



**EFF Submission to the OHCHR Consultation on the
Practical Application of the United Nations Guiding
Principles on Business and Human Rights to the
Activities of Technology Companies**

February 22, 2022

Katitza Rodríguez, Policy Director for Global Privacy - katitza@eff.org
David Greene, Senior Staff Attorney and Civil Liberties Director - davidg@eff.org

Thank you for providing the Electronic Frontier Foundation (EFF) the opportunity to add our submission to the consultation on the Practical Application of the United Nations Guiding Principles on Business and Human Rights (UNGP) to the Activities of Technology Companies.

EFF is an international civil society non-governmental organization with more than 35,000 donors worldwide dedicated to the protection of individuals' fundamental freedoms online. EFF engages in strategic litigation in the United States and works in a range of international and regional policy venues to protect human rights, foster innovation, and empower consumers.

The first part of our submission focuses on the utility of the UNGP as a self-regulatory tool in assuring that social media content moderation practices are consistent with human rights principles. The second part focuses on the privacy and data protection implications of Extended Reality Technologies (XR), which include Virtual Reality (VR) and Augmented Reality (AR), contributing to session one, "Addressing human rights risks in business models."

I. The UNGP as a Self-Regulatory Tool for Content Moderation by Online Intermediaries

Technology companies, and online intermediaries in particular, face the difficult task of moderating user content consistent with respect for their users' freedom of speech. This content moderation is widespread – practically every intermediary moderates user speech that is legal under the applicable law, but unwanted nonetheless. Content moderation may be an effort to prevent or address harms, such as abuse, harassment, and misinformation. But it also may simply be a reflection of an intermediary's own editorial preferences. In either case, intermediaries frequently must decide whether to take down or prevent the publication of legal speech, suspend or cancel user accounts, deprioritize or demonetize user content, and many other forms of what has become known as "content moderation."

EFF has long advocated that such content moderation be conducted within a human rights framework. We have maintained the website onlinecensorship.org which provides users with resources regarding the content moderation practices of some of the largest companies, and which previously reported on global incidents of content moderation. We have helped formulate and endorse the Santa Clara Principles on Transparency and Accountability in Content Moderation, which offer both foundational and operational self-regulatory principles to guide human rights-compliant practices.¹

The UNGP has an important role to play in content moderation. As a prominent example, in

¹ The Santa Clara Principles, <https://santaclaraprinciples.org/>

each of its decisions, the Meta Oversight Board² has used the UNGP, and Meta’s announced commitment to them, as the source of the human rights principles that inform its analysis of Meta’s human rights responsibilities.

Recommendation to the OHCHR

- Consider the Santa Clara Principles, particularly the Foundational Principles of Human Rights and Due Process, Understandable Rules and Policies, Culture Competence, State Involvement, and Explainability and Integrity, in any revision to the UNGP.

II. Addressing Human Rights Risks in Extended Reality’s Business Model

The UNGP has served as a guideline to address human rights risks linked to a company’s business models. As XR—which includes VR and AR—develops and becomes more widely adopted, the human rights risks associated with XR technology and companies’ business models become more prevalent.³ This technology promises to enhance our lives with new forms of entertainment, education, and free expression; yet it also risks eroding our rights online.⁴ OHCHR has an important opportunity to foster conversation and investigate human rights risks from XR’s business models as the industry is still nascent. Without respect for human rights built in, XR development could replicate and exacerbate the human rights risks we’ve seen from prior technologies that enable mass surveillance and potential manipulation.

