epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER to

EUROPEAN COMMISSION

Virtual Worlds (Metaverses) – A Vision for Openness, Safety and Respect

May 3, 2023

By notices published April 5, 2023, the European Commission (Commission) has solicited input to inform the Commission's vision for, and any potential guidance or regulations related to, emerging virtual worlds (also referred to as metaverses or the metaverse).[1] The desired input should aid the Commission in honing its vision for virtual worlds, addressing opportunities and societal challenges, and drafting future implementation measures.

Pursuant to the European Commission's request for comments, the Electronic Privacy Information Center (EPIC) submits these comments to aid the Commission in 1) identifying privacy risks within the metaverse, 2) examining current legal challenges to virtual worlds, and 3) putting forth proposals to mitigate privacy risks.

I. Introduction

EPIC is a public interest research center established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC is a leading advocate for privacy and privacy-enhancing techniques for emerging technology,

[1] European Commission Public Initiative: Virtual Worlds (metaverses) – A Vision for Openness, Safety and Respect (Apr. 5, 2023), available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13757-Virtual-worlds-metaverses-a-vision-for-openness-safety-and-respect_en.
[2] EPIC, *About Us* (2023), https://epic.org/about/.

with a particular interest in identifying privacy and civil liberties risks and addressing these risks early in the life cycle of the emerging technology. EPIC has frequently submitted formal comments to various agencies, including the Department of Homeland Security, the Federal Trade Commission, and the Department of Transportation, and provided Congressional testimony on uses and risks of emerging technologies.[3]

EPIC urges the European Commission to investigate the serious privacy risks and impacts of the metaverse, consider how the metaverse already may violate current EU regulations, and promulgate guidelines and regulations that will address these risks and protect metaverse users.

II. Background

In discussing the "metaverse," we must first be clear about what all falls under the term's scope. While the definition can vary depending on who is speaking, we understand the metaverse as technologies that use XR or "extended reality."[4] This includes the full spectrum of immersive computing, from technology that creates environments that are wholly artificial, as in virtual reality (VR), to technology that overlays virtual elements onto existing physical environments, as in augmented reality (AR) and mixed reality (MR).[5]

---

[3] *See, e.g.,* EPIC Comments to the Dep't of Homeland Sec., Agency Information Collection Activities: Public Perceptions of Emerging Technologies (July 12, 2021), https://epic.org/documents/agency-information-collection-activities-public-perceptions-of-emerging-technologies/; EPIC Testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, Commerce Committee, *The Promises and Perils of Emerging Technologies for Cybersecurity,* 115th Cong. (Mar. 22, 2017), https://epic.org/documents/hearing-on-the-promises-and-perils-of-emerging-technologies-for-cybersecurity/; EPIC Comments to the Dep't of Transportation, Request for Comment: Non-Traditional and Emerging Transportation Technology (NETT) (April 8, 2022).

[4] Eric Ravenscraft, *What Is the Metaverse, Exactly?,* Wired (Apr. 25, 2022), https://www.wired.com/story/what-is-the-metaverse/.

[5] *See* Bernard Marr, *The Important Difference Between Virtual Reality, Augmented Reality and Mixed Reality,* Forbes (July 19, 2019), https://www.forbes.com/sites/bernardmarr/2019/07/19/the-important-difference-between-virtual-reality-augmented-reality-and-mixed-reality.

These technologies process an enormous amount of personal data, collected from users of the technologies, from bystanders whose presence or actions may be picked up by technologies used in their vicinity, and from third parties via contractual agreements.[6] Some of the data collection and use is common in other technologies as well: usernames, account information, logs, purchases, communications, and actions taken within the technology, etc. However, XR is unique in both the source/type and volume of information that it collects. XR combines the more expected data it collects with additional biometric information (such as physical movements, feedback from the environment and surroundings, voice prints, face prints, haptics, and more), real-time data collection, and big data analytics.[7] In addition, the volume of data collected by XR technology sets it apart—just twenty minutes in a VR simulation can result in nearly 2 million unique body language recordings.[8]

This amount of data processing and the sensitivity of the data processed leads to serious privacy risks within the metaverse that must be addressed by any guidance or regulations. Current regulations do not have a clear enough application to XR technologies to sufficiently curb harmful metaverse data practices and are ill-enforced where metaverse data use does clearly violate current law. Regulations specific to the metaverse could provide much-needed protections for users and bystanders and clarity for companies diving into the metaverse.

