Virtual Worlds, Real People

Human Rights in the Metaverse

accessnow

ELECTRONIC FRONTIER FOUNDATION

Today, December 10, is International Human Rights Day. On this day in 1948, the U.N. General Assembly adopted the Universal Declaration of Human Rights, the document that lays out the principles and building blocks of current and future human rights instruments. In honor of this anniversary, Access Now and the Electronic Frontier Foundation (EFF) are 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.

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 Big Tech is 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 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 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 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 illegitimate access to our lives, exacerbating already severe intrusions on our privacy.

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.

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.

Here's what we know:

- We know that self-regulation on data protection and ethical guidelines are not sufficient to rein in the harms caused by technology.
- We know that we need human rights standards to be placed at the center of developments in XR to ensure that our rights are not only respected, but indeed extended, in the metaverse.
- We need appropriate regulation and enforcement to protect people's privacy and other human rights in the metaverse.
- We also need to nurture the grassroots, rights-respecting tech being developed today. Lawmakers need to be vigilant that Big Tech companies don't swallow up all their competitors before they have a chance to develop rights-respecting alternatives to dominant, surveillance-driven platforms.

To this end, we ask governments to ensure that protections against state and corporate overreach and intrusion apply to XR, as follows:

- Governments must **enact or update data protection legislation** that limits data collection and processing to include data generated and collected by XR systems, including medical or psychographic inferences. Governments should clearly define this data as sensitive, strongly protected personal data under the law, even when it does not meet the high threshold to be classified as biometric, personal data,

or personally identifiable information (PII) under current law. Legislation should recognize XR systems can be used to make problematic, invasive inferences about our thoughts, emotions, inclinations, and private mental life.

- Responsible independent authorities 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, legal loopholes, and the complexities of modern data processing. Authorities 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 notice-and-choice as it is practiced today needs to be challenged.

- The metaverse should not belong to any one company. Competition regulators must take steps to **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. These pro-competitive interventions should include merger scrutiny, structural separation of dominant firms from adjacent elements of their supply chains, prohibitions on anticompetitive conduct such as predatory pricing, mandatory interoperability of key protocols and data structures, and legal safeguards for inter-operators who use reverse engineering and other "adversarial interoperability" to improve a service's security, accessibility, and privacy. This is not an exhaustive list, and, should metaverse technologies take hold, they will almost certainly give rise to new, technology-specific human rights and competition concerns and remedies.

- 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. 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 proportional measures, consistent with the Santa Clara Principles, balancing legitimate objectives with the freedom to receive and impart information.

Companies have a responsibility to uphold human rights as guided by the U.N. Guiding Principles on Business and Human Rights, a global standard of "expected conduct for all business enterprises wherever they operate," applicable in all situations.

The corporate responsibility to respect human rights also means addressing adverse impacts that may occur, as follows:

- Companies should publicly pledge to require governments to get the **necessary legal process to access XR data**, notify users when allowed by law, regularly publish transparency reports, utilize encryption (without backdoors), and fight to limit data that can be accessed to what is necessary, adequate, and proportionate.
- Companies, including manufacturers and providers, should not only protect their users' right to privacy against government surveillance but also their users' right to data protection. They must resist the

urge, all too common in Silicon Valley, to "collect it all," in case it may be useful later. Instead, companies should **apply strict data minimization and privacy-by-design principles**, collecting only what is required for base functionality or to provide specific services users have requested and agreed to, and retaining it only as long as necessary. The less data companies collect and store now, the fewer unexpected problems will arise later if the data is stolen, breached, repurposed, or seized by governments. Any processing of data should also be fair and proportionate.

- Companies should be **clear with users about who has access to their data**, including data shared as part of one's terms of employment or school enrollment, and adopt strong transparency policies, explicitly stating the purposes for and means of data processing, and allowing users to securely access and port their data.
- The development and deployment of XR technology must be scrutinized to **identify and address potential human rights risks** and ensure they are deployed with transparency, proportionality, fairness, and equity.

To investors:

- Investors should evaluate their portfolios to determine where they may be investing in XR technologies and use their leverage to ensure that portfolio companies **adhere to human rights standards** in the development and deployment of XR technologies.

Digital rights activists and the XR community at large have a significant role to play in protecting human rights, as follows:

- XR enthusiasts and reviewers should **prioritize open and privacy-conscious devices**, even if they are only entertainment accessories. Activists and researchers should focus on creating a future where XR technologies work in the best interests of users and society overall.

- Digital rights advocates and activists should **start investigating XR technologies now and make their demands heard** by companies and regulators, so their expertise can inform developments and government protections at this early stage.
- XR communities should **educate themselves about the social and human rights implications** of the technologies they are developing, and commit to responsible practices.

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.