UCLA Institute for Technology, Law & Policy

GOVERNING XR

Developed by the UCLA Information Policy Lab.

Edited by Michael Karanicolas, Melodi Dincer, Maria Fernanda Muñoz, and Noah Keith.

October 2024

Table of Contents

Introduction — Getting Real about Extended Reality

Michael Karanicolas
Melodi Dincer

Extended reality technologies, often referred to as XR, are likely to transform the ways that we engage with the world. XR has had a number of false starts, but its endurance demonstrates its allure over the tech industry. The consistent fascination with developing XR tools suggests a future where our interface with the information society breaks away from the current screen-based paradigm into something more immersive and interactive. We may not know when this change is likely to happen, or which company, or companies, are likely to lead this transition, but once it occurs, it will introduce new challenges to our relationship with technology that will require creative legal and policy protections. This Report tackles those challenges head on, exploring the ways in which XR pushes law and policymakers to rethink our current approaches to digital content moderation, privacy, governance, and civic participation.

What Is XR?

There are various terms associated with immersive technologies that are defined somewhat inconsistently. As a general category, they are best understood through their capacity to offer deeper, more physiologically impactful ways to interact with information systems. For simplicity, XR technologies can be divided into two main types: virtual reality (VR) and augmented reality (AR).

In VR systems, the user is placed inside an interactive virtual environment through use of a wearable interface, typically a "head-mounted display" (HMD). These headsets display two separate video feeds for each eye, which employ additional lenses to focus the image, and create a realistic, three-dimensional effect due to the different perspectives. There are a number of tricks these headsets use to make the experience as realistic as possible, such as foveated rendering, which tracks the users' pupils in order to concentrate computing resources on details at the center of one's field of vision. However, these techniques also require an incredibly invasive level of data collection to maximize their efficacy, monitoring every twitch and reaction to provide a more persuasive experience.

By contrast, AR systems tend to layer virtual content on top of the user's real environment, though without necessarily taking account of the real objects within that environment. Technologies where virtual content is layered onto, and takes account of, the real environment are known as mixed reality. The interface typically achieves this effect by using cameras to analyze the user's field of vision, and superimposing text or graphics into the existing world. These interfaces can be wearable, as was the case for Google Glass, but can also be accessed through one's smartphone or mobile device, as players did with the notorious AR game Pokémon Go. Although they do not incorporate the same level of data collection as VR devices, AR technologies nonetheless require a high level of surveillance to function, particularly related to the user's location, field of attention, and visual movements. They may also capture bystanders in the vicinity of a user, posing risks to non-users who may not be aware of AR's presence and do not consent to their inclusion in these datastreams.

What Makes XR Unique?

Among the primary features of XR are its heightened feeling of reality towards the environment being presented, to the extent that participants in VR will respond physiologically to virtual experiences, such as being slapped, or perching on top of a high building. Depictions of first-person death in VR, for example, are described as incredibly intense. Powerful sensations have been reported even where the image quality of the graphics is less than photorealistic, and in fact, representative environments can sometimes be even more effective since they encourage the brain to fill in missing details. Aspects of the immersive experience are most commonly visual and acoustic, but can also include haptic stimulators to create a full sensory experience. In short, these technologies generate a sophisticated all-encompassing sensory package to trick your body into experiencing a different reality.

The false sense of "embodiment" that XR technologies generate can create a powerful connection between users and their virtual selves. While this phenomenon is not unique to XR, XR technologies are a particularly powerful driver of it. Emotional responses to sensory cues can also be stronger in an immersive context. The activation of spatial memory also means users retain immersive technology experiences more powerfully, rendering these experiences closer to reality than traditional two-dimensional video.

XR Policy and Governance Challenges

This Report explores a number of challenges XR technologies pose to existing governance, privacy, and content moderation regimes today. Each chapter highlights a particular challenge, describing how XR is different from non-immersive technologies and providing policy suggestions to adapt regulations to better address potential harms and, where needed, create new regulations altogether.

First, the biggest players in this space aim to capture users in a fully interconnected XR experience that spans across devices and applications to immerse them in a singular, navigable virtuality. If this ambition is achieved, a major governance challenge will be determining the rules that will govern this shared landscape, including the behavioral and technological norms which will determine how users are able to access and enjoy various aspects of the XR universe. This is especially important as XR spaces are overwhelmingly designed by private tech companies with proprietary, corporate-centric functionalities in mind; when designers and developers make choices that prioritize exclusivity, hoping to expand market share and drive profits, this cuts against users' ability to enjoy cohesive XR environments regardless of which companies' specific tools they have at hand (or around their heads). Left alone to their own devices, these companies have already begun to adopt industry-wide standards that bind different providers to some level of interoperability. The issue with these standards is that they are likely to further the business priorities of the handful of companies with the most power and sway, locking their users into their own proprietary systems and disincentivizing newer, smaller groups from getting different XR tools in front of users.

As an alternative to industry-set standards, we recommend adopting a human-centric approach to interoperability across XR spaces. We recognize that there are various types of interoperability which each pose their own distinct challenges and opportunities, including technical, usage, and jurisdictional interoperability. Ultimately, we focus on the need for robust technical interoperability standards set by pluralistic groups that include members beyond the tech industry. To ensure interoperability, we recommend:

- Adopting open and common technical standards;
- Government intervention in the standard-setting process;
- Robust enforcement of existing laws, like the interoperability rules in the European Union General Data Protection Regulation and Digital Markets Act, to XR providers; and
- Balancing technical interoperability with information privacy and security protections.

Second, echoing earlier hopes for social media platforms, XR proponents point to the technology's potential for increasing democratic participation through immersive, interactive features. They believe that XR virtuality can expand access for citizens and encourage seamless social and political participation, including through state actors providing public services and engaging with constituents in XR. This utopic view glosses over the many factors that could hinder public engagement in XR, as well as the natural limitations of virtual experiences in building real-life empathy and community — necessary elements of political activism. To foster public participation in XR spaces responsibly, we recommend:

- Opening democratic spaces for citizens to engage with each other within XR devices and applications;
- Democratizing the governance structures within XR spaces; and
- Direct government involvement in establishing XR venues for participation and public services.

Third, XR amplifies existing challenges around content moderation online. XR spaces pose unique challenges to moderating harmful content stemming from their immersive qualities, which influence both the substance and the form of harmful content compared to image and text-based content on non-immersive platforms. When XR users encounter harmful content, they have an embodied experience of it. Even assuming that content laws governing social media platforms apply equally to XR content, XR moderation is mired in challenges stemming from the dynamic nature of the XR environment, including the massive amounts of real-time, diverse data generated by XR encounters. From hate speech to copyright violations, this chapter explores a range of harmful XR content and the difficult balance between safety and speech. We provide a few guiding concepts and recommendations for ensuring effective content moderation in the XR space:

- Incorporating safety by design;
- Integrating community engagement in moderation efforts; and
- Rethinking legal liability frameworks to better address XR harms and regulatory enforcement.

Finally, XR is likely to pose a challenge to existing data privacy frameworks. XR differs from non-immersive technologies when it comes to privacy: XR tools collect more data, a greater range of data, data in real-time interactions, data of bystanders in the background of someone's device space, and aggregate data from both on- and off-device sources. The novel ways that XR devices collect and process data strain existing, nascent privacy laws which were developed to regulate non-immersive technologies. However, the normalized practices of commercial and government surveillance translate directly from prior technologies into the XR space, meaning users' personal information is vulnerable whether it lives on one's smartphone, in the cloud, or on their XR device. Existing data privacy regimes, like the European Union General Data Protection Regulation and the California Consumer Privacy

Act, which are already scrambling to keep up with the modern surveillance economy, fall well short of addressing XR's unique challenges to data privacy and user control over data. To foster stronger protections for data generated by XR users, we recommend:

- Mandating data minimization and purpose limitation for XR data;
- Creating iterative ways to capture user consent throughout virtual experiences;
- Enabling users to access, control, and delete their data;
- Requiring privacy-enhancing technologies within XR environments; and
- Strengthening antitrust regulations and enforcement mechanisms to enable competitive, data-protective practices and interoperability.

Acknowledgments

This publication was developed as part of an innovative new experiential learning class aimed at onboarding students into the tech policy space and developing their critical analytical capabilities by training them to answer emerging policy questions. Developed by the Institute for Technology, Law and Policy at UCLA, the **Information Policy Lab** engaged a group of students to work through the policy implications of this new technology.

The 2024 Information Policy Lab was co-taught by Michael Karanicolas and Melodi Dincer, based on a syllabus designed in collaboration with Maria Fernanda Muñoz. The authors wish to thank Chris Riley, Delara Derakhshani, Brittan Heller, Jordan Fieulleteau, Justin Hendrix and Ben Lennett who provided helpful feedback and inputs for the development of this work, though the opinions and conclusions expressed are solely those of the authors. Thanks as well to Alexandra Mata for her work in support of ITLP, and to Juliana Gallin, for designing the formatting and cover.

The **Institute for Technology, Law and Policy** is a collaboration between the UCLA School of Law and the Samueli School of Engineering whose mission is to foster research and analysis to ensure that new technologies are developed, implemented and regulated in ways that are socially beneficial, equitable and accountable.

Executive Summary

Interoperability and Technical Standards in the Metaverse

Interoperability and technical standards will be pivotal for the development of a human-centric approach to the Metaverse. Strategies in this space should include:

1. **Adopt open and common technical standards**. To achieve the highest degree of interoperability, the focus must be on developing open and common technical standards that promote horizontal interoperability across the entire XR ecosystem rather than just facilitating third-party vertical interoperability. These standards should at least consider technical, usage, and jurisdictional interoperability.
2. **Government intervention in the standard-setting process.** Governments should oversee and intervene in standard-setting processes to ensure that interoperability standards are embedded in the Metaverse architecture. Standard-setting processes should also integrate inclusivity by having individuals from marginalized communities act as experiential experts on community advisory boards and any other space where policy decisions are made.
3. **Enforcing existing laws.** GDPR's and DMA's interoperability rules should continue to be enforced and updated to apply appropriately to virtual worlds. For example, DMA's designated core platform services should be updated to include services specifically related to XR. At the same time, companies' self-preferencing actions should be considered under specific interoperability legislation and by applicable antitrust laws.
4. **Interoperability vs Privacy and Security.** While promoting interoperability, it's crucial to maintain user control over data sharing and digital identity and ensure safety measures, especially for vulnerable users like children.

Additional Considerations:

1. **XR spaces have primarily been designed with corporate-dominated functions in mind.** As it stands now, the Metaverse behaves more like a fragmented technology that encompasses multiple proprietary systems rather than the one ecosystem envisioned to be open and interoperable. XR companies are envisioning the Metaverse as one mainly governed by technical standards groups, so it is likely that public-benefit standards, like interoperability, will collide with the business priorities of the large companies leading the standard-setting process.
2. **The importance of interoperability and technical standards.** Interoperability and other related technical standards are essential to foster a human-centric approach to XR by helping ensure that users are not confined to one XR platform, with limited access, movement, and autonomy in the digital world. Enhancing users' experience across the XR ecosystem can also open XR companies to future growth and innovation, allowing this technology to reach its full, seamless, and interconnected potential.
3. **Limitations of existing regulation.** In Europe, the GDPR's right to data portability and the DMA's protocol interoperability mandates are strong starting points for evaluating interoperability and its feasibility in the Metaverse. However, because these rules were not crafted with the unique characteristics of XR in mind, their practical implementation within the XR space is still uncertain. At the same time, most XR companies are still based in the United States, where there are no mandatory interoperability rules at a federal level.

XR and the Digital Citizen

To harness the potential of XR technologies for enhanced citizen engagement and public service delivery, strategies should include:

1. **Opening democratic spaces for citizens to engage with each other.** Platforms should take steps in the metaverse to consciously and actively promote democratic actors and narratives. To use XR to foster empathy between citizens and cultures, policymakers should prioritize authentic representation and understanding of diverse experiences.
2. **Democratizing XR governance structures.** Developers and policymakers should proactively support alternative governance mechanisms, including voting systems, oversight councils, and employee mobilization. Citizen engagement should also include representation from diverse interests and communities, reflecting the totality of the user base and the public at large.
3. **Implementing XR government services responsibly.** Governments wanting to implement XR technologies should introduce them through an iterative process, ensuring accessibility for marginalized groups. They should also collaborate with XR companies to reduce the complexity of government services in XR and invest in research and policy instances (e.g. sandboxes) to test whether these technologies provide better and more equitable services and decision-making. Finally, governments should incorporate measures to address privacy concerns in the XR space.
4. **Developing comprehensive XR policies.** Governments should develop enforceable XR-specific policies that guide the interaction and distinguish the roles and responsibilities of governments, companies, and human subjects in this space. These standards should provide robust protections against discrimination or other human rights violations through these technologies.