---

[6] Franziska Roesner, Tamara Denning, Bryce Clayton Newell, Tadayoshi Kohno, and Ryan Calo, *Augmented Reality: Hard Problems of Law and Policy,* 2014 ACM Int'l Joint Conf. on Pervasive and Ubiquitous Computing (UbiComp '14): Adjunct Publication 1283 (August 18, 2014), https://ssrn.com/abstract=2482198; Suchismita Pahi & Calli Schroeder, *Extended Privacy for Extended Reality: XR Technology Has 99 Problems and Privacy is Several of Them,* 4 Notre Dame J. on Emerging Technologies 1, 13 (Apr. 2023), https://ndlsjet.com/wp-content/uploads/2023/04/4-1_Pahi-Schroeder.pdf.

[7] Pahi & Schroeder, *supra* note 6, at 13.

[8] Jeremy Bailenson, *Protecting Nonverbal Data Tracked in Virtual Reality,* 2018 J. Med. Ass'n Pediatrics 905.

III. Privacy Risks

The metaverse is rife with privacy risks—both those common to current technologies and some unique to this space. These risks are substantial and could cause serious harm if not mitigated quickly.

Data Misuse

Data misuse can cover a broad range of practices—typically these harms stem from unexpected, undisclosed, or improper data access, sharing, or use.[9] Improper access could put individuals at risk for physical, emotional, reputational, or monetary harm. One example is if an XR system, which collects real-time location data on users, is accessible by an abusive partner.[10] That partner could then track the user's movements, endangering their safety and preventing them from moving freely. If this information is used by a stalker, it can be a means of harassing or threatening the individual as well.

Sharing data with other parties opens up problems as well, generating risks of employment discrimination, surveillance, denial of disability benefits, and more. For example, an XR technology may be collecting information on a user's movements within the XR environment. If it then shares those movement logs with the user's employer who wants to challenge the user's assertion that they have been injured, this could affect the user's employment.

---

[9] Pahi & Schroeder, *supra* note 6, at 19.

[10] *See, e.g.,* Adrienne Matei, *'I was just really scared': Apple AirTags lead to stalking complaints,* The Guardian (Jan. 20, 2022), https://www.theguardian.com/technology/2022/jan/20/apple-airtags-stalking-complaints-technology; Samantha Cole, *Police Records Show Women Are Being Stalked With Apple AirTags Across the Country,* Vice (Apr. 6, 2022), https://www.vice.com/en/article/y3vj3y/apple-airtags-police-reports-stalking-harassment; Coco Khan, *'Smart' tech is being weaponized by domestic abusers, and women are experiencing the worst of it,* The Guardian (Apr. 4, 2023) https://www.theguardian.com/commentisfree/2023/apr/04/smart-tech-domestic-abusers-women.

Any of these entities with access to the vast spectrum of personal data processed by XR systems could use that information for discrimination or harassment as well. This is a particular risk when sensitive information is collected or inferred. For example, XR technology picks up minute movements of facial muscles, eyes, and the body while in operation. This information can be fed into facial or behavioral analysis or emotion recognition systems, which may result in discrimination against those with physical disabilities, neurodivergence, or cultural differences in emotional expression.[11]

Biometric Data

XR technology collects mass amounts of extraordinarily detailed biometric information.[12] This information is particularly sensitive since it is highly identifiable, often immutable, may reveal additional sensitive information, and may be produced by the user involuntarily. XR systems collect motions that a user may be aware of making, such as swinging a virtual racket at a virtual ball or looking toward a virtual object within the environment, but also collect several motions and features that a user cannot easily control or change. These include gait, vocal tone, facial dimensions, and micromovements.[13]

