorithmic biases potentially undermining the human rights of minorities and others. The coalition uses this knowledge to inform global standards for Accessibility, Ethics, Inclusion, and Safety for immersive technologies. CyberXR advocates the use of technologies to create an equitable future with the benefits of scientifically valid technologies with appropriate contexts and proposes global standards to implement safeguards against anticipated and unanticipated misuse or harm.

Topic 6. Governance programs, practices, or procedures applicable to the context, scope, and data use of a specific use case

With the newly-emerged focus on the Metaverse, which is going to be the confluence of various technologies such as XR, AI, BCI, Robotics and more it is imperative to extend data protection beyond just PII (Personally Identifiable Information or Personal Data and understand the context for putting better safeguards in place. XRSI commenced its mission in early 2019 and immediately started researching and investigating these matters via the XR Data Classification Public Working Group.[7]

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;
XRSI began conducting a series of closed roundtables last year. The goal of the roundtables is to connect stakeholders, technologists, and human rights experts in a dialogue sharing their insights, research, data, experiences, and concerns to address the implications of enormous amounts of data being collected and shared in the immersive ecosystems. Through the multidisciplinary roundtables XRSI is able to collaboratively map the classification contexts and schemes that enable and drive the adoption of various augmented reality (AR) and virtual reality (VR) technologies.

b. Best practices or insights regarding the design and execution of pilots or trials to inform further policy developments;
The magnitude and scale of XR data make it challenging to categorize in a simplified manner. Regardless, an attempt must be made to look through and analyze such a large amount of data with a filter of Information Security, privacy and safety principles.

[7] XR Data Classification Public Working Group https://dc.xrsi.org/working-group/

Since XR has the potential to record all new kinds of user information (from eye movements and emotions to the movement of a user's entire body through space), ensuring that this data is managed in a responsible way has become paramount for virtual XR researchers and commercial entities alike.
XRSI's Medical XR Advisory Council is currently studying various use cases and as preliminary research to discover potential areas of concern for patient harm and privacy violation unique to XR.

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 development of Data Classification guidance, common vocabularies, and Data sets will certainly contribute to the understanding of potential risks associated with XR data.

d. Safeguards or limitations regarding approved use (including policy and technical safeguards), and mechanisms for preventing unapproved use;
The outcome and framework from the data classification will serve as the foundation to further build safeguards for the immersive technology domain via XRSI Privacy and Safety Frameworks

e. Performance auditing and post-deployment impact assessment (including benefits relative to current benchmarks and harms);
Planned for further development of XRSI Privacy and Safety Framework version 2.0

f. Practices regarding the use of biometric technologies in conjunction with other surveillance technologies (e.g., via record linkage);
Planned for further development of XRSI Privacy and Safety Framework version 2.0

g. Practices or precedents for the admissibility in court of biometric information generated or augmented by AI systems;
Currently in development via XR Data Classification Public Working Group

h. Practices for public transparency regarding: Use (including notice of use), impacts, opportunities for contestation and for redress, as appropriate.
Planned for further development of XRSI Privacy and Safety Framework version 2.0