Additional Considerations:

1. **XR potential for citizen engagement.** XR technologies offer powerful opportunities for meaningful citizen engagement and empathy-building among decision-makers and the public at large, to promote transparency and inform public decision-making, and improve public service delivery.
2. **The problem with growth-oriented governance structures.** Governance that is guided by purely commercial interests tends to disfavor vulnerable groups since they are more likely to be marginalized from digital spaces, with limited access or ability to influence the decision-making processes of tech companies. Achieving a democratic and inclusive metaverse requires a more democratic governance model.
3. **The risks of adopting XR for public services.** While the use of XR for public service delivery carries significant potential value, there are also risks and hurdles. Public skepticism and resistance to change, privacy and cybersecurity concerns, marginalized groups' lack of accessibility, the lack of transparency related to adoption decisions, and the role of the private sector in e-governance efforts may hinder governments' use of XR platforms to engage with their constituents.
4. **The tension between public and private interests.** While governments can benefit from leveraging the technical expertise of private companies, public-private arrangements sometimes blur the distinction between government and business entities. Relying on private sector contractors to deliver public services can also create grey areas regarding the applicability of human rights, accountability, or transparency rules that typically bind the public sector.

Content Moderation in XR

Due to its immersive nature and the diversity of engagement structures, XR presents unique challenges for content moderation. Our recommendations for creating safer and more trustworthy XR environments are:

1. **Implement "Safety by Design" features into XR platforms.** "Safety by design" principles should emphasize accountability, transparency, and user empowerment in XR architecture. This includes making reporting mechanisms easily accessible for minors, setting safety and security defaults to the strongest option possible, giving users more control over recommendation and communication features, offering in-platform resources to guide users on the standards for appropriate behavior, and proactively encouraging users to review platform settings.
2. **Develop new automated tools.** Invest in research to develop tools capable of grappling with the vast array of social and informational cues that manifest in an XR environment. Where these tools cannot be readily deployed, it should lead to questions as to whether the technology itself is ready for market.
3. **Adopt a community-based approach to content moderation.** Leverage user communities to establish and enforce content norms. XR platforms should develop company-wide codes of conduct that provide baseline standards, but will have to delegate most enforcement to decentralized leadership teams responsible for their own sub-communities.
4. **Update existing laws and regulations to address XR-specific issues.** Existing tort liability frameworks may need to be revised to adequately reflect how harm manifests in an XR context. Likewise, expectations about the speed and efficacy of content moderation will need to be adapted from the text-based enforcement models that regulators are more familiar with.

Additional Considerations:

1. **There are critical differences between moderation in XR environments and the traditional social media space.** The increasingly vivid and accurate representations of reality enabled by XR's immersive nature can further amplify hate speech's impact and misinformation's ability to influence users. XR can also support new types of CSAM (e.g., through deepfake images), facilitate grooming tactics, and exacerbate the negative impacts of sexual harassment.
2. **Safety and free speech trade-offs in XR environments require careful consideration.** On one hand, regulations that curtail free expression could hinder the growth and adoption of XR. On the other hand, users may also be driven away by a hostile virtual environment. While European democracies have largely embraced the need to strengthen regulation over digital speech, the appropriate scope of government or private intervention remains controversial in American discourse.
3. **Traditional content moderation tools are inadequate for XR environments' dynamic and immersive nature.** Analyzing XR users' speech and movement at scale is an exceedingly difficult task. The amount of data aggregated in real-time is far too great for content to be moderated externally on a case-by-case basis. The ability to monitor XR spaces is also hampered by the current state of moderation technology. As a result, XR companies have turned to personal moderation tools that enable users to shield themselves from unwanted content (e.g., "space bubbles"), but these are ineffective at dealing with many forms of speech-related harms.

Privacy and XR

Data minimization, purpose limitation, meaningful consent, access and control to personal data, and privacy by design will be key principles to ameliorate the inevitable privacy challenges posed by XR:

1. **Data minimization and purpose limitation.** Authorities should focus on carefully overseeing compliance with purpose limitation and data minimization requirements, including those found in the GDPR, to the XR space. In the U.S., policymakers should introduce new legislation to prevent harmful surveillance in the virtual world.
2. **GDPR's limitations and meaningful consent.** Some aspects of the GDPR should be revisited and tailored to XR. For example, the quality of protected biometric data should not depend on companies' processing purposes but be presumed by default every time this data is processed in XR. Policymakers should also develop new immersive and user-friendly ways to give and revoke consent in the XR space.
3. **Access and control mechanisms.** Users should be able to review, edit, or delete their data and settings to manage privacy preferences and permissions within XR environments. XR companies should also take steps now to ensure user data is portable.
4. **Privacy-enhancing technology.** Further specifications from European authorities should identify which privacy-enhancing technologies will serve as a minimum baseline for companies to legally comply with GDPR's privacy-by-design requirements in the XR space. Governments should also participate in the standard-setting process to ensure that companies are building privacy-by-design mechanisms into their ecosystems' architecture.
5. **Antitrust measures.** To prevent a handful of providers from centralizing XR data, authorities will need to enforce existing antitrust laws and draw on interoperability rules and standards to prevent and sanction the raising of artificial barriers to entry into the XR space.

Additional Considerations:

1. **XR data collection capabilities differ from non-XR technologies.** XR devices must collect immense quantities of highly sensitive and accurate data to create immersive experiences for users, which are then aggregated and further processed both on- and off-device. XR devices also pose a privacy risk to bystanders who are unwittingly caught in the XR data collection range.
2. **XR as a surveillance mechanism.** XR companies have the potential to create a commercial surveillance system of unprecedented power that advertisers and other private companies can exploit for profit. XR data collection also creates a treasure trove of information for governments to use via direct access to devices or through overbroad legal requests.
3. **Limitations of existing privacy regulations.** GDPR already places strong limitations on tech companies' behavioral advertising models. However, applying the GDPR's consent rules in the XR space is not straightforward. The types of biometric data protected by the GDPR depend on companies' original processing purposes, and the complexities of the XR space challenge the notion of meaningful and freely given consent. In the U.S., there is no federal privacy law and various state laws face significant limitations to safeguard users' privacy rights.
4. **Privacy by design for XR.** Certain technological innovations, such as end-to-end encryption, jammers, or blurring images, can mitigate the privacy risks of XR. While privacy by design is already required by the GDPR, it is ultimately up to the companies to decide which measures to embed in their systems' architecture.

Interoperability and Technical Standards in the Metaverse

Megan Bradley
Maria Fernanda Muñoz
Elizabeth Mzungu
Chen Yan

Introduction

With tech companies, users, and governments betting on a future mediated by XR technologies, some are expecting the Metaverse to become the next generation of the World Wide Web.[1] In such a context, governance concerns, such as who will govern the Metaverse and how users, companies, and governments will interact with each other in virtual worlds, are already arising in the XR landscape. If the promise of a fully interconnected XR space became real (whether under the name of the Metaverse or not), one major governance question is what rules should govern it and to what extent the Metaverse should be interoperable.

As with other related governance concerns, interoperability in the Metaverse will have to deal with the fact that XR spaces have primarily been designed with proprietary, corporate-dominated functions in mind. In contrast to the initial development of the Internet, which was designed to be decentralized and to serve certain public functions,[2] the Metaverse is currently "a completely private space owned, managed, and operated by profit-driven companies."[3] Because the early Internet was developed as a government-centric and academic project, "its architecture naturally prioritized spaces for education, opportunities for experimentation, and open collaboration."[4] In contrast, the Metaverse is being designed by a few large tech companies, including Meta, Microsoft, Roblox, and Apple. As profit-driven companies, these major players will likely want to embed their commercial priorities into the Metaverse architecture. For example, public documentation suggests that Meta, whose business model generally revolves around advertising and the collection and processing of personal information, will develop its XR technologies with an eye towards further bolstering its advertising business.[5]

Revisiting Lawrence Lessig's famous code-as-law theory, Brittan Heller highlights the profound social, political, and economic consequences of the choices made in designing the architecture of the Metaverse. How the Metaverse is designed will impact who has access to it, how and who can move across different virtual worlds, and how users self-identify in the XR space.[6] While the Metaverse's

---

[1] *See, e.g.,* Mitchell Goldberg & Fabian Schär, *Metaverse Governance: An Empirical Analysis of Voting Within Decentralized Autonomous Organizations,* 160 J. Of Bus. Rsch. 113764 (2023).

[2] Andrew McStay, *The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons,* 36 Philos. & Tech. 13 (2023).

[3] Vincent Mosco, *Into the Metaverse: Technical Challenges, Social Problems, Utopian Visions, and Policy Principles,* 30 Javnost - The Pub. 161, 167 — 68 (2023).

[4] Brittan Heller, *Revisiting Code as Law: Regulation and Extended Reality* 1, 40 (Sept. 1, 2023), available at https://ssrn.com/abstract=4559458.

[5] Ben Egliston & Marcus Carter, *Critical Questions for Facebook's Virtual Reality: Data, Power and the Metaverse*, 10 Internet Pol'y Rev. (2021).

[6] Heller, *supra* note 4.

code-as-law could be constrained by Lessig's other modalities of regulation — the law, social norms, and the market — the problem with how the Metaverse is currently being developed is that the market "is an overwhelmingly powerful modality in comparison to the others."[7]

The prevalence of the market modality of regulation has already been reflected in large tech companies' view of the Metaverse as one purely governed by technical standards groups.[8] For example, the Metaverse Standards Forum (MSF) is an industry-wide effort to harmonize standards for the Metaverse that includes tech giants like Google, Meta, and Microsoft, standards groups like Khronos Group and Web3D Consortium, and other tech stakeholders.[9]

The problem with a Metaverse entirely governed by standards groups like MSF is that public-benefit standards, like interoperability, will likely collide with the business priorities of the large companies leading the standard-setting process.[10] Because the same large technology companies that dominate current digital environments are the ones setting the Metaverse's rules, it is expected that technical standards set by them could lock users into their proprietary systems, leaving other relevant actors constrained in their opportunity to shape the new virtual worlds.

In a purely business-centric Metaverse, our identities and behaviors within are commodified,[11] there are no public areas,[12] and the government is reduced to an allocated play area.[13] But if the Metaverse were to become central to our participation in society, there are good reasons to treat it as a public good. At the very least, the public interest should be embedded into the shaping and functioning of the Metaverse.[14] A human-centric or public-interest approach to the Metaverse will thus be essential to incorporate the voices of the users, governments, and businesses into the code-as-law of the Metaverse, as each of these groups will coexist and be directly impacted by the new digital society.

To be sure, while the profit-driven development of the Metaverse may be a distinct feature of how this technology is *currently* envisioned, this does not mean that the Metaverse will or should be determined solely by the interests and visions of the large technology companies investing in it. The Metaverse is still an empty signifier,[15] one with high interpretative flexibility,[16] and as with any other technology, it is not static; its meaning can change over time and is subject to social construction.[17] As Heller puts it, if code-as-law and market forces end up creating unfair outcomes — i.e., excluding participants from the virtual worlds — social norms can drive the Metaverse's governance to include public values and conventions.[18] Thus, the trajectory of the Metaverse can — and probably should — be changed

---

[7] Heller, *supra* note 4, at 42.

[8] McStay, *supra* note 2, at 14.

[9] George Lawton, *The Metaverse Standards Forum: What You Need to Know,* Techtarget (Feb. 29, 2024), https://www.techtarget.com/searchcio/feature/The-Metaverse-Standards-Forum-What-you-need-to-know [https://perma.cc/JPH6-FCQ4].

[10] McStay, *supra* note 2, at 12–16.

[11] Mosco, *supra* note 3, at 167–68.

[12] *Id.*

[13] McStay, *supra* note 2, at 14.

[14] *See* McStay, *supra* note 2.

[15] *Id.* at 3.

[16] Mateusz Dolata & Gerhard Schwabe, *What is the Metaverse and Who Seeks to Define It? Mapping the Site of Social Construction*, 38 J. Of Info. Tech. 239, 240 (2023).

[17] *Id.* at 242.

[18] Heller, *supra* note 4, at 34–60.

according to the interests of other actors beyond big technology companies, including those that will be the most impacted by this technology.

Under our conception of a human-centered Metaverse, governance should be designed and shaped to at least enable open and interoperable virtual worlds, assets, and identities, by setting governance standards in participatory and inclusive spaces. Interoperability and other related technical standards are essential for users to move freely in the Metaverse, allowing them to take their identities and assets with them across different virtual worlds.[19] To be sure, a human-centric approach would also need to be considered when dealing with privacy, safety, and other governance-related concerns. However, here we focus on interoperability because it is one of the main factors that will tackle the distribution of power between the different actors across the XR space.

In what follows, we first explain why interoperability is important to achieve a human-centric approach to the Metaverse, how existing legal frameworks could help meet this goal, what their limitations are in the XR context, and what types of interoperability should be encouraged in the Metaverse. In the second section, we address the complexities of interoperability as a technical standard, what are the benefits and downfalls of letting standard-setting bodies decide the future governance of the Metaverse, and what lessons we can learn from similar past and current experiences of governance bodies led by industry players, standard-setting bodies and governments. We then provide our policy recommendations and conclusion.

I. A Human-Centric Approach to Interoperability

Interoperability is the ability to interact, exchange, and use data to enable movement, transactions, and participation across systems, platforms, environments, and technologies.[20] Interoperability will be an essential aspect of XR governance and presents a huge opportunity to advance a human-centric approach to the Metaverse's governance. Interoperability provides several benefits to users of the XR space, including the potential for a centralized experience,[21] the persistency and transferability of assets and user identities across the XR space,[22] efficient expansion,[23] and greater inclusion across XR platforms.