The risk of collection and processing of such immutable characteristics is already concerning, but that risk is heightened when inferences use this data to conclude even more intimate and sensitive data about the individual. Minute motions and expressions have been used to infer medical conditions in some cases, such as indicating that an individual may be neurodivergent or using vocal tone to indicate depression.[14] Not only can this data reveal

---

[11] Pahi & Schroeder, *supra* note 6, at 19.
[12] Bailenson, *supra* note 8.
[13] *Id.*
[14] *Id.,* Jennifer A. Kingson, *"Voice Biomarker" Tech Analyzes Your Voice for Signs of Depression,* Axios (Oct. 20, 2022), https://www.axios.com/2022/10/20/voice-biomarkers-depression-anxiety-ai-telehealth.

sensitive information about the individual they may want to keep private, but it can also be misused to discriminate against or target individuals based on biometric, emotional, or mental characteristics.

Vulnerable groups

While the listed privacy risks exist for everyone, the impact and likelihood of those risks may increase based on whether the affected individual belongs to a vulnerable or marginalized group. For example, real-time tracking poses a higher risk when connected to children, immigrants, activists, religious and racial minorities, LGBTQIA individuals, and other groups that face increased surveillance and persecution. Data collected and inferences made relating to these categories that is then shared with or sold to other parties—including advertisers—may out these traits to others, endangering the individuals. In some cases, the vulnerable status may expose the individual to additional abuse, such as systems exerting undue influence on children.

Bystander Risk

Collection of bystander data is one of the more metaverse-specific privacy problems we have seen. XR technologies, particularly AR and MR which overlay digital components on a real-world environment, often scan their surroundings in order to function. This, combined with the mobility of many XR devices, means it is likely that XR technology will pick up images and audio of other people in both public and private spaces.

When bystander images or speech is picked up, the information can be used to identify the individual (via facial recognition or voice print). If the XR company holding this information chooses to, they could create shadow profiles on these individuals, whether they are users of XR

or not.[15] Not only can those files identify the individual and their precise location at the time of data collection, they may also be combined with other files from data brokers related to the individual, creating a map of individual movements and a full picture of a person whose only interaction with XR was existing in the same space as a device.

Bystanders will probably be wholly unaware that their information is being collected, depending on how obvious the XR device is. Even where the bystander knows they've been recorded by a device, they likely will not know what XR company holds information on the bystander, whether the information is saved anywhere, or whether it can be used in other ways. Because of this problem, bystanders have little to no ability to exercise rights over their data—how can you request that a company delete your data when you have no idea that the company has it in the first place?

Inferences

While existing technologies also make inferences out of existing personal data, the sensitivity and volume of personal data picked up by XR allows inferences to be much more specific and invasive.[16] As mentioned previously, just minutes in the metaverse can result in millions of unique body movement recordings, demonstrating both the volume and sensitivity of data collected (in this case, biometrics).[17] XR systems also pick up cues from the surrounding environment, an individual's interactions, appearance, voice, motions, and more that can lead to inferences that place a user within a vulnerable category, such as concluding that a user is

---

[15] Facebook has created shadow profiles on non-users in the past, and other companies may do the same. *See, e.g.,* Russell Brandom, *Shadow Profiles Are the Biggest Flaw in Facebook's Privacy Defense,* Verge (Apr. 11, 2018), https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy; Kurt Wagner, *This Is How Facebook Collects Data on You Even If You Don't Have an Account,* VOX (Apr. 20, 2018), https://www.vox.com/2018/4/20/17254312/facebook-shadow-profiles-data-collection-non-users-mark-zuckerberg.
[16] Pahi & Schroeder, *supra* note 6, at 10-11.
[17] Bailenson, *supra* note 8.

transgender.[18] If they are labelled as such within the system, that inference could lead to unethical stereotyping and misuse, potentially harming the individual or revealing that status to the public if the dataset is shared.