Under the UNGP, companies are expected to conduct human rights due diligence across their business activities and relationships. This requires companies to proactively identify when their business models and technologies create or exacerbate human rights risks, and take action to address these situations—whether by mitigating risks within existing business models or by innovating entirely new ones. XR companies can, for example, conduct human rights impact assessments before deploying any XR tools or features, including on the rights of particular groups; conduct periodic ad hoc human rights impact assessments, and make them available to the public; consult with multi-stakeholder groups, ideally including civil society, from across the world, to better address the potential impact of XR technologies on users in different regions. If a specific XR feature has a potential adverse impact, they should refrain from deploying it until

² The Meta Oversight Board, <https://oversightboard.com/>

³ United Nations Human Rights Office of the High Commissioner, *Addressing Business Model Related Human Rights Risks A B-Tech Foundational Paper*, July 2020, https://www.ohchr.org/Documents/Issues/Business/B-Tech/B_Tech_Foundational_Paper.pdf

⁴ Rodriguez, Katitza; Opsahl, Kurt; Mir Rory; Leufer, Daniel, *Virtual Worlds, Real People: Human Rights in the Metaverse*, December 9, 2021, <https://www.eff.org/deeplinks/2021/12/virtual-worlds-real-people-human-rights-metaverse>

the risks have been appropriately addressed, and where no mitigation measures are possible, refrain from deploying such features.

We have divided this section into the critical risks associated with two types of data collected by XR systems: data collected by the sensors about their users (ego-centric data collection) and data collected about the world around the user (by-stander privacy).

2.1 Inward Facing Data Collection: Ego-centric data collection

A B-Tech foundation paper recognized that technology companies' business models have traditionally sought to accumulate extensive behavioral data about a person to make "increasingly accurate and highly lucrative predictions about the interests and behaviors of individuals and groups in society."⁵ XR has the potential to bring the privacy risk to a new level, by gathering even more behavioral data, including from involuntary physiological reactions to situations that a user encounters. Such data can be used to make inferences that have the potential to reveal peoples' beliefs, attitudes, and interests even when the user had no intention of disclosing this information, and can be used to make inferences even if these predictions are inaccurate.⁶

XR headsets are often designed with body-worn and environmental sensors which can collect unprecedented amounts of data about their user and their context. New sensors can make XR technology the frontier of more intimate forms of surveillance. These include monitoring vocal patterns, facial expressions or gazes⁷, and, when coupled with other technology like smartwatches, even heartbeats and body temperature. Body worn sensors also track the unconscious responses that a user's body makes, like eye movements, head motions, and hand gestures. This tracking can be needed for making virtual scenes feel natural, but can also reveal sensitive medical and psychological information, which companies may choose to store on their own servers.⁸

⁵ United Nations Human Rights Office of the High Commissioner, *Addressing Business Model Related Human Rights Risks A B-Tech Foundational Paper*, July 2020, pg. 5,

https://www.ohchr.org/Documents/Issues/Business/B-Tech/B_Tech_Foundational_Paper.pdf

⁶ Leon Kröger, Jacob; Hans-Martin Lutz, Otto; Müller, Florian, *Privacy Implications of Voice and Speech Analysis – Information Disclosure by Inference*, March 2020, https://rd.springer.com/chapter/10.1007/978-3-030-42504-3_16. Heller, Brittan, *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, 23 *Vanderbilt Law Review* 1, 2021, <https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1000&context=jetlaw>

⁷ Leon Kröger, Jacob; Hans-Martin Lutz, Otto; Müller, Florian, *What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking*, March 2020, https://link.springer.com/chapter/10.1007/978-3-030-42504-3_15

⁸ Heller, Brittan, *Reimagining Reality: Human Rights and Immersive Technology*, July 2020, https://carrcenter.hks.harvard.edu/files/cchr/files/ccdp_2020-008_brittanheller.pdf

Moreover, some of these data are not adequately covered by existing data protection laws, as strong protections are often only afforded to ‘biometric data’ which is, in the European Union’s General Data Protection Regulation, for example, limited to a subset of physical, physiological and behavioral data that allows for unique identification. This means that granular data related to eye movement or head inclination, for example, may fail to meet the criteria to be defined as biometric data, and thus not be subject to as strong a protection as data related to a person’s face. Despite lacking strong protections, data about eye movements could be used to make inferences about extremely sensitive aspects of a person, such as sexual orientation, and thus lead to discrimination.⁹