At the same time, enhancing users' experience across the XR ecosystem can open XR companies to future growth and innovation, allowing this technology to reach its full, seamless, and interconnected potential.[24] Interoperability standard-setting is also a good place to start in the mission of establishing strong XR governance approaches because it is considered less intrusive than other regulation methods and is well-suited to digital business models and evolving technology.[25] Furthermore, interoperability standards can foster a public interest approach to XR by helping ensure that users are not confined to

---

[19] George Lawton, *Metaverse Interoperability Challenges and Impact,* Techtarget (Mar. 7, 2024), https://www.techtarget.com/searchcio/tip/Metaverse-interoperability-challenges-and-impact [https://perma.cc/3R4H-GQVX].

[20] Cathy Li Et Al., World Econ. F., Interoperability In The Metaverse 5 (2023).

[21] *See* Accenture Fed. Servs., Government Enters The Metaverse: Four Trends Reshaping Government For The Metaverse Continuum 18 (2022).

[22] *Id.*

[23] Fiona M. Scott Morton et al., *Equitable Interoperability: The "Supertool" of Digital Platform Governance*, 40 Yale J. Regul. 1013, 1015 (2023).

[24] Lawton, *supra* note 19.

[25] Morton et al., *supra* note 23, at 1015.

one XR platform, with limited access, movement, and autonomy in the digital world.[26] To have a true XR universe, there cannot be completely disconnected sub-universes and ecosystems; rather, the XR space needs to be developed with compatibility in mind.

To achieve the goal of a fully immersive and frictionless Metaverse, interoperability standards should be adopted as early in the overall XR-universe development as possible. Enacting interoperability standards later on will probably increase governance costs and slow compatibility. Other adverse effects include the ongoing exclusion of marginalized communities, the further stratification of XR, and a decreased willingness to collaborate as companies become more incentivized to raise network effects on their own XR platforms rather than foster the growth of XR generally. Many of these problems, already present in Web 2.0, are addressed by existing interoperability rules that will also apply to the XR space.

A. Existing Legal Frameworks

The European Union has advanced its interoperability goals for the current digital space through rules included in the General Data Protection Regulation (GDPR) and the Digital Markets Act (DMA). The first of these regulations includes the right to data portability as one of the GDPR-granted individual rights.[27] This right allows users to reuse the data they provide to platforms across IT environments without affecting usability.[28] While this right does not create an obligation for data controllers to adopt or maintain technically compatible processing systems, recital 68 of the GDPR encourages the development of interoperable formats that enable data portability.[29] Since technically compatible systems should reduce the cost of complying with data portability, the GDPR serves as the first strong incentive for XR companies to develop interoperable systems within the Metaverse.

The DMA's protocol interoperability mandates are another strong starting point for evaluating interoperability and its feasibility in the XR space.[30] In an effort to tackle the market power of the main tech companies, the DMA specifically applies to a number of "gatekeeper" platforms — among them Apple, Google, Meta, and Microsoft — which also have the potential to serve as gatekeepers in the XR space.[31] These rules mandate that large tech companies be vertically interoperable with third-party applications and horizontally interoperable between competing interpersonal communication services. The act also establishes that gatekeepers cannot take any action that would undermine

---

[26] *What Are the Challenges to Building an Interoperable Metaverse?*, XR Today (July 5, 2022), https://www.xrtoday.com/virtual-reality/what-are-the-challenges-to-building-an-interoperable-metaverse/ [https://perma.cc/93WD-AQ5Y].

[27] 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) [hereinafter GDPR], art. 20, OJ 2016 L 119/1.

[28] *Right to Data Portability*, Info. Comm'r Off., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-data-portability/ [https://perma.cc/T86L-6XQ9].

[29] GDPR, recital 68.

[30] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [hereinafter DMA], OJ 2022 L 265/1. Note that while the DMA includes a precise definition of "interoperability" which refers only in the context of protocol interoperability, our use of the term in this chapter is intended to be understood more broadly.

[31] Mitch Stoltz et al., *The EU Digital Market Act's Interoperability Rule Addresses an Important Need, But Raises Difficult Security Problems for Encrypted Messaging*, Elec. Frontier Found. (May 2, 2022), https://www.eff.org/deeplinks/2022/04/eu-digital-markets-acts-interoperability-rule-addresses-important-need-raises [https://perma.cc/2HXP-L53Y].

interoperability, and it encourages them to rely on technical standards to achieve interoperability.[32] Additionally, Article 7 of the DMA states that "end users . . . shall remain free to decide whether to make use of the interoperable basic functionalities that may be provided by the gatekeeper."[33]

According to proponents of these rules, their benefits are many-fold, and they stem from a human-centric approach. First, users benefit from interoperability by being empowered to escape the confines of one platform and move to another without having to start from scratch. In addition, once users are more easily able to switch platforms, the platforms are motivated from a business perspective to improve the online user experience, rather than merely relying on network effects to carry them forward.[34]

The DMA sparked initiatives such as a new data portability project through the Google Takeout service to allow Google's Android users to move data out of Google services, Apple's allowance of third-party marketplaces to distribute iOS apps, and Microsoft's giving its users the ability to disable its default Bing web search.[35] This demonstrates that even the Big Tech platforms, when given specific requirements and timelines for complying, are able to take steps toward the greater goal of achieving interoperability.

Despite these advances, considering that the DMA was not crafted with the unique characteristics of XR in mind, its practical implementation within the XR space is still uncertain. Beyond the technical challenges of applying interoperability rules, which could face new and further challenges in the 3D virtual spaces, most of the designated gatekeepers' core platform services under scrutiny by the European Commission (EC) are those operating in the current 2D digital space.[36] In the near term, the dominant players will likely take advantage of the EC' focus on the 2D space to introduce restrictive compatibility requirements in the XR space. For example, Meta currently only offers the full immersive experience of its platform to users with one of the company's Oculus VR Headsets.[37]

Furthermore, although GDPR's and DMA's rules should incentivize XR companies to set third-party-accessible vertical interoperability and data portability standards from the outset, these types of mandates can only enable a partial degree of interoperability. As the United Kingdom's Office of Communications (Ofcom) noted, the highest degree of interoperability can only be achieved through the widespread adoption of open and common technical standards.[38] To achieve a truly interoperable Metaverse, these standards should promote horizontal interoperability across the entire XR ecosystem and not just provide a partial solution for specific services within the XR space.

Finally, while the GDPR and DMA apply to companies based outside the EU as long as they offer goods and services to individuals in the EU, most XR companies are still based in the United States, where

---

[32] *See* DMA.

[33] *Id.*

[34] *Id.*

[35] *The EU's New Competition Rules are Going Live — Here's How Tech Giants are Responding,* Verge (Mar. 6, 2024), https://www.theverge.com/2024/3/6/24091592/eu-dma-competition-compliance-deadline-big-tech-policy-changes [https://perma.cc/6AKF-YJC8].

[36] *See Gatekeepers,* Euro. Comm'n, https://digital-markets-act.ec.europa.eu/gatekeepers_en [https://perma.cc/S8KR-JNLD].

[37] Antonio Lopes dos Santos, *Roaming the Metaverse Under a Digital Market Lens,* whatnext.law (Mar. 9, 2023), https://whatnext.law/2023/03/09/roaming-the-metaverse-under-a-digital-market-lens/ [https://perma.cc/8SSX-BQDU].

[38] Ofcom, Mandated Interoperability in Digital Markets (2023), https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/economic-discussion-papers-/discussion-paper-mandated-interoperability-in-digital-markets/?v=330343 [https://perma.cc/YD85-388J].

there are no mandatory interoperability rules at a federal level. The California Consumer Privacy Act (CCPA) and other state laws include a similar data portability rule as the GDPR,[39] but they don't mandate horizontal interoperability. Bills like The Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act have attempted to incorporate interoperability mandates in the US.[40] Notably, the ACCESS Act requires the National Institute of Standards and Technology (NIST) to develop technical standards to make covered platforms interoperable.[41] This is a noteworthy starting point as it relies on governmental intervention in the standard-setting process to ensure that interoperability standards are embedded in the platforms' architecture. However, it is still uncertain whether these kinds of efforts will reach a political consensus.

Considering the shortcomings of existing interoperability regulations, as proposed below, their enforcement should be complemented by governments' oversight and involvement in the technical standard-setting process. To achieve this, the below types of interoperability and their individual challenges must first be considered.

B. Interoperability Goals in the Metaverse

Interoperability standards in the XR space should focus on three main opportunities: technical, usage, and jurisdictional.[42] Taken together, these opportunities encompass the XR space, supporting image rendering, artificial intelligence, the import and export of asset formats, tool usage, and authoring activities.[43]

Technical Interoperability

Technical interoperability, or the ability to build a frictionless experience across XR ecosystems,[44] focuses on networks, asset ownership, intellectual property, payment, identity, data privacy, and security.[45] This type of interoperability is especially important to enable an open and seamless experience within the Metaverse because it ensures compatibility of standards across the XR space.[46] Technical interoperability standards will help build knowledge networks, encourage innovation, promote integration between the physical and digital world, and facilitate digital twins (virtual representations of physical objects).[47] Some open standards are already being used in the XR space, such as Open XR and Web XR for rendering, WASM for portable code formatting, and VRM as a file format for virtual avatars.[48]

However, because data is at the center of this type of interoperability, privacy concerns could conflict

---

[39] *What Rights Do Consumers Have Under the CCPA?,* Bloomberg L. (May 3, 2023), https://pro.bloomberglaw.com/insights/privacy/what-rights-do-consumers-have-under-the-ccpa/ [https://perma.cc/S5PY-4SRV].

[40] H.R. 3849, 117th Cong. (1st Sess. 2021).

[41] *Id*

[42] Li et al., *supra* note 20, at 4.

[43] Lijuan Yang, *Recommendations for Metaverse Governance Based on Technical Standards*, 10 Humans. & Soc. Sci. Commc'n 1, 4 (2023).

[44] Li et al., *supra* note 20, at 12.

[45] *Id.*

[46] Yang, *supra* note 43, at 3.

[47] *Id.* at 4.

[48] *Id.* at 6.

with the ambition of a frictionless experience in the Metaverse. For example, while a centralized authentication system could enhance users' experience in the XR space, some might want to remain anonymous within certain ecosystems or retain the possibility of having multiple identities and sharing different sets of information across the Metaverse. Thus, in its goal to support persistence and presence, technical interoperability will have to be balanced with existing privacy regulations and principles that may limit how much data and what type of information can be exchanged in the digital space.[49]

Usage Interoperability

Usage interoperability centers on the goal of an inclusive metaverse. It enables participation from various demographic groups while considering their human needs to develop standards that, for example, treat first-time users in the Metaverse differently than cybersecurity experts or are designed with inclusivity for wide-ranging groups in mind.[50]

From a human-centric perspective, this is one of the foundational interoperability standards to develop.[51] From the users' standpoint, one of the most important usage interoperability standards are identity frameworks. These standards should be developed with an understanding that XR users will want to control and maintain stable identities in virtual worlds while also having enough flexibility to adopt different identities. In this way, a human-centric approach should especially consider the importance of selective anonymity or pseudonymity.[52]

Another relevant aspect of usage interoperability includes encouraging and facilitating accessibility and user engagement in the XR space. Just as is required to develop digital engagement, XR engagement requires more than simply access to the technology. Users must have ongoing and meaningful access and should be presented with opportunities to learn how the technology operates and what it can do.[53]

One of the main challenges of incorporating inclusive interoperability into the Metaverse is that stakeholders involved in the standard-setting process must be broad enough to encompass people across a variety of cultural settings to ensure that the standards will truly facilitate a better human experience on XR platforms.[54] Creating an inclusive XR space requires input from technical policy and experiential experts who are living in or closely associated with the digital experience.[55] This will be essential considering that interoperability will inform the way that XR platforms work both in their own ecosystems and across ecosystems. Since "societal inequalities often morph into online marginalization,"[56] if marginalized voices that are not normally included in policy discussions are also excluded from XR discussions, they are at risk of losing access to the technology in detrimental ways.

---

[49] Li et al., *supra* note 20, at 13.

[50] *Id.*

[51] Megan Bradley & M. Fernanda Muñoz, *Making your "XRself" Yours in the Metaverse*, Tech Pol'y Press (May 1, 2024), https://www.techpolicy.press/making-your-xrself-yours-in-the-metaverse/ [https://perma.cc/QTZ9-2NYY].

[52] Li et al., *supra* note 20, at 15.

[53] *See* Chu-Yang Chang et al., *The Role of Digital Literacy in Augmented, Virtual, and Mixed Reality in Popular Science Education: A Review Study and an Educational Framework Development*, 27 Virtual Reality 2461 (2023).

[54] Li et al., *supra* note 20, at 13.

[55] Meg Young et al., *Toward Inclusive Tech Policy Design: A Method for Underrepresented Voices to Strengthen Tech Policy Documents,* 21 Ethics & Info. Tech. 89, 90 (2019).

[56] Inga Trauthig & Samuel Woolley, *Addressing Hateful and Misleading Content in the Metaverse,* 1 J. Online Trust & Safety 1, 11 (2023).

To avoid this, inclusivity must be integrated into the standard-setting process by having individuals from marginalized communities act as experiential experts — i.e., diverse stakeholders whose lives will be substantially impacted by the specific implementation of certain technologies — on community advisory boards and any other space where policy decisions are occurring.[57]

Jurisdictional Interoperability

Jurisdictional interoperability focuses on XR's lawfulness and ensures that XR platforms operate within and across jurisdictions while conforming to different regulatory requirements.[58] This requires global cooperation to create global standards — both in the sense of requiring all platforms to be involved and in the sense of needing to transcend boundaries.[59] Creating and maintaining jurisdictional interoperability can foster a safer metaverse for all users by creating a better understanding of what "order" looks like in the digital world.

