European Center for Not-for-Profit Law

accessnow

ELECTRONIC FRONTIER FOUNDATION

ECNL, Access Now, and the Electronic Frontier Foundation (EFF) joint statement in response to European Commission consultation on 'Virtual worlds (metaverses) - a vision for openness, safety and respect'.

Access Now, the Electronic Frontier Foundation, and the European Center for Not-for-Profit Law welcome the Commission's initiative to develop a vision for virtual worlds that respect human rights and European Union law. On International Human Rights Day in 2021, Access Now and the Electronic Frontier Foundation (EFF) issued the joint statement, Virtual worlds, real people: human rights in the metaverse, calling upon governments and companies to address human rights in the context of virtual and augmented reality (VR and AR) and ensure that these rights are respected and enforced. In response to this consultation on 'Virtual worlds (metaverses) – a vision for openness, safety and respect,' we hereby submit an updated version of the statement.

Extended Reality (XR) technologies, including virtual and augmented reality, are the foundations of emerging digital environments, including the so-called metaverse. They are still at an early stage of development and adoption, but venture capitalists and Big Tech are investing heavily in these technologies, and there is a scramble to assert dominance and cement monopolies in what tech investors and executives claim will be the next generation of computing and social media.

Like any other technology, XR can have many positive impacts on our daily lives. It can be a useful tool in areas like medicine, science, and education. Artists are using XR creatively to make virtual worlds their canvas and create new forms of expression. Protests and social movements have also used these technologies to raise awareness on collective issues, or to connect, organize, and make their voice heard when it is physically impossible or dangerous.

Yet XR also poses substantial risks to human rights. VR headsets and AR glasses, coupled with other wearables, could continue the march towards ever-more-invasive sensitive data collection and ubiquitous surveillance. This data harvesting, sometimes done by companies with a history of putting profit before protections, sets the stage for unprecedented invasions into our lives, our homes, and even our thoughts, as data collected by XR devices is used for targeted advertising and to enable new forms of "biometric psychography" to make dubious inferences about our deepest desires and inclinations. Once collected, there is little users can do to mitigate the harms done by leaks of data or data being monetized by third parties.

These devices will also collect huge amounts of data about our homes and private spaces, and could allow governments, companies, and law enforcement disproportionate access to our lives, exacerbating already severe intrusions on our privacy. It can also be used to profile users, in a way that can be discriminatory and put already vulnerable groups at risk of more harm, such as activists, human rights defenders and journalists. Moreover, governments and international organizations are advocating for the implementation of XR in the name of combating crime or terrorism and ensuring national security. However, they often do so without sufficient human rights protections or fully comprehending the potential negative consequences these technologies may have on human rights.

These new technologies also create new avenues for online harassment and abuse. AR glasses risk drastically undermining expectations of privacy in both private and public spaces. A person wearing the glasses can easily record their surroundings in secret, which only becomes more dangerous if surveillance technologies such as face recognition are incorporated. These risks disproportionately impact marginalized groups such as racialized persons, women and non-binary persons, LGBTQIA+, and refugees and migrants, among others.

We have learned many lessons from everything that's gone wrong, and right, with the current generation of smart devices and social media, and we need to apply these lessons now to ensure that everyone can take advantage of XR technologies and the metaverse without sacrificing fundamental human rights we hold dear.

Leverage Lessons Learned for Safeguarding Human Rights:

- We recognize that self-regulation on data protection and ethical guidelines are insufficient for mitigating the harms caused by technology.
- We underscore the necessity of placing human rights standards, including due process, stakeholder engagement, and access to remedy at the center of developments in XR. This will guarantee that not only are our rights safeguarded, but they are also expanded in virtual worlds.
- We would like to draw attention to the potential adverse effects of EU laws when they are copied outside the EU, particularly on internet users and marginalized groups residing in countries with authoritarian practices. This is especially concerning for individuals outside the EU who may not have the same legal protections nor fair trial rights as those within the EU.
- We need to nurture the grassroots, rights-respecting tech being developed today. We need to support the development of grassroots, rights-respecting technologies that can provide alternatives to the current surveillance-driven platforms, as large tech corporations may acquire their competitors.

For any new measures that are introduced, we suggest that the European Commission consider the following principles to ensure that people's rights are protected against state and corporate overreach and intrusion in the context of XR:

- The Commission must ensure the proper enforcement of the General Data Protection Regulation and the Law Enforcement Directive and ensure that data generated and collected by XR systems is subject to strong protections. In particular, any such data used to make medical or psychographic inferences must be subject to the strictest protections, especially in sensitive areas such as criminal justice, national security, and counterterrorism.
- Lawmakers should protect people against the use of XR systems that can make harmful, invasive inferences about our thoughts, emotions, inclinations, and private mental life. Lawmakers should ensure that people are protected against inherently discriminatory categorisation based on their biometrics, as well as dubious and invasive technologies such as emotion recognition.
- Data protection authorities (DPAs) must act to enforce data protection laws and protect people's rights. Research has shown that people's privacy "choices" to let businesses process their data are typically involuntary, prone to cognitive biases, and/or circumventable due to human limitations, dark patterns, and the complexities of modern data processing. DPAs should require transparency about and control over not only the collected data but also the use or disclosure of the inferences the platform will make about users (their behavior, emotions, personality, etc.), including the processing of personal data running in the background. Thus, the legal paradigm of "forced consent" as it is practiced today needs to be challenged.
- The metaverse should not belong to any one company. The Commission must safeguard the diversity of metaverse platforms and prevent monopolies over infrastructure and hardware, so users don't feel locked into a given platform to enjoy full participation in civic, personal, educational, social, or commercial life, or feel that they have to tolerate these failures to remain connected to vital realms of human existence.
- Governments should ensure that the 13 International Principles on the Application of Human Rights to Communications Surveillance are applied, existing privileges against government intrusion are reaffirmed, and legal protections are extended to other types of data, such as psychographic and behavioral data and inferences drawn from them.
- Governments should increase transparency around their use of XR, especially in sensitive areas such as criminal justice, national security, and counterterrorism. As governments start using XR for training and simulations, deliberation, and decision-making and public meetings, new kinds of information will be produced that will constitute public records that should be made available to the public under freedom of information laws.
- As XR technologies become ubiquitous, companies should respect and governments should protect people's right to repair, alter, or investigate the functionality of their own devices.

- As in real life, governments must refrain from censoring free expression and inhibiting journalistic freedoms, and instead encourage participatory exchanges in the marketplace of ideas. With the rise of regulatory initiatives around the world that threaten to chill free expression, it is crucial to adhere to necessary and proportionate measures, consistent with the Santa Clara Principles and international human rights law, balancing legitimate objectives with the freedom to receive and impart information.

The European Commission should ensure that external stakeholders can meaningfully be involved in mapping the impacts on human rights and civic space of XR, as well as in developing policy and regulatory measures to address any human rights risks and adverse impacts. Emphasis should be given to meaningful participation of civil society, academics, affected communities, and marginalized groups.

Additional recommendations for companies, investors, as well as the XR community of developers, can be found in EFF and Access Now's 2021 statement.

Our XR data should be used in our own interests, not to harm or manipulate us. Let's not let the promise of the next generation of computing fail in the same ways the prior generation has. The future is tomorrow, so let's make it a future we would want to live in.

This statement was written by Access Now, the Electronic Frontier Foundation, and the European Center for Not-for-Profit Law