Specifically, providers may analyze data in an attempt to infer a user's thought, personality or mental traits, our “biometric psychographic”¹⁰ as well as the efficacy of the companies’ influence on a user, such as with advertisements. Existing fitness and health phone apps and smart devices already ask users to input their feelings, and some are embarking¹¹ on tone-of-voice analysis.¹² Too often these machine learning algorithms are unsuccessful in understanding their subject, and suffer from racial or gender bias.¹³

Nevertheless, companies’ continued efforts to quantify our public, social, and inner lives will profoundly impact our daily lives in the years ahead. The increasingly intimate measurement of how we interact with stimuli in XR environments can be a risk to users’ autonomy depending on the company’s business model and the way it can exploit involuntary and even unconscious behaviors, aggregating them to produce powerful psychological profiles.¹⁴ This functions like a “like button” that people click without even trying to do so.

Some companies' business models may anticipate subsidizing hardware or services through the monetization of users’ data. It will be tempting to apply this sensitive information to other purposes such as detecting emotion and interest for targeted advertising,¹⁵ and to find the most

⁹ Access Now’s submission to the European Commission’s adoption consultation on the Artificial Intelligence Act, <https://www.accessnow.org/cms/assets/uploads/2021/08/Submission-to-the-European-Commissions-Consultation-on-the-Artificial-Intelligence-Act.pdf>

¹⁰ Heller, Brittan, *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, 23 *Vanderbilt Law Review* 1, 2021, <https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1000&context=jetlaw>

¹¹ Fowler, Geoffrey, Kelly Heather, *Amazon’s new health band is the most invasive tech we’ve ever tested*, December 2020, <https://www.washingtonpost.com/technology/2020/12/10/amazon-halo-band-review/?arc404=true>

¹² Bell, K, *The Next Generation of Wearables Will be a Privacy Minefield*, September 25, 2020, <https://www.engadget.com/next-generation-wearables-privacy-191237188.html>

¹³ See e.g. Ledford, Heidi, *Millions of Black People Affected by Racial Bias in Health-care Algorithms*, *Nature*, October 2019, <https://www.nature.com/articles/d41586-019-03228-6>

¹⁴ Brittan Heller, Bar-Zeev Avi, *The Problems with Immersive Advertising: In AR/VR, Nobody Knows You Are an Ad*, <https://tsjournal.org/index.php/jots/article/view/21/10>

¹⁵ Bar-Zeev Avi, *The Eyes Are the Prize: Eye-Tracking Technology Is Advertising’s Holy Grail*, *Motherboard*, May 2019, <https://www.vice.com/en/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail>

psychologically compelling ways to target users' emotional vulnerabilities through strategies that could be difficult for the user to perceive and resist. If aggregated, this sensitive data may let XR companies identify patterns that let them render people more vulnerable to influence, more precisely predicting (or causing) certain behavior and even emotions.¹⁶

How a company decides to use users' data can drastically shift the consequences of a body-worn sensor. Eye tracking, for instance, may be helpful to reduce disorientation in a virtual world, or to increase image quality where a user is currently looking. It may even be used as a form of hands-free user interface to allow clicking on objects with one's eyes.¹⁷ But it can also show a person's interests in one particular topic, person, advertisement, or slogan over another. Using eye tracking data in ways that do not directly benefit the user or the user can't comprehend that such tracking benefits them can be an intrusion into a person's innermost thoughts and desires.

Some uses of these technologies could be extremely valuable, as, for example, assistive technologies. If the OHCHR chooses to focus on these concerns, it can begin exploring how to ensure that sensitive data is used consensually and only for the user's benefit, and not against them. As the B-Tech project suggested, "if the company cannot take effective steps to prevent or mitigate negative human rights impacts within the framework of its existing business model then that model—or features of it—will need to be adapted or perhaps even transformed by the company acting alone, on an industry-wide basis, or as a consequence of regulatory action."¹⁸

2.2 Outward-facing Data Collection or Bystander Privacy

AR product companies will introduce more and more products that capture and analyze large amounts of video, audio and other information from users' surroundings. AR glasses are the most familiar form of such products, and the likeliest to become widespread in the near future, with several companies already having early versions on the market.¹⁹ While existing "smart

¹⁶ Elaine Sedenberg, John Chuang, *Smile for the Camera: Privacy and Policy Implications of Emotion AI*, <https://arxiv.org/ftp/arxiv/papers/1709/1709.00396.pdf>

¹⁷ MobileWorld, *Apple Patent Application Details Eye Tracking Solution for VR Headsets*, September 2021, <https://mobileidworld.com/apple-patent-application-details-eye-tracking-solution-vr-headsets-092105/>

¹⁸ United Nations Human Rights Office of the High Commissioner, *Addressing Business Model Related Human Rights Risks A B-Tech Foundational Paper*, July 2020, pg. 7, https://www.ohchr.org/Documents/Issues/Business/B-Tech/B_Tech_Foundational_Paper.pdf

¹⁹ Circuit stream, *16 Augmented Reality Glasses of 2021*, February 2022, <https://circuitstream.com/blog/16-augmented-reality-glasses-of-2021-with-features-breakdowns>

glasses” are still far from fully fledged AR glasses, some already indicate where companies such as Meta,²⁰ Snap,²¹ and Apple²² are heading.

AR glasses provide innovative possibilities like directions for walking or cycling, an avatar to view while talking to your family, and a visualization of how a new lamp will look in your home. Some of these applications, depending on the companies’ decisions and business models, can require sensors to determine where the wearer is looking, which can be implemented with inward-facing cameras. And the ability to easily collect and analyze images and other information in one’s environments can also be a great benefit for journalism and freedom of expression.

These devices will present serious questions about the privacy of persons other than the XR user. The extent to which this outward-facing data collection presents human rights concerns will vary depending on what information is collected, how it is processed, where it is stored, what it is used for, whether and how it is encrypted, and how long it is retained. One application might use a series of images of the user’s surroundings for a very brief time—and not transferred outside the user’s device—to display navigation directions, while another might take advantage of all its users’ movements to obtain and upload surveillance video of an entire city.

These concerns persist even though large numbers of cameras are already present in most public spaces, and people in densely-populated areas are already likely to be photographed even without XR. However, new and different concerns are raised by expanding the scope, duration, undetectability, and centralization of surveillance.

One recent AR product is Ray-Ban and Facebook’s Ray-Ban Stories, a new generation of smart glasses, unveiled in September 2021.²³ These smart glasses look just like normal Ray-Ban glasses but can also record pictures and videos, potentially capturing bystanders in public and private spaces. The product was roundly criticized for inadequately notifying bystanders that they were being recorded,²⁴ with Irish and Italian Data Protection Regulators calling on Meta to demonstrate that the white activity light provides effective notification.²⁵ Indeed, Meta fails to

²⁰ Facebook, *Project Aria*, <https://about.facebook.com/realitylabs/projectaria>

²¹ Heath, Alex, *Snap’s First AR Spectacles Are an Ambitious, Impractical Start*, December 2021, <https://www.theverge.com/22819963/snap-ar-spectacles-glasses-hands-on-pictures-design-features>

²² Lynch, Gerald, Peckham James, *Apple Glasses: here’s everything we know so far*, January 2022, <https://www.techradar.com/news/apple-glasses>

²³ Facebook, *Ray-Ban and Facebook Introduce Ray-Ban Stories, First-Generation Smart Glasses*, September 2021, <https://tech.fb.com/ray-ban-and-facebook-introduce-ray-ban-stories-first-generation-smart-glasses>

²⁴ Daniel Leufer, *Why You Shouldn’t Buy Facebook Ray-Ban Smart Glasses*, Access Now, September 2021, <https://www.accessnow.org/facebook-ray-ban-stories-smart-glasses-privacy-review>

²⁵ Ireland Data Protection Commission, *Statement Concerning Facebook View (Glasses)*, September 2021, <https://www.dataprotection.ie/en/news-media/latest-news/data-protection-commission-statement-concerning-facebook-view-glasses>

sufficiently prioritize human rights in the design of Ray-Ban Stories. As EFF and Access Now have written, “human rights standards [should] be placed at the center of developments in XR to ensure that our rights are not only respected but indeed extended.”²⁶

Notification alone may not resolve all concerns about the privacy of bystanders. Ubiquitous recordings or live-streams from enormous numbers of camera-glasses, collected in a central location, geographically tagged, and readily accessible to governments, represent a kind of surveillance panopticon—including the ever-present knowledge that one could be observed at any moment in public or semi-public spaces. As recording and analysis expand, “systematic or permanent recording and the subsequent processing of images could raise questions affecting the private life of individuals.”²⁷ Enough smart glasses in a location can create a virtual time machine to revisit that exact moment in time and space.

With additional emerging visual analytics, albeit unproven (everything from aggression analysis to lie detection based on facial expressions), this technology poses a truly staggering threat of surveillance and bias.²⁸ At the same time, capabilities to recognize features of one’s environment and others’ behavior can be of great value in assistive technologies, and may help journalists and activists exercise their rights to free expression.

The B-Tech Project Foundational Paper notes the dangers in companies’ “propensity to act fast including when ‘testing in the wild’ and deploying innovations at scale”;²⁹ that tendency is a noteworthy risk for AR glasses.

This is an urgent area for stakeholder collaboration to tackle the challenges of protecting the privacy of bystanders, far beyond notifying bystanders. The OHCHR can explore human rights principles for when AR glasses are capable of running facial recognition and other complex applications, as well as the tensions between privacy, freedom of expression, and freedom of association that arise when some places and subjects can be treated as off-limits for recording.

Smart glasses can exacerbate the pervasive monitoring issues that cameras and smartphones are already creating; we risk losing even more of the privacy of crowds. Far more thorough

²⁶ Rodriguez, Katitza; Opsahl Kurt; Mir, Rory; Leufer, Daniel, *Virtual Worlds, Real People: Human Rights in the Metaverse*, December 10, 2021, <https://www.eff.org/deeplinks/2021/12/virtual-worlds-real-people-human-rights-metaverse>

²⁷ Rodriguez, Katitza; Opsahl, Kurt, *Augmented Reality Must Have Augmented Privacy*, EFF, October 2020, <https://www.eff.org/deeplinks/2020/10/augmented-reality-must-have-augmented-privacy>

²⁸ Stanley Jan, *The Dawn of Robot Surveillance*, ACLU, June 2019, <https://www.aclu.org/report/dawn-robot-surveillance>

²⁹ United Nations Human Rights Office of the High Commissioner, *Addressing Business Model Related Human Rights Risks A B-Tech Foundational Paper*, July 2020, pg. 11, https://www.ohchr.org/Documents/Issues/Business/B-Tech/B_Tech_Foundational_Paper.pdf

records of our sensitive public actions, including our presence at a political rally or protest, or at church or a doctor's office, will be permanently recorded and easy to search for and analyze.

Recommendation to the OHCHR under 2.1 and 2.2:

- Identify new human rights safeguards in the context of XR, in particular, companies' corporate responsibility vis-a-vis government data demands, including across border;
- In cooperation with the Working Group on business and human rights, explore in a multi-stakeholder dialogue about which human rights safeguards will need to be strengthened in the XR context, for example, against unwanted emotion detection and inferences;³⁰
- In cooperation with the Working Group on business and human rights, author a report on the impact of XR on human rights, including on marginalized groups;
- In cooperation with multi-stakeholder partners, consider drafting a set of guiding principles on XR and human rights;
- Discuss XR and its human rights implications at the next UN Forum on Business and Human Rights.³¹

³⁰ OHCHR, Working Group on the issue of human rights and transnational corporations and other business enterprises, <https://www.ohchr.org/EN/Issues/Business/Pages/WGHRandtransnationalcorporationsandotherbusiness.aspx>

³¹ OHCHR, UN Forum on Business and Human Rights, <https://www.ohchr.org/EN/Issues/Business/Forum/Pages/ForumonBusinessandHumanRights.aspx>