However, jurisdictional interoperability cannot be achieved without recognizing that regulations in the online space are pluralist, with governments lacking some of the power they traditionally wield. With the current profit-driven configuration of the XR space, the interaction between the government, online citizens/users, and digital platforms in the Metaverse may shift even more than the already-established evolution of governance responsibilities that accompanied the growth of social media. As Jack Balkin noted, there is now a "privately owned infrastructure of digital communication composed of firms that support and govern the digital public sphere."[60] While Balkin's argument is focused on free speech rights, it translates to a range of other freedoms and liberties, such as the right to education, to work, to healthcare, and to freedom of association, and is especially profound in the world of immersive technology.[61] Thus, jurisdictional interoperability will be an important component and a facilitator of the interaction between government, citizens, and the platforms that are building the Metaverse.

Some argue that shifting the governance role from State actors to industry and the platforms has some benefits, especially because governments are often not agile enough in assessing the challenges and potential of quickly evolving technologies.[62] Lobbying has been an important component in why immersive technologies are even on the radar of policymakers in the first place. The work of lobbying groups, such as the XR Association (XRA),[63] demonstrates how the industry can affect governmental decision-making. XRA successfully educated lawmakers on XR and its role in the technology ecosystem, resulting in "immersive technology" being a category added to the Endless Frontier Act, which was then incorporated into the CHIPS bill to encourage investment in research and development for emerging technologies.[64]

While there are benefits to giving platforms some deference, there are also risks that suggest a need

---

[57] Young et al., *supra* note 55, at 90.

[58] Li et al., *supra* note 20, at 14.

[59] Yang, *supra* note 43, at 7.

[60] Jack M. Balkin, *Free Speech is a Triangle,* 118 Colum. L. Rev. 2011, 2012 (2018).

[61] *See* Michael Karanicolas, *Understanding the Internet as a Human Right,* 10 Can. J.L. & Tech. (2012).

[62] Sam Sprigg, *Why Governments and Policymakers are Key to the XR Industry's Growth*, AWE (Aug. 18, 2022), https://www.awexr.com/blog/why-governments-and-XR-industry-should-work-together [https://perma.cc/C375-PFG4].

[63] XRA, https://xra.org/ [https://perma.cc/R436-7ZRN].

[64] *CHIPS and Science Act of 2022,* XRA, https://xra.org/public-policy/us-innovation-and-competition-act/ [https://perma.cc/D9TU-UR4U]; Sprigg, *supra* note 62.

to ensure that the Metaverse's governance rests in the hands of citizen users or governments rather than concentrating it on a handful of platforms with their own business priorities, which may not align with those of their users or of the public at large. In fact, some jurisdictions have already started working on general guidelines to influence the future of XR governance vis-à-vis tech companies. Acknowledging its active role in shaping the future trajectory of the Metaverse, the EU has delineated several principles based on a human-centric approach in its Strategy to lead on Web 4.0 and Virtual Worlds. According to this strategy, one way to achieve jurisdictional interoperability is for stakeholders to develop regulatory sandboxes, which include creators, users, and media companies.[65] These types of sandboxes have proven to foster innovation, consumer protection, and regulatory certainty with regard to other digital spaces and can deliver the same benefits for XR.[66]

Finally, it is worth highlighting that although technical and usage interoperability goals will be pivotal for the Metaverse's governance, they can also undermine other equally important goals, like privacy and safety.[67] In fact, one of the benefits of "walled garden" systems is that they can create "idiosyncratic user experiences within controlled environments that can be optimized by a defined group of stakeholders."[68] For example, a completely frictionless Metaverse could expose children to elements from XR ecosystems built for adults, such as appearances and assets from combat games, that might not be suitable for children.[69] As seen with technical interoperability, users can also benefit from exercising control over the type and amount of information they share with different applications and actors within the Metaverse, creating a tension between interoperability and privacy.[70]

Stakeholders can still foster goals like privacy and safety through jurisdictional interoperability by agreeing on common enforcement mechanisms and policies, reducing the number of resources needed to build individual solutions, and securing a continuous, safe, and private space.[71] The right interoperability formula for the Metaverse will depend on the interplay between these different goals.

Whether mandated by legislation or not, the complexities of interoperability will, in whole or in part, be determined by the technical standards developed by the stakeholders to meet these different goals, so it is equally important to address how these standards are going to be set. Below we address the challenges of achieving an interoperable Metaverse through technical standards and standard-setting initiatives.

---

[65] European Commission Press Release IP/23/3718, Towards the Next Technological Transition: Commission Presents EU Strategy to Lead on Web 4.0 and Virtual Worlds (July 11, 2023).

[66] Sharmista Appaya & Mahjabeen Haji, *Four Years and Counting: What We've Learned From Regulatory Sandboxes,* World Bank Blogs (Nov. 18, 2020), https://blogs.worldbank.org/en/psd/four-years-and-counting-what-weve-learned-regulatory-sandboxes [https://perma.cc/7WHN-2AYK].

[67] Li et al., *supra* note 20, at 7.

[68] Adrian Kuenzler & Dylan Reim, *Metaverse Interoperability is Essential. How Will Regulation Play a Part?,* World Econ. Forum (Aug. 6, 2024), https://www.weforum.org/agenda/2024/08/metaverse-interoperability-regulation/ [https://perma.cc/LJN9-MKXR].

[69] *Id.*

[70] *Id.*

[71] Li et al., *supra* note 20, at 9.

II. Governance through Technical Standards

Technical standards may be defined as "a set of norms, requirements or features of a technology, process, or method."[72] Standards provide the basis for the functioning of most of the technologies we use every day, and for the Metaverse, they will be essential to reach the aspiration of interoperability and openness across interconnected virtual worlds.

Due to its need to integrate different virtual worlds, the Metaverse will be more dependent on technical standards than previous technologies. Standards will be key in enabling aspects that will inform users' Metaverse experience, such as user identity, social relations, and digital asset ownership.[73] However, because these technical standards are yet to be determined, "the current technical conditions are still the threshold for entering the metaverse."[74] Thus, to realize an ecosystem of interconnected virtual worlds, XR actors will first need to develop clarity regarding the technical standards that will establish the Metaverse architecture.[75]

As the code-as-law of the Metaverse, technical standards provide several benefits that other modalities of regulation cannot offer because of their inherent limitations. Technical standards can constrain users' behavior without the complexity of legal rules. Moreover, unlike traditional legal frameworks, technical standards are better placed to navigate the intricate challenges of designing, hosting, maintaining, and interacting with virtual worlds.[76]

As it stands now, the Metaverse behaves more like a fragmented technology that encompasses multiple proprietary systems rather than the one ecosystem envisioned to be open and interoperable.[77] The problem with a fragmented ecosystem — as is evident from Web 2.0 — is that users face switching costs that impede them from migrating to different providers, even if they feel dissatisfied with the platform they are in.

Ideally, under a human-centric approach to the Metaverse, we want technical standards to enable design choices that act as a countervailing power to the big tech companies' tendency to advance their own interests in the Metaverse's structural development. Because most of the fundamental decisions about the Metaverse's governance are taking place in the standard-setting processes governed by XR companies,[78] users, governments, and other relevant stakeholders should intervene early on in these spaces to incorporate the public good in the Metaverse's architecture.

---

[72] McStay, *supra* note 2.

[73] Yang, *supra* note 43, at 3–4.

[74] *Id.*

[75] *Id.* at 7.

[76] McStay, *supra* note 2.

[77] Melodena Stephens, The Ieee Global Initiative on Ethics of Extended Reality (Xr) Report: Metaverse and Its Governance (2022).

[78] McStay, *supra* note 2.

III.Standard-Setting Initiatives

To achieve a human-centric approach to the Metaverse, it is essential that technical standards are created in pluralistic spaces that include the voices of diverse stakeholders beyond just the companies.[79] Standards-setting bodies should be structured to enable meaningful participation and decision-making by stakeholders other than the main tech players. Greater inclusion in the standard-setting process would also benefit the platforms, providing them with greater legitimacy and user appreciation.[80]

The following discussion highlights three different governance initiatives related to the XR space or developed for existing digital platforms that could shed light on XR governance. One was taken by an industry player, one by an industry forum, and one by the European Commission. Each of these initiatives has presented benefits and downfalls, so the examination of their results can inform how standard-setting processes and governance initiatives, in general, should be addressed in the XR space both via stakeholder participation and government intervention.

Facebook's Oversight Board

When it was created in 2019, Facebook's (now Meta's) Oversight Board was a huge step in the industry. Amid backlash for its content moderation decisions and their implications on human rights, the Oversight Board began because of a unilateral order from CEO Mark Zuckerberg, as a public mechanism of accountability around the company's decision-making. himself.

Other voices within Facebook's corporate board were less convinced of the wisdom of the Oversight Board, voicing concerns that it would inhibit Facebook's business interests.[81] In the XR space, the same types of objections will likely appear in response to calls for a human-centric approach to the Metaverse, which prioritizes users' needs before companies' bottom lines.

The Oversight Board was conceptualized as Facebook's own "Supreme Court", a corporate tribunal with no modern equivalent.[82] Still, questions about how powerful it should be arose immediately.[83]Ultimately, when it was created, Facebook enabled the Oversight Board to hear cases involving takedowns but placed restrictions on its power.[84] From the beginning, Facebook's ability to curb the powers of the board was a target of criticism from observers who claimed its decisions would be biased in the company's favor.[85]

Despite stating that the Board would be independent of Facebook, Mark Zuckerberg edited and changed the Board's charter and bylaws to make them "more approachable."[86] Additionally, Facebook was able to choose the initial members of the Board, though subsequent members were chosen independently.

---

[79] Thomas A. Hemphill, T*he 'Metaverse' and the Challenge of Responsible Standards Development,* 10 J. Responsible Innov. 1, 5 (2023).

[80] *Id.*

[81] Kate Klonick, *Inside the Making of Facebook's Supreme Court,* The New Yorker (Feb. 12, 2021), https://www.newyorker.com/tech/annals-of-technology/inside-the-making-of-facebooks-supreme-court.

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] *Id.*

While they were allowed to choose the rest, some experts cautioned against this approach because it would result in them picking "more people that look like them."[87]

The Oversight Board has its proponents, but it also demonstrates the limits of governance standards that are entirely in the hands of the companies that are being subject to them. Despite key differences in the technologies, XR shares much in common with the social media space, including a number of the same dominant players. Meta has a large and important role in informing the development of XR ecosystems, and while it might be willing to create an oversight committee or technical standards-setting bodies for the Metaverse, failing to develop a uniquely independent body will come at the cost of advancing cohesive and interoperable XR policies.

Another ongoing concern about membership on the Oversight Board is a belief that the Board isn't representative of, or doing enough to serve, the vulnerable communities that are often the subject of its decisions.[88] This is another serious critique that must be addressed in any effort to create a similar governing board for the XR space. This underscores why calls for a governing board in the XR space that takes a human-centric approach and is not solely composed of industry members will be beneficial.

Despite concerns about the Oversight Board's efficacy, it nonetheless presents an intriguing model for the future of XR governance, particularly as it contemplates engaging with companies other than Meta. One of the Board's members has stated that the Board is "seeking to understand how we might interrelate with other companies" and "interact with companies setting up different types of councils or bodies to talk about standards."[89] This type of momentum and willingness to work together across company boundaries should encouraged for XR. However, the industry should also consider the importance of governance structures which are fully multistakeholder, as opposed to operating under the auspices of a single industry player.

The Metaverse Standards Forum

The Metaverse Standards Forum is a group of industry stakeholders that aims to encourage the development of interoperability standards in the XR space. The forum does not create standards but fosters the conversations necessary to forge them between different existing standard-setting bodies.[90] The forum's membership is highly technical and largely informed by corporate interests. It is composed of over 2,400 standards-related organizations, companies, and institutions and includes some of the major XR players, such as Google, Meta, and Microsoft.[91] Importantly, one of the forum's goals is to work with organizations, such as the World Wide Web Consortium and the Khronos Group, to make decisions about how existing standards can be adjusted to address user experience in the XR space.[92]

---

[87] *Id.*

[88] Corynne McSherry & Jillian C. York, *Facebook's Oversight Board: Who (and What) Is Missing From the Picture So Far,* Elec. Frontier Found. (May 20, 2020), https://www.eff.org/deeplinks/2020/05/facebooks-oversight-board-lacks-appropriate-representatione [https://perma.cc/6W3L-7E9V].

[89] Steven Levy, *Inside Meta's Oversight Board: 2 Years of Pushing Limits,* WIRED (Nov. 8, 2022), https://www.wired.com/story/inside-metas-oversight-board-two-years-of-pushing-limits/ [https://perma.cc/QJ26-P39V].

[90] Ben Egliston et al., *Who Will Govern the Metaverse? Examining Governance Initiatives for Extended Reality (XR) Technologies,* 0 New Media & Soc'y 1, 13 (2024); *see also Join the Forum,* Metaverse Standards F., https://metaverse-standards.org/members [https://perma.cc/94RQ-2TQY].