Even where the data itself that a system is using to generate an inference is not sensitive, the inference may be sensitive or high-risk, as in the example regarding a transgender inference above. There are other potentially damaging inferences from "benign" data as well—a user's economic status may be inferred from the type of hardware they use or their engagement in virtual shopping scenarios.[19] User relationships may be inferred from interactions or communications within the XR system.[20] In some cases, researchers compared reactions and behaviors of students diagnosed with ADHD with those of other students within a VR environment to test theories on distractibility, potentially used in other circumstances to diagnose ADHD via metaverse reactions and behaviors.[21]

Once inferences are incorporated into an individual's profile, it can be very hard to challenge or remove that inference. If incorrect inferences are accepted as true, it may also create a cycle where increasingly flawed inferences are drawn relating to the individual, all based on mistaken conclusions. The metaverse's data processing poses significant risk of generating inferences that either reveal something that the user did not intend to reveal or infer incorrect

---

[18] *See, e.g.,* Paul Mozur, *One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority,* The New York Times (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html (describing how China is using facial recognition to infer race by looking for facial markers on individuals); Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did,* Forbes (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=3ef724106668 (describing how Target inferred that a teenager was pregnant based on recent purchases and items viewed).

[19] Pahi & Schroeder, *supra* note 6, at 11.

[20] *Id.*

[21] Thomas Parsons, Todd Bowerly, J Galen Buckwalter, & Albert A Rizzo, *A Controlled Clinical Comparison of Attention Performance in Children with ADHD in a Virtual Reality Compared to Standard Neuropsychology Measures,* 13 Child Neuropsychology 4, 363 (2007).

information about an individual. These risks must be addressed by any proposed regulation or frameworks on the metaverse.

IV. Legal Challenges

Certain metaverse practices may already run afoul of current regulations. While there may be many member state regulations that touch on aspects of the metaverse, we look particularly at the GDPR and the AI Act.

GDPR

The GDPR includes both general principles and specific requirements that directly apply to XR technologies and personal data processing, some of which may in fact prohibit common data practices in the metaverse. The GDPR applies to any personal data processing conducted by entities based in the EU or relating to EU residents.[22] All processing under the GDPR must meet certain principles, including that data must be processed transparently, must only be processed for a specific and explicit purpose, must be accurate, and must be limited to only what is necessary for the processing purposes.[23]

Current XR practices already run into conflicts with these principles. For example, how can data collection relating to bystanders be considered "transparent" when bystanders very likely are unaware that personal data on them is collected at all? Are XR companies reusing data collected for device functionality by selling that data to advertisers in violation of the specific purpose for processing? Can XR companies guarantee that inferences made from data are accurate and can all additional inferences stemming from that inaccurate basis be corrected? Are

[22] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation)* (2016), Art. 3.
[23] *General Data Protection Regulation,* Art. 5.

XR companies actively limiting what data they hold to only what is strictly necessary for device functionality?

Outside of these principles, the GDPR also mandates that an individual be informed of several things when personal data is collected, including who is collecting the data, what is being collected, for what purpose it is being collected, and more.[24] This notification must come at the time of or prior to data collection. As mentioned earlier, any XR technologies that collect personal data of bystanders will have a particularly difficult time satisfying this requirement. XR technologies must either develop methods of notifying everyone around an XR device of data collection with the necessary details or must, by default, not collect any bystander data.

Finally, the GDPR lists several categories of data that are considered "special" and cannot be processed unless a specific exception applies. This includes data on racial or ethnic origin, genetic data, biometric data used for identification, health data, and more.[25] Court cases have determined that these protections also extend to information that could "reveal" sensitive categories, including through inferences.[26] As discussed earlier in this paper, not only is biometric data collected on a large scale and ongoing basis through XR systems, that data and additional data can be used to make inferences regarding several of these protected categories.

There are limited exceptions that would allow XR technology to process this sensitive data. One possible exception is if the data subject gives explicit consent to process the data for a specified purpose.[27] This would require fully informed consent from the individual regarding the

[24] *General Data Protection Regulation,* Art. 13.
[25] *General Data Protection Regulation,* Art. 9(1).
[26] Case C-184/20, Court of Justice of the European Union (Aug. 1, 2022), https://curia.europa.eu/juris/document/document.jsf?text=&docid=263721&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=481514.
[27] *General Data Protection Regulation,* Art. 9(2)(a).

data and require that it be processed for specific and limited purposes—a challenge when it comes to bystanders.

While XR companies may argue that such processing falls under the exception for processing data "manifestly made public,"[28] mere use of an XR technology is unlikely to be considered manifestly making data public. Further, bystander data picked up by devices is unlikely to be considered manifestly made public since any inferences made from a bystander's image or voice would likely not fall into that category and XR devices can be inconspicuously brought into both public and non-public spaces where recording is not anticipated or expected. This exception is unlikely to apply to data processing in XR, and express consent seems the only viable path forward for XR systems collecting and inferring sensitive personal data.

AI Act

Though the AI Act has not yet been finalized, it must be considered when informing the Commission's vision for the metaverse. In particular, the current AI Act text specifically prohibits the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes as well as exploiting certain vulnerabilities to influence behavior.[29]

Since XR technology is mobile, it may frequently be used in publicly accessible spaces and constantly picks up real-time biometric markers of its user and other individuals in those spaces that can be used to identify those individuals. While the initial use of these systems may not always explicitly be "for law enforcement purposes," there is every possibility of law enforcement requesting data access and use from XR companies, thereby falling under this prohibition.

---

[28] *General Data Protection Regulation,* Art. 9(2)(e).
[29] European Union Artificial Intelligence Act, Title II Article 5(I)(b) and (d) (as of May 1, 2023).

In addition, the AI Act explicitly prohibits AI that exploits vulnerabilities of a group of people due to "age, physical or mental disability" to "materially distort" a group member's behavior in a way that causes or is likely to cause physical or psychological harm. As discussed earlier, XR collects enormous amounts of personal data, some of which may include age and physical or mental disability and some of which may allow inferences regarding age and physical or mental disability. Once a person is known to belong to one of these categories, there is risk that another party could exploit this knowledge, including through deliberately manipulating that person's behavior in harmful ways. It is critical that the metaverse be carefully monitored and controlled to prevent this possibility.

V. Proposed Solutions

We have set forth many of the possible privacy risks and harms of the metaverse that we urge the Commission to consider when shaping its vision. In the event that the Commission decides to craft regulation specifically addressing these concerns, we propose the following as possible mitigation methods.

Ban

In some cases, the risks to individuals and the risk of data misuse may simple be considered too high to mitigate. In particular, we believe this may apply to data uses pertaining to "social scoring," inferring traits of an individual (such as criminality or trustworthiness), tracking or detecting emotion, diagnosing injuries or conditions, inferring sensitive categories of personal data, linking the individual to a marginalized or at-risk group, or identifying and tracking bystanders. We strongly recommend that the Commission consider fully prohibiting these data practices.

Bystander Protections

There are both legislative and technical ways to address bystander privacy risks and enshrine bystander rights in the metaverse. On a technical level, XR systems may be structured such that they automatically blur or distort images or audio of bystanders. XR systems could also store only direct user data by default, allowing any non-user data to instantly pass out of the system and preventing it from being stored and used for additional purposes.

These technical proposals can be mandated by regulation, which could also enshrine specific bystander privacy rights. However, automatic technical solutions are likely more protective since bystanders must still be aware that their personal data is being processed in order to exercise their data privacy rights.[30] Not collecting bystander data in the first place addresses the problems at their source.

Regulatory Considerations

As the Commission drafts legislation to regulate the metaverse, the language must be carefully crafted in order to include the wide range of technologies and data involved. For example, any proposed regulation must explicitly include both inferences and pseudonymized data within the definition of personal data, making it subject to all personal data protections. In addition, regulation must make clear that the metaverse encompasses all XR technology—not solely virtual reality.

VI. Conclusion

The metaverse is rife with privacy risks, many of which are tied to sensitive data and vulnerable groups. Current data processing practices in the metaverse may already run afoul of

[30] *See* Pahi & Schroeder, *supra* note 6, at 51.

European law. We urge the Commission to develop a vision that directly confronts these privacy risks and protects its citizens from the continuously-expanding reach of the metaverse.

Respectfully submitted,

/s/ Calli Schroeder
EPIC Senior Counsel &
Global Privacy Counsel