[91] *Join the Forum, supra* note 92.

[92] Lawton, *supra* note 9.

The forum operates through a series of working groups with distinct focuses, such as the interoperable characters/avatars group, the 3D asset interoperability group, the industrial metaverse interoperability group, and the ethical principles in the metaverse group.[93] These working groups are pragmatic ways to deal with all the different components of the Metaverse and provide an opportunity to fill interoperability gaps.[94]

This type of standard-setting structure offers its own benefits. It promises to build trust and collaboration between forum members, facilitating a more likely pathway for them to set interoperability standards and achieve a cohesive XR ecosystem. It also provides a space for large XR companies to interact with other relevant stakeholders while having their commercial interests heard.[95]

While forums like this are undeniably meaningful, there is a risk that the voices heard within the forum, despite its large membership size, are mainly those of the major platforms. Although collaboration among the major platforms should be encouraged, the vision of a human-centric metaverse will not be achieved solely by this action. The forum should actively encourage greater diversity in its members, including additional stakeholders affected by decisions made concerning XR.[96] Because the power already held by the major players in the XR space is unlikely to be balanced by the sole involvement of individual stakeholders like members of civil society and academia, democratic governments should also intervene and, when appropriate, try to lead decisive standard-setting processes.

The European Commission

The European Commission has taken various steps to facilitate the development of XR standard-setting. First, at the beginning of 2023, the Commission introduced the Gigabit Infrastructure Act to recognize the need for more flexible and innovative digital services for EU citizens in the face of new technologies like the Metaverse.[97] The Act was approved at the beginning of 2024 and will soon become law in the EU.[98] This Act is inherently human-centric in its approach since one of its main purposes is to ensure meaningful access to digital networks.

After proposing the Gigabit Infrastructure Act, the European Commission also announced the EU's strategy for Web 4.0 and virtual worlds to "ensure an open, secure, trustworthy, fair and inclusive digital environment for EU citizens, businesses, and public administration."[99] The plan is designed as a series of strategic pillars, one of which is: "Shaping global standards for open and interoperable virtual worlds and Web 4.0."[100] This pillar specifically focuses on preventing a few major players from dominating the market and setting standards that will grant themselves a first-mover advantage. To achieve this, the European Commission plans to engage with internet governance stakeholders around

---

[93] *Active Domain Groups,* Metaverse Standards F., https://metaverse-standards.org/domain-groups/ [https://perma.cc/QP3U-NNWT].

[94] Hemphill, *supra* note 79, at 4.

[95] Michael Koziol, *The Metaverse Needs Standards, Too,* IEEE Spectrum (Aug. 31, 2022), https://spectrum.ieee.org/metaverse-standards-forum [https://perma.cc/T7NS-DJXD].

[96] Hemphill, *supra* note 79, at 5.

[97] European Commission Press Release IP/23/985, Commission Presents New Initiatives, Laying the Ground for the Transformation of the Connectivity Sector in the EU (Feb. 23, 2023).

[98] *Gigabit Infrastructure Act,* Eur. Comm'n, https://digital-strategy.ec.europa.eu/en/policies/gigabit-infrastructure-act [https://perma.cc/3XU2-34MY].

[99] European Commission Press Release IP/23/3718, *supra* note 65.

[100] *Id.*

the world to promote Web 4.0 standards in line with the EU's vision and values.[101]

The Commission's calls to action on this front include exploring a new European Partnership to develop an industrial and technological roadmap,[102] supporting the development of standards for open and interoperable virtual worlds,[103] promoting the use of virtual worlds regulatory sandboxes,[104] and bringing member states together to share best practices for the development of virtual worlds through an expert group.[105] By explicitly considering the public good in the standard-setting process, we consider this pillar to be fundamental for a human-centric approach to the Metaverse's governance. At the same time, this initiative demonstrates that governments can participate actively in the debate about the Metaverse's standard-setting process and that an approach which defers entirely to industry is not inevitable.

IV. Recommendations and Conclusions

With companies investing more and more in XR technologies and users' and governments' increasing willingness to populate the XR space, the stakes are high that XR technologies may have a huge impact on the socio-economic domain. While many companies profess their commitment to an open and interoperable XR ecosystem, the reality is that the technology is being developed as a fragmented space in which the proprietary interests of companies are prioritized.

A human-centric approach to the Metaverse's governance should reflect the interests of companies, users, and governments by enabling an open and interoperable Metaverse. To achieve this, the following recommendations should be considered.

1. **The need for open and common technical standards.**

    a. The Metaverse's early architecture should enshrine robust interoperability standards which allow the XR ecosystem to develop with a user-focused approach.

    b. The GDPR's data portability rules and the DMA's interoperability mandates are noteworthy starting points for incorporating interoperability in this space. However, the highest degree of interoperability can only be achieved through the widespread adoption of open and common technical standards.

    c. To achieve the highest degree of interoperability, the focus must be on developing open technical standards that promote horizontal interoperability across the entire XR ecosystem rather than just facilitating third-party vertical interoperability.

    d. These standards should at least consider ways to achieve three relevant types of interoperability: technical interoperability, usage interoperability, and jurisdictional interoperability.

---

[101] *Id.*

[102] Eur. Comm'n, An Eu Initiative on Virtual Worlds: A Head Start in the Next Technological Transition 12 (2023).

[103] *Id.*

[104] *Id.*

[105] *Id.*

2. **Governmental intervention in the standard-setting process.**

    a. GDPR- and DMA-style rules should be complemented with governmental oversight and intervention in standard-setting processes to ensure that interoperability standards are embedded in the Metaverse architecture.

    b. In the U.S., this idea has been incorporated in the proposed ACCESS Act through the participation of NIST in the interoperability standard-setting process for existing digital platforms. However, if the technical complexities of the XR space make the government's identification and development of interoperability standards unfeasible, a more mixed approach could also be considered.

    c. The European Commission's plan to engage with Internet governance stakeholders around the world to promote interoperability standards for virtual worlds and to encourage the use of regulatory sandboxes could be a more collaborative approach that will enable governments to work with companies in the standard-setting process. This alternative could allow governments to oversee the standard-setting process while leveraging the technical expertise of XR companies.

    d. Standard-setting processes should also ensure that integrate inclusivity by having individuals from marginalized communities act as experiential experts on community advisory boards and any other space where policy decisions are made.

3. **Enforcement of existing laws.** While GDPR's and DMA's interoperability rules will not be enough to secure a full degree of interoperability in the Metaverse, these types of regulations should continue to be enforced and updated to apply appropriately to virtual worlds. For example, DMA's designated core platform services should be updated to include services specifically related to the XR. At the same time, self-preferencing actions by companies should not only be considered under specific interoperability legislation but also by applicable antitrust laws.

4. **Interoperability vs Privacy and Security.** When developing technical standards for the Metaverse, interoperability should be balanced with other equally important goals (i.e. privacy and safety). For example, to protect privacy, users could be given control over the type and amount of information they can share with different applications and actors within the Metaverse. Users should also be given the opportunity to maintain stable identities in virtual worlds while having enough flexibility to adopt different identities. To promote safety, some elements of the Metaverse, such as appearances and assets from adult spaces, should be excluded from child-friendly spaces.

XR and the Digital Citizen

Megan Bradley
Maria Fernanda Muñoz
Elizabeth Mzungu
Chen Yan

Introduction

The immersive and interactive features of XR technology have the potential to act as a powerful tool for individuals to interact with each other and for society to pursue democracy more effectively. Policymakers should seize the opportunities of XR to democratize social and political participation by opening spaces for citizens, democratic entities, states, cities, and local communities to engage with each other in the metaverse.

However, many factors could hinder these goals, including resistance to change, lack of knowledge about XR technologies, digital exclusion of marginalized groups, the fear that authoritarian states could manipulate virtual environments, and the lack of transparency of platform operators' design of environments and governance choices.

These promises and concerns are similar to those associated with social media platforms like Twitter and Facebook. While these platforms promote citizen engagement with matters of public importance, they also unleash problematic types of speech, including hate, exclusion, and disinformation.[1] This has been enabled in part by growth-oriented strategies adopted by the leading tech players, and the power structures within these companies.[2] Governance which is guided by pure commercial interests tends to disfavor vulnerable groups, since they are more likely to be marginalized from digital spaces, with limited access or ability to influence decision-making processes of tech companies. Negative externalities caused by a growth-oriented strategy also tend to be externalized across the public at large, and marginalized groups in particular, as opposed to within tech companies.

Considering XR's revolutionary power, it is important for the different players in the XR space to incorporate mechanisms that address the harms of the previous generation of innovation and prevent problems of greater magnitude from embedding themselves in the technological governance ecosystem. Achieving a democratic and inclusive metaverse requires a more democratic governance model, including robust citizen engagement and bottom-up decision-making structures both inside and outside the companies.

At the same time, as more governments enter the metaverse, it is expected that a meaningful part of citizen participation in this space will be through moves by State actors to provide public services and engage with their constituents through XR. The extent and quality of citizens' participation in XR-enabled public services will depend on how well governments manage to meet the needs of their constituents when using XR for service delivery.

---

[1] Jonas Fegert, *Virtual Realities, Real Participation. Challenges and Opportunities of Public Participation in the Metaverse,* Project Immersive Democracy (Nov. 13, 2023), https://www.metaverse-forschung.de/en/2023/11/13/virtual-realities-real-participation-challenges-and-opportunities-of-public-participation-in-the-metaverse [https://perma.cc/6W6M-TDVC].

[2] Hans Gersbach, *Democratizing Tech Giants! A Roadmap*, Econ. of Gov. 351, 352–361 (2020).

In this section, we explore how policymakers can foster citizen participation in the metaverse by seizing the opportunities and addressing the challenges of opening democratic spaces for citizens to engage with each other, democratizing governance structures within the XR space, and enhancing citizen engagement with public services provided through XR.

I. Citizen Engagement and Democracy in the XR Space

One of the main values of XR is its ability to provide people with virtual venues where they can meet and interact with one another. Interactions in the XR space are more immersive and thus feel more "personal" to the participants. For instance, there are many developers, such as Ministry XR, that provide venues for events that are purely virtual or hybrid.[3] Products like this make virtual public discussions and remote engagement feel more like an in-person event, opening up opportunities for deeper engagement.

However, meaningful citizen participation will only be possible if the virtual worlds that the metaverse opens are safe, inclusive, and democratic. In fact, research has shown that democratic discourse in digital spaces depends on "actively strengthening democratic actors and narratives."[4] Actions to suppress speech, especially by the State, should be a measure of last resort to stop malevolent actors. In this respect, the challenge of enabling citizen participation in the Metaverse bears some resemblance to existing debates around content moderation on social media.

Aside from providing venues, XR technology can also promote transparency and inform the public's decision-making. For instance, a city's zoning and construction decisions can be more understandable and accessible by displaying planning proposals or the results of previous projects in XR, making them open for the public to see and review.[5] One of the main challenges in enabling public participation in decision-making processes is "to create easy-to-understand visualizations as well as reliable and user-friendly feedback mechanisms."[6]

Immersive experiences can also help improve governance by fostering empathy among decisionmakers, and the public at large, by allowing people to observe and engage directly with other people's experiences. One example is the "Clouds Over Sidra" VR film, which was created in collaboration with the United Nations to allow viewers to experience the daily life of a Syrian girl living in a refugee camp.[7] These types of presentations can humanize abstract social problems, helping the public to understand why expenditure to help refugees, or other vulnerable groups, are necessary and important. Similarly, XR can be used to preserve and celebrate diverse ethnic identities, promoting cross-cultural engagement and understanding. For example, CyArk offers an XR experience where users can immerse themselves

---

[3] *Take Your Events Into the Metaverse,* Ministry XR, https://ministryxr.com/metaverse/ (last accessed May 8, 2024).

[4] Octavia Madeira & Georg Plattner, *A Safe Space for Everyone — a Plea for a Democratic and Participative Metaverse,* Project Immersive Democracy (Aug. 22, 2023) https://www.metaverse-forschung.de/en/2023/08/22/a-safe-space-for-everyone-a-plea-for-a-democratic-and-participative-metaverse/ [https://perma.cc/3L3M-5ACC].

[5] Ernest Chrappah, *Six Takeaways from the Augmented World Expo for a Future with Mixed Reality and Metaverse,* NYU Sch. Prof. Studs (June 13, 2023), https://www.sps.nyu.edu/homepage/metaverse/metaverse-blog/Six-Takeaways-from-the-Augmented-World-Expo-for-a-Future-with-Mixed-Reality-and-Metaverse.html [https://perma.cc/4ZFA-PKB3].

[6] Fegert, *supra* note 1.

[7] *Syrian Refugee Crisis,* U.N. Virtual Reality, https://unvr.sdgactioncampaign.org/cloudsoversidra/ [https://perma.cc/8EYS-AMC6].

in historical sites around the world spanning over 3000 years of human history.[8]

Using XR to foster empathy between citizens and cultures will also face limitations. As the XR world is constructed through selective summarization and reduction of reality, the effort to promote empathy sometimes results in reiterations of existing biases and overgeneralizations if done inadequately.[9] To address this challenge, policymakers should prioritize authentic representation and understanding of diverse experiences, thereby promoting empathy as a tool for social understanding and equity.

II. Democratizing Private Sector Governance in the XR Space

A human-centric approach to the Metaverse should empower individuals to participate in the decisions that govern the space in which they will play, work, and interact with each other. This entails constructing alternative governance mechanisms that give the individuals who will be most impacted by XR the power to influence how these technologies are developed and deployed. Some of these mechanisms may include voting systems, oversight councils, and tech workers' mobilization.

Voting Systems

One of the most straightforward ways to empower users and enable accountability is by creating systems to assess user sentiment on particular policy questions. This moves the governance dynamic beyond the current contract-based relationship between users and platforms by assigning a more proactive governance role to the users.[10] Voting and polling systems can be achieved through a selective pool of voters or by assembling "user councils" to offer inputs on policy questions.[11]

The XR space could lend itself to particularly intensive forms of user organization as it allows users to interact with each other in a more vivid and engaging way compared to traditional online platforms. User consultation and empowerment will also help developers to track emerging social harms that can be challenging to anticipate in the deployment of new technologies.

User Councils

Citizen engagement with the metaverse could also be fostered by user councils tasked with advising, guiding, and supervising XR governance decisions. As discussed in the interoperability section, Facebook has already experimented with establishing an oversight board, which "adjudicates" the hardest content moderation cases.[12] In 2019, Google also initiated its Advanced Technology External Advisory Council, or ATEAC, which provides the company guidance on how to ethically develop new technologies such

---

[8] *Explore Cultural Heritage in Virtual Reality*, CYARK (Feb. 4, 2020), https://cyark.org/about/blog/?p=case-study-8 [https://perma.cc/VA2K-DSCX].

[9] Dylan Fox & Isabel Guentte Thorton, IEEE, Extended Reality (Xr) Ethics and Diversity, Inclusion, and Accessibility (2023).

[10] *See, e.g.,* Stephen P. Mulligan & Chris D. Linebaugh, *Data Protection Law: An Overview,* Cong. Rsch. Serv. R45631 (Mar. 25, 2019), https://crsreports.congress.gov/product/pdf/R/R45631 [https://perma.cc/4YSP-MEYS].

[11] Hans Gersbach, *Co-voting Democracy,* Economics Working Paper Series, No. 16/256 , ETH ZURICH CER-ETH CTR. ECON. RSCH (Aug. 2016), https://www.econstor.eu/bitstream/10419/171699/1/wp-16-256.pdf [https://perma.cc/8F36-8JZA].

[12] Kate Klonick, *Inside the Making of Facebook's Supreme Court*, New Yorker (Feb. 12, 2021), https://www.newyorker.com/tech/annals-of-technology/inside-the-making-of-facebooks-supreme-court

as AI.[13] However, critics pointed out that the goals and responsibilities of the initiative were never made clear, and the council ultimately lapsed due to backlash against a controversial attendee.[14]

Both Facebook and Google's experiments in this space provide important lessons on how to organize alternative governance modes via oversight councils. Firstly, companies should give more transparency and clarity regarding the functions of the councils. The companies should clarify the council's goals, roles, responsibilities, and authorities, as well as consider their procedural and representation aspects clearly from the outset. Though some delegation of this work to the councils themselves may be beneficial, it is difficult for the participants to perform their function without first knowing the responsibilities and goals of the board itself. In the XR space, companies should attach greater significance and give more deference to councils' inquiries, perspectives, and expert opinions over the ethical and social implications of their products. Another important point is that the council should not consist only of scholars or high-profile figures. It is also necessary to include representatives of groups that are particularly vulnerable to harms that manifest through the deployment of XR technologies.

Employee Mobilization

Employees within XR companies are also important forces to help democratize decision-making because they are well positioned to understand the technical and social implications of the XR revolution.[15] Employees may mobilize and advocate for alternative community norms and solidarity with other social movements, striking a balance between social justice and technological advancement. Employee resistance and mobilization are not new in the tech sector. For instance, Googlers were active in pushing back against the Maven and Dragonfly projects, and Amazonians protested against a government contract to supply facial recognition technology for law enforcement.[16]

XR workers have begun to mobilize in this space, but their efforts face significant challenges.[17] In the U.S., where most of the XR companies are located, the current laws work to constrain employee activism, including only limited whistleblower protections.[18] The current wrongful termination laws still generally uphold employers' general right to terminate employment at will with very limited

---

[13] Bobbie Johnson & Gideon Lichfield, *Hey Google, Sorry You Lost Your Ethics Council, So We Made One for You,* MIT Tech. Rev. (Apr. 6, 2019), https://www.technologyreview.com/2019/04/06/65905/google-cancels-ateac-ai-ethics-council-what-next/ [https://perma.cc/PB99-DEVN].

[14] Nick Statt, *Google Dissolves AI Ethics Board Just One Week After Forming It,* Verge (Apr. 4, 2019), https://www.theverge.com/2019/4/4/18296113/google-ai-ethics-board-ends-controversy-kay-coles-james-heritage-foundation [https://perma.cc/B7LF-HWV7]. The actual effect of outside councils' approach remains unclear to the scholars. *See, e.g.,* Michael Veale et al., *AI and Global Governance: Modalities, Rationales, Tensions,* 19 Ann. Rev. L. & SOC. SCI. 255 (2023).

[15] *See, e.g.,* Hannah Bloch-Wehba, *Algorithmic Governance From the Bottom Up,* 48 BYU L. Rev. 69 (2022).

[16] *See, e.g.,* Jay Greene, *Amazon Bans Police Use of Its Facial-recognition Technology for a Year,* Wash. Post (June 10, 2020), https://www.washingtonpost.com/technology/2020/06/10/amazon-rekognition-police/; *see also* Ben Tarnoff, *Tech Workers Versus the Pentagon* (June 6, 2018), https://jacobin.com/2018/06/google-project-maven-military-tech-workers [https://perma.cc/ZC7P-7HKZ].

[17] *See, e.g.,* XR INCLUSION, https://xrinclusion.org/about/ [https://perma.cc/HJ3R-3JX8].

[18] *Federal Employee Speech & the First Amendment: A Know-Your-Rights Guide,* ACLU, https://www.acludc.org/sites/default/files/field_documents/free_speech_fed_employees_kyr.pdf [https://perma.cc/FLG9-RE28].

exceptions, including firing employees because of their advocacy and political views.[19] Employee speech protections are very limited, and it is likely that employee advocacy against product development decisions causing social harm might lead to their dismissal.[20]

The absence of unions across most of the tech sector also leaves workers vulnerable to being discharged in response to raising ethical concerns.[21] Many software engineers, data analysts, and product managers are foreign hires, working under the H-1B visa scheme which leaves them further subject to the whims of employers.[22]

A final obstacle concerns the lack of diversity in the tech sector, including a disproportionately low percentage of female tech workers and the underrepresentation of Latino and African American workers.[23] The absence of these groups limits the representative nature of employee mobilization efforts, since for many companies their user base will be very different from the workforce that is building the products.

III. Government Services in the Metaverse

XR provides immense opportunities to improve governments' efficacy in service delivery and expand e-governance capacity. The Metaverse's immersive and interactive features promise to enable personalized public services that meet citizens' unique preferences, foster a sense of community, and create new, meaningful ways for citizens to engage with public services.[24] To maximize the potential of XR to improve e-governance, governments need to adapt existing regulatory and governance tools to maximize XR's benefits while avoiding the risks that could hinder citizen engagement with government services and the XR space as a whole.

Human-Centered Public Service Delivery

In 2023, the XR Association and the Digital Trade and Data Governance Hub reported that a number of different countries, including the governments of the United States, South Korea, the United Kingdom, the European Union, and China, are already investing resources in research and development around

---

[19] Charlotte Garden, *Was It Something I Said? Legal Protections for Employee Speech,* Econ.. Pol'y Inst. (May 5, 2022), https://www.epi.org/unequalpower/publications/free-speech-in-the-workplace/ [https://perma.cc/QG3G-RQED].

[20] Labor Board v. Electrical Workers, 346 U.S. 464, 468 (1953).

[21] *See, e.g., Why is Tech so Anti Union?,* Reddit, https://www.reddit.com/r/bayarea/comments/10jtjoq/why_is_tech_so_anti_union/ (last visited Apr. 9, 2024).

[22] *Tech Companies Hiring the Most H-1B Workers*, Boundless (Dec. 13, 2023), https://www.boundless.com/blog/tech-companies-hiring-h-1b-workers [https://perma.cc/4HCS-AELN].

[23] Sarah K. White, *Women in Tech Statistics: The Hard Truths of An Uphill Battle,* CIO (Mar. 8, 2024), https://www.cio.com/article/201905/women-in-tech-statistics-the-hard-truths-of-an-uphill-battle.html; Atopia, *Who's Really Using VR these days? Six Data-Driven Insights Into Today's VR User Demographic,* Medium (Oct. 11, 2023), https://medium.com/@annabell_37704/whos-really-using-vr-these-days-six-data-driven-insights-into-today-s-vr-user-demographic-422372a75c8c#:~:text=Nearly%20half%20of%20VR%20users,t%20far%20behind%20at%2040%25 [https://perma.cc/3LKE-WHTV].

[24] Martin Lnenicka et al., *Government in the Metaverse: Requirements and Suitability for Providing Digital Public Services,* 203 Technol. Forecast. Soc. Change 1, 9 (2024).

immersive technology and human-machine interfaces.[25] For example, the Government of South Korea has implemented Metaverse Seoul, the world's first urban metaverse app. This immersive platform allows users to embark on a virtual journey through Seoul's iconic landmarks, participate in civic activities such as paying taxes or filing civil complaints, and facilitate interactions with other metaverse residents.[26]

The Risks of Adopting XR for Public Services

While the use of XR for public service delivery carries significant potential value, there are also risks and hurdles. First, governments may face public skepticism and resistance to using emerging XR platforms to serve and engage with citizens.[27] Studies have identified several reasons for users to resist the adoption of XR generally, including lack of understanding, lack of regulation, nausea, claustrophobia, loss of social ties, disconnection from reality, and lack of recognition of XR's benefits.[28] Regarding the government use of the Metaverse particularly, an empirical study from 2024 shows that while the perceived ease of use, perceived enjoyment, and herd behavior could act as key enablers of adoption, privacy concerns, cyber risks, and resistance to change are salient inhibitors.[29]

To combat citizens' resistance to change, the same study highlights the importance of simplifying usage and reducing the complexity of government services by creating instances — i.e., community forums, marketing campaigns, surveys, testing programs, immersive tutorials, and sandboxes — to aid citizens in getting comfortable with and discovering the benefits of these new applications.[30] Besides these, as argued in the interoperability section, usage interoperability standards, such as identity frameworks, will be pivotal to enhancing user experience in the Metaverse.

Governments also have an important role to play in alleviating privacy and cybersecurity concerns related to their adoption of XR. While some of these challenges may be addressed through strategies such as security audits and strict data protocols, the inherent mass surveillance potential of these technologies is bound to lead to some trepidation.[31]

Another factor that could impact citizen participation in XR public services is that many citizens may lack the digital skills to take advantage of these technologies.[32] Digital exclusion will likely have a greater impact on the elderly, disabled, and low-income groups, leading to further division and discontent.[33] VR headsets may also create challenges for citizens with "visual, vestibular, or cognitive disabilities

---

[25] Susan Aaronson et al., *Reality Check: Why the U.S. Government Should Nurture XR,* XR Assoc. (XRA) & Digital Trade and Data Governance Hub at Geo. Wash. U. (2023), https://xra.org/wp-content/uploads/2023/11/FINAL-XRA-REALITY-CHECK-White-Paper.pdf [https://perma.cc/R78F-N8ZD].

[26] *You Can Now Visit Seoul in the Metaverse*, World. Econ. Forum, https://www.weforum.org/videos/seoul-metaverse/ [https://perma.cc/UGM5-L8BU].

[27] *Id.*

[28] Michael SW Lee & Damien Chaney, *The Psychological and Functional Factors Driving Metaverse Resistance* (2023), https://papers.ssrn.com/abstract=4657053 (last visited Sep 11, 2024).

[29] Ahman Samed Al-Adwan, *The Government Metaverse: Charting the Coordinates of Citizen Acceptance,* 88 Telematics and Informatics 102109 (2024)

[30] *Id.* at 11.

[31] *Id.* at 10.

[32] Lnenicka et al., *supra* note 24, at 3.

[33] *Id.*

who may need additional support to navigate and interact with digital government services."[34]

To address these issues, projects like Metaverse Seoul are implementing their XR advancements through an iterative process. One of the goals of the project's second and third phases is to provide metaverse education to digitally marginalized groups.[35] This phased approach is appropriate given the novelty of the technology. Governments seeking to migrate services into XR should consider an appropriate timeframe to secure the accessibility and usability of XR technologies by marginalized groups, assess their performance, and receive feedback from different stakeholders. Governments should also provide alternative channels to access public services until an inclusive adoption of meta-government is ensured.[36]

Broader governance risks, such as a lack of transparency related to adoption decisions and the role of the private sector in e-governance efforts, could also impact citizens' participation in this space. Governments should heed lessons learned from previous efforts at incorporating new technologies into their operations, such as by developing policies from the outset which guard against potential violations of human rights and anti-discrimination rules.[37]

To get ahead of potential controversies, governments should invest in research and policy instances (e.g. sandboxes) before implementing XR services, to test whether these technologies actually provide better and more equitable public services and decision-making. Ethical and governance frameworks could also help in distinguishing the roles and responsibilities of private companies and governments in service delivery and set basic principles to guide the use of XR for government operations.

IV. Stakeholders and Frameworks

To implement effective governance recommendations, it is important to acknowledge the complex relationship between the public and private sectors in the XR space. In countries such as China and South Korea, the rise of the Metaverse has been significantly driven by public-private partnership (PPP) efforts.[38] Private sector companies have already begun offering products to improve government services through the use of XR in service delivery, security services, and other public sector areas.[39]

While governments can benefit from leveraging the technical expertise of private companies, public-private arrangements sometimes have the effect of blurring the distinction between government and business entities, for example by implying that the government endorses problematic behavior that the business is otherwise connected to.[40] In other instances, the reliance on private sector contractors to deliver public services can create grey areas regarding the applicability of human rights, accountability,

---

[34] *Id.* at 10.

[35] Nir Kshetri et al., *Metaverse for Advancing Government: Prospects, Challenges and a Research Agenda,* 41 Gov. Info. Q. 1, 10 (2024), https://www.sciencedirect.com/science/article/pii/S0740624X24000236.

[36] *Id.*

[37] Brittan Heller, *Reimagining Reality: Human Rights and Immersive Technology,* Carr Center for Human Rights Policy, Harv. Kennedy Sch. (Spring 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4563877 [hereinafter *Reimagining Reality*].

[38] Kshetri et al., *supra* note 35, at 4.

[39] *Immersive Technologies in the Public Sector: The Role of AR, VR, and the Metaverse in Government Services,* Vection Techs., https://vection-technologies.com/solutions/industries/public-sector/ [https://perma.cc/RZB7-FPR7].

[40] Kshetri et al., *supra* note 35, at 7.

or transparency rules that typically bind the public sector. It is important to maintain a clear legal and ethical framework that distinguishes the roles of the different parties involved in the provision of public services in a metaverse context, provides a solid ethical baseline for the deployment of these products, and ensures that appropriate accountability frameworks continue to apply to instances where private contractors fulfil a public function. For example, a number of countries hold that public right to information or freedom of information legislation applies to private companies to the extent that they perform a public function.[41]

South Korea, one of the leaders in implementing XR in the public sector, has made the development of a supportive legal system for this space part of its XR strategy.[42] They were the first OECD member to propose Metaverse Ethical Principles, which call for metaverse developers and users to follow the principles of authenticity, autonomy, reciprocity, privacy protection, fairness, inclusiveness, and responsibility for the future.[43] The principles target individuals and organizations in the private and public sectors, such as companies, academia, research institutes, and civil society.[44] They also set the government as one of the main entities that should implement them while acting as a facilitator in supporting the private sector's efforts to incorporate them into their products.[45]

Another ethical framework tailored for the XR space is the Global Initiative on Ethics of Extended Reality, developed by the Institute of Electrical and Electronic Engineers Standard Association (IEEESA).[46] This initiative produced separate white papers addressing a range of different ethical considerations.[47]

The IEESA's general recommendations are for (i) the establishment of XR-specific procedural policies setting out the ethical standards of XR's interactions with human subjects; (ii) proposed solutions that are adjustable to the ever-changing nature of XR technology; and (ii) making use of working groups from various disciplines that have expertise on XR, spatial web, and relevant experts to draft the relevant policy documents (workshops, white papers and Performance and Accountability Reporting requirements (PARs)) for creators and users of XR.

IEESA's instruments highlight some of the specific concerns governments will need to resolve when implementing XR. For example, for governments that are primary administrators of public education, the IEEESA's Ethics in Education White Paper highlights four challenging areas that must be considered, namely Equity, Acceptance, Safety, and Privacy. The IEEESA rightly raises ethical concerns about how students will retain control over their biometric and psychometric data within the education context when using XR technology and the extent to which XR educational systems will increase the gap between rich and poor.

---

[41] Michael Karanicolas, *A FOIA for Facebook: Meaningful Transparency for Online Platforms,* 66 St. Louis U. L.J. 49, 67 (2021).

[42] Aaronson et al, *supra* note 25, at 41.

[43] *Id.*

[44] *Ethical Principles for the Metaverse,* Ministry Sci. and ICT of Korea, https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=10&mPid=9&pageIndex=&bbsSeqNo=46&nttSeqNo=17&searchOpt=ALL&searchTxt= [https://perma.cc/CLD3-XRF4].

[45] *Id.*

[46] Dylan Fox & Isabel Guentte Thorton, IEEE, Extended Reality (Xr) Ethics and Diversity, Inclusion, and Accessibility (2023).

[47] *Id.*

While South Korea's and IEESA's ethical frameworks are valuable, neither provides a complete template for regulating XR. It is noteworthy that the South Korean principles are not legally binding, and were adopted as part of a broader relaxation of existing regulations to boost the metaverse economy.[48] On the other hand, IEESA's standards are formulated primarily by engineers. While there are advantages to involving designers in the regulatory development process, human-centric policies should ideally be developed through multidisciplinary engagement including experts from law, public policy, the humanities and social science.[49] Conducting effective consultations with users with diverse backgrounds and lived experiences will also be helpful towards ensuring that policies reflect the needs and priorities of the citizen body.[50]

V. Recommendations and Conclusions

Fostering citizen participation in the metaverse entails seizing the opportunities and addressing the challenges of opening democratic spaces for citizens to engage with each other, democratizing the governance structures within the XR space, and enhancing citizen engagement with public services provided through XR. To achieve this, the following recommendations should be considered.

1. **Opening democratic spaces for citizens to engage with each other:**

    a) To build democratic resilience, platforms should take steps in the metaverse to consciously and actively promote democratic actors and narratives. This will be closely related to the content moderation debate.

    b) To use XR to foster empathy between citizens and cultures, policymakers should prioritize authentic representation and understanding of diverse experiences.

2. **Democratizing the governance structures within the XR space:**

    a) Developers and policymakers should proactively support alternative governance mechanisms, including voting systems, oversight councils, and employee mobilization.

        (1) Voting and polling systems can be achieved by selecting a pool of voters or standing up user councils.

        (2) Oversight councils should operate independently and objectively. The council's goals, roles, responsibilities, and authorities should be transparent, and the council should include users of various groups that will be vulnerable to XR enabled harms.

        (3) Tech workers' mobilization efforts should receive adequate legal protection, including where these target policy changes.

    b) Citizen engagement should include representation from diverse interests and communities reflecting the totality of the user base and the public at large.

---

[48] Aaronson et al., *supra* note 25, at 41.

[49] Guilani Molinegro et al., *Process Expertise in Policy Advice: Designing Collaboration in Collaboration,* 8 Humanities. & Soc. Sci. Commc'ns 310 (2021).

[50] Meg Young et al., *Toward Inclusive Tech Policy Design: A Method for Underrepresented Voices to Strengthen Tech Policy Documents,* 21 Ethics & Info. Tech. 89, 103 (2019).

3. Government Services in the Metaverse:

a) Governments wanting to implement XR technologies should introduce them in an iterative process, establishing a specific time frame to secure the accessibility and usability of XR technologies by marginalized groups. Governments should also provide alternative channels to access public services until the proper and inclusive adoption of XR-based public services is secured.

b) Governments should work with XR companies to simplify usage and reduce the complexity of government services offered in XR. Governments should also support the creation of usage interoperability standards.

c) Governments should address privacy concerns through measures like encrypting citizen data, allowing anonymous identities, requiring multi-factor authentication, establishing strict data protocols, and conducting regular security audits.

d) Before implementing XR services, governments should invest in research and policy instances (e.g. sandboxes) to test whether these technologies actually provide better and more equitable services and decision-making.

e) Governments should develop enforceable XR-specific policies that guide the interaction between governments, companies, and human subjects in this space These standards should clearly distinguish the roles and responsibilities of XR companies, users, and governments in these interactions, and should provide robust protections against discrimination or other human rights violations through these technologies.

Content Moderation in Extended Reality

Pablo González Mellafe
Angela Kim
Tammana Malik
Noah Usman

Introduction

Due to the rapid evolution of extended reality (XR) technologies, content moderation is an important issue regulators and platforms must address to develop practices and strategies for a better and safer virtual world.[1] Unlike some traditional social media, XR has many different use contexts ranging from channels for private communication, virtual meeting rooms for specific groups, and full simulations of a virtual world among thousands of other avatars. This diversity of engagement structures, and the multidimensional expressive context of the XR world, creates a range of policy, regulatory, and technical challenges to achieving a comparable level of moderation to what users, governments, and advertisers currently want and expect.

This chapter outlines XR-specific content moderation issues and provides recommendations for content moderation in XR. In Part I, we detail the challenges XR technology creates for content-moderation issues of illegal content, such as Child Sexual Abuse Material, and "lawful but awful" content, which is not illegal but is usually moderated to create safe and enjoyable online environments. In Part II, we discuss some of the tradeoffs content moderation in the XR space poses for free speech and safety. And in Part III, we detail our high level recommendations to XR platforms on how best to moderate content. We first recommend that one of the most effective content moderation strategies is through intentional design of the XR products themselves.[2] Second, platforms should espouse a community-reliant, norms-centered approach to help regulate these spaces. Finally, as XR spaces replace more of our everyday social interaction, platforms can consider whether active policing, like we see in modern communities, could be an effective way to maintain safety in XR spaces.

I. The Challenges of XR Content-Moderation

Content moderation can be divided into two general categories: illegal content, which platforms are typically required to remove once they are aware of its existence; and the so-called "lawful but awful" material that platforms are not required to take down but generally choose to remove in order to promote a safe and enjoyable online space.[3] The types of illegal online content vary greatly in different jurisdictions, but common examples include Child Sexual Abuse Material (CSAM), fraud,

---

[1] *See Content Moderation: Key Practices & Challenges,* Tremau (June 5, 2023), https://tremau.com/content-moderation-key-practices-challenges/ [https://perma.cc/ZPU8-8YCB].

[2] *See* John Perrino, *Using 'Safety by Design' to Address Online Harms,* Brookings (July 26, 2022) https://www.brookings.edu/articles/using-safety-by-design-to-address-online-harms/ [https://perma.cc/HBT9-F5RP].

[3] *See* Daphne Keller, *Lawful but Awful? Control over Legal Speech by Platforms, Governments, and Internet Users*, U. Chi. L. Rev. Online (June 28, 2022), https://lawreviewblog.uchicago.edu/2022/06/28/keller-control-over-speech/ [https://perma.cc/W3LN-QVQS].

and infringements of intellectual property.[4] In the context of traditional social media, platforms' moderation of these forms of content is by no means perfect, though they typically devote significant resources as a result of liability flowing from poor moderation performance.

In contrast, "lawful but awful" content is material "that cannot be prohibited by law but that profoundly violates many people's senses of decency, morality, or justice."[5] Examples include sexual harassment or bullying;[6] misinformation;[7] content that promotes terrorism or terrorist groups;[8] and various forms of hate speech or obscene content.[9] As these examples demonstrate, the two categories are relatively fluid, since certain forms of misinformation, hate speech, and terrorist content are prohibited in some countries but not in others. Both categories present novel and resource intensive challenges in an XR context, though platforms typically have greater flexibility in how "lawful but awful" content is managed.

For both categories of content moderation, platforms typically employ a mix of human review and automated review.[10] The scale of modern content moderation means that, across traditional social media, automated review accounts for the bulk of moderation actions. This is despite the fact that, while automated systems have proven reasonably successful at detecting certain types of content, such as CSAM, other more contextual forms of prohibited content, such as hate speech or harassment, are far more difficult for automated systems to reliably identify. There are also enormous gaps between how automated moderation systems perform in the context of English language content versus smaller language groups.

Content laws that apply to traditional social media are likely to also apply in an XR context. Users are also likely to have similar expectations with regards to moderating "lawful but awful" content and are unlikely to choose to spend much time on a service that is teeming with hate or abuse. However, there are critical differences between how moderation works in an XR environment versus the traditional social media space. By simulating a virtual world, XR bears some similarities to "ephemeral social media," which is content that is designed to disappear after a short period, like Instagram stories and voice-based social media (e.g., Discord).[11] Ephemeral social media sites tend to lean more heavily on community-based moderation methods, or self-service tools, such as allowing users to individually

---

[4] *Illegal Content on Online Platforms,* Eur. Comm'n (June 7, 2022), https://digital-strategy.ec.europa.eu/en/policies/illegal-content-online-platforms [https://perma.cc/RY7L-Z4J2].

[5] Keller, *supra* note 3.

[6] *See, e.g.,* Tanya Basu, *The Metaverse has a Groping Problem Already,* MIT Tech. Rev. (Dec. 16, 2021), https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/ [https://perma.cc/A2XU-CUW5].

[7] *Misinformation*, Meta Transparency Ctr, https://transparency.meta.com/policies/community-standards/misinformation [https://perma.cc/SQT3-PDBY].

[8] *See* Bennett Clifford, *Moderating Extremism: The State of Online Terrorist Content Removal Policy in the United States,* Geo. Wash. U. Program on Extremism (Dec. 2021), https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/Moderating%20Extremism%20The%20State%20of%20Online%20Terrorist%20Content%20Removal%20Policy%20in%20the%20United%20States.pdf [https://perma.cc/5RWJ-QBHK].

[9] *See* Naomi Nix, *Meta Doesn't Want to Police the Metaverse. Kids are Paying the Price.,* Wash. Post. (Mar. 8, 2023), https://www.washingtonpost.com/technology/2023/03/08/metaverse-horizon-worlds-kids-harassment/ [https://perma.cc/J993-9BLD].

[10] Nazanin Sabri et al, *Challenges of Moderating Social Virtual Reality, in* Proceedings of the 2023 Chi Conference on Human Factors in Computing Systems (2023), https://dl.acm.org/doi/fullHtml/10.1145/3544548.3581329#BibPLXBIB0118 [https://perma.cc/LH5C-VEZ6].

[11] *Id.*

mute or block disfavored accounts. This is partly due to the challenges in carrying out effective realtime analysis, especially when dealing with audio conversation or video-based content.[12]

However, moderation in XR space is further complicated by the dynamic nature of the virtual environment, which involves the interaction of user-generated or user-hosted content, as well as person-to-person communication and physical movements, with virtually generated environments.[13] The immersive nature of the environments, including engaging with a variety of physical responses, has the potential to create increased harm from negative or violent encounters.[14] The ability to monitor XR spaces is also hampered by the current state of moderation technology. Because XR technologies create or replicate perceived physical environments, the amount of data aggregated in real time is far too great for content to be assessed and moderated externally on a case-by-case basis. Automated systems, which already struggle with context in a purely text-based environment, will face enormous challenges due to the novelty of this medium, as well as the even more subtle and contextual nature of expressive activities.

As more and more users migrate into XR, illegal content will inevitably follow, posing a challenge to regulators and to the companies and individuals potentially hosting this content. Typically, the sharpest edge of this challenge manifests in the form of CSAM, which tends to attract particularly aggressive enforcement responses. XR not only offers avenues to share existing CSAM in a way that is roughly analogous to its distribution across social media, but also opportunities to generate and share new types of CSAM. Increasingly realistic deepfake images and customized fantasy characters may be used to create sexualized representations of children — material that currently falls into a legal gray area because it does not depict an "actual" child — or to create non-consensual pornography.[15]

Grooming is also likely to be a problem in XR, facilitated by the ability to adopt or create child-like avatars, enabling abusers to approach underage users in a non-threatening manner and gain their trust by presenting themselves as peers, while also allowing them to avoid detection by third-parties who find it difficult to ascertain their real age. Adult users may approach children using the service to try and encourage them to engage in sexual acts online or in the real world.[16] Virtual depictions of child sexual abuse may also be used as a grooming tactic to desensitize potential victims.

While most XR platforms contain age-restrictions, underage users can easily bypass them. For instance, the Terms of Service of VRChat states that users must be over 13 years of age to access and use the platform, but that eligibility is based on the user's self-declaration without any effective means of verification.[17] Similarly, the Sony Play Station VR Instruction Manual indicates that the minimum

---

[12] *See Safety and Moderation,* Discord, https://discord.com/community-moderation-safety [https://perma.cc/34G2-ZXSL] (describing the vast array of approaches server moderators can use to moderate content).

[13] Daniel Castro, *Content Moderation in Multi-User Immersive Experiences: AR/VR and the Future of Online Speech,* Info. Tech. & Innovation Found. (Feb. 28, 2022), https://itif.org/publications/2022/02/28/content-moderation-multi-user-immersive-experiences-arvr-and-future-online/# [https://perma.cc/3Y8B-EHGH].

[14] Brittan Heller, *Revisiting Code as Law: Regulation and Extended Reality,* Stan. Cyber Pol'y Ctr. 1, 22–23 (Sept. 1, 2023), http://dx.doi.org/10.2139/ssrn.4559458.

[15] *See* Drew Harwell, *AI-Generated Images of Child Sexual Abuse are on the Rise,* Wash. Post. (June 19, 2023), https://www.washingtonpost.com/technology/2023/06/19/artificial-intelligence-child-sex-abuse-images/.

[16] *See* Angus Crawford & Tony Smith, *Metaverse App Allows Kids Into Virtual Strip Clubs*, BBC News (Feb. 23, 2022), https://www.bbc.com/news/technology-60415317 [https://perma.cc/H9BZ-V5C5].

[17] *See Terms of Service,* VRChat (Nov. 22, 2023), https://hello.vrchat.com/legal [https://perma.cc/KH2S-7U58].

age to use the device is 12 years old, however, there is no effective means of verifying a user's age.[18] XR platforms generally place the responsibility for age control on parents, avoiding more effective verification or control mechanisms, which ultimately results in children being able to easily evade such mechanisms.

These concerns are not unique to XR, and there have been a range of proposals in recent years aimed at safeguarding children online, particularly through the use of new technical safeguards. For example, the California Age-Appropriate Design Code Act (AADC), which is modeled on the United Kingdom's Age-Appropriate Design Code (UK AADCA), was passed in September 2022 and applies to websites and online services that are "likely to be accessed" by users under 18 years of age.[19] The Act requires such websites and online services providers to estimate the age of child users.[20] However, the District Court for the Northern District of California, while granting a preliminary injunction preventing the enforcement of the AADC on the basis of First Amendment violations, found that this requirement may actually increase the potential for harm to minors by requiring them to divulge more personal information that would make such an estimation possible.[21] The Ninth Circuit recently affirmed the district court's preliminary injunction.[22] Similarly, the Kids Online Safety Act (KOSA) passed by the U.S. Senate in May 2023 has been criticized over privacy and censorship concerns.[23]

The other category of illegal content which typically dwells on the leading edge of moderation challenges is intellectual property violations. Mandatory takedown programs, such as the copyright rules in the *Digital Millennium Copyright Act*, are likely to generate significant enforcement pressures on XR service providers, as users inevitably engage in infringing activities.[24]

XR platforms will likewise face challenges related to the enforcement of their own community guidelines.[25] As has been the case with traditional social media, users, advertisers, and governments are likely to present competing pressures to remove problematic or harmful content while respecting users' demands for an open expressive environment.[26] Although the specific legal standards for incitement to violence and terrorist acts vary by jurisdiction, both are widely banned by traditional social media companies through their terms of service.[27] Due to the more immersive and realistic nature of XR platforms, it is easy to imagine the amplified efficacy of propaganda in an XR context.

---

[18] *See Instruction Manual,* Sony PlayStation VR, https://www.playstation.com/content/dam/global_pdc/en/corporate/support/manuals/psvr-docs/cuh-zvr1/EN_PSVR_CUH-ZVR1_Instruction_Manual_Web.pdf [https://perma.cc/T89R-L34Y].

[19] Cal. Civ. Code § 1798.99.31

[20] *Id.*

[21] NetChoice, LLC v. Bonta, 692 F. Supp. 3d 924, 951 (N.D. Cal. 2023), *aff'd in part,* 2024 WL 3838423 (9th. Cir. 2024).

[22] *See* NetChoice, LLC v. Bonta, No. 23-2969, 2024 WL 3838423 (9th. Cir. August 16, 2024).

[23] *See, e.g.,* Molly Buckley, *The U.S. House Version of KOSA: Still a Censorship Bill,* Elec. Frontier. Found. (May 3, 2024), https://www.eff.org/deeplinks/2024/05/us-version-kosa-still-censorship-bill [https://perma.cc/BEB7-FUDB].

[24] *See* Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

[25] *See, e.g., Promoting Safety and Expression,* Meta, https://about.meta.com/actions/promoting-safety-and-expression/# [https://perma.cc/4XAW-E3PW] ("We remove hate speech, harassment, threats of violence . . . .").

[26] *See* Stefan M. Herzog et al., *Resolving Content Moderation Dilemmas Between Free Speech and Harmful Misinformation* (Feb. 7, 2023), https://www.pnas.org/doi/full/10.1073/pnas.2210666120 [https://perma.cc/2Y6F-6HCB].

[27] Stuart Macdonald, Sara Giro Correia & Amy-Louise Watkin, *Regulating Terrorist Content on Social Media: Automation and the Rule of Law,* Int'l J. L. Context 183, 184–85 (2019), https://www.cambridge.org/core/journals/international-journal-of-law-in-context/article/regulating-terrorist-content-on-social-media-automation-and-the-rule-of-law/B54E339425753A66FECD1F592B9783A1.

However, the analysis of XR users' speech and movement at scale and in real time presents challenges that go far beyond screening a text-based medium like Facebook or X. Effective tools for moderators to view relevant data from ephemeral spaces present an exceedingly difficult task which also implicates privacy and free speech concerns.[28]

Hate speech, which is also widely prohibited across the community guidelines of most XR services, presents similarly thorny challenges. The International Covenant on Civil and Political Rights (ICCPR) defines hate speech as "any propaganda for war and any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence."[29] While many countries and jurisdictions prohibit hate speech, the United States and others do not.[30] And even among the various jurisdictions where it is illegal, there is no uniform definition of what constitutes hate speech.[31]

Many social media platforms prohibit hate speech under their private moderation rules,[32] but hate speech is still prolific in social media spaces. Online hate speech has tangible consequences: It can breed prejudice, discrimination, intolerance, stereotypes and hostility toward target groups, and in extreme cases, incite violence or criminal activity toward them; these consequences are exacerbated in the increasingly vivid and accurate representations of reality that can be generated in XR.[33] And while hate speech exists in both real life and traditional online ecosystems, its proliferation and potential impact is amplified on XR platforms.

In addition to the speed and scale of dissemination in a digital context, and the sense of anonymity that is typical of most online interactions, the immersive features unique to XR mean the effects of hate speech are more visceral and persuasive.[34] These include users' capabilities to express hate speech through their avatars' nonverbal offensive expressions and body language as well as the ability to manipulate the spatial proximity to victims' avatars and sense of presence to mimic the feeling of face-to-face interaction. Such interactions can feel more personal and real than an anonymous comment on social media platforms.

While private platforms can regulate content that is lawful but violates their conduct code, such as hate speech, the determination of whether given content constitutes hate speech is not only inconsistent

---

[28] Sabri et al, *supra* note 10.

[29] International Covenant on Civil and Political Rights art. 20 para 2, Sept. 8, 1992, 999 U.N.T.S 178, https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/CCPRGeneralCommentNo11.pdf [https://perma.cc/6FTH-93JD].

[30] *Comparing Hate Speech Laws in the U.S. and Abroad,* NPR News (Mar. 3, 2011), https://www.npr.org/2011/03/03/134239713/France-Isnt-The-Only-Country-To-Prohibit-Hate-Speech [https://perma.cc/JP6R-EDWB].

[31] *See Hate Speech and Hate Crime*, ALA (Dec. 12, 2017), http://www.ala.org/advocacy/intfreedom/hate [https://perma.cc/2HVY-HK74] (defining hate speech as "any form of expression through which speakers intend to vilify, humiliate or incite hatred against a group or a class of persons on the basis of race, religion, skin color, sexual identity, gender identity, ethnicity, disability or national origin"); *see also What is Hate Speech?,* UN, https://www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate-speech [https://perma.cc/7GK4-CN3Q] (defining hate speech in terms of both its content and its harm to the recipient).

[32] *See, e.g., Hate Speech,* Meta, https://transparency.meta.com/policies/community-standards/hate-speech/ [https://perma.cc/B3SV-64GV].

[33] Sergio Andrés Castaño-Pulgarín et al., *Internet, Social Media and Online Hate Speech. Systemic Review,* 58 Aggression & Violent Behav. 1, 2 (Apr. 6, 2021), https://doi.org/10.1016/j.avb.2021.101608.

[34] Esen Küçüktütüncü & Dani Shanley, *Hate Speech in the Metaverse,* Project Immersive Democracy (July 11, 2023), https://www.metaverse-forschung.de/en/2023/07/11/hate-speech-in-the-metaverse/ [https://perma.cc/9TTE-DXAS].

but also heavily nuanced and influenced by public pressure.[35] According to international standards, the question of whether something is hate speech is a fundamentally contextual determination, based in part on the actual impact of the material on its intended audience. This means that a particular statement made in an area with high ethnic tensions might be considered hate speech in that jurisdiction, but not in another part of the world where the situation is less dangerous. As individuals from various jurisdictions of the world mingle in one interactive virtual space, the need for platforms to moderate harmful hate speech while remaining conscious to the interacting factors, including geographically-sensitive cultural and societal norms and laws of the parties involved, grows more pressing.[36]

Misinformation raises similarly complicated regional dynamics, and is even more difficult to consistently and comprehensively define.[37] Given the significant risks associated with misinformation in traditional digital platforms, the potential for even more immersive forms of content in XR technologies can significantly complicate existing harms.[38] Scholars have further posited that, as XR becomes more accurate in mimicking real-world conditions, users will find it increasingly difficult to separate between real and false information, especially given the influence of generative AI in propagating artificially created images at the behest of their users.[39]

One additional form of harmful content which presents a pervasive challenge across digital interactive media is harassment, including sexual harassment. The harms of online harassment are well researched.[40] However, the effects of physical forms of harassment are compounded in XR due to a phenomenon unique to XR called the "phantom touch illusion" (PTI) where users of XR technology describe experiencing tingling sensations on their body in areas corresponding with where their avatars were touched.[41] While these unique features can be harnessed to assist with trauma-informed therapy or phantom limb pain,[42] they also exacerbate the negative impacts that harassment, including sexual harassment, has on XR users. Attacks and harassment on XR are much more traumatic than those faced in traditional online forums and feel much closer to real life interactions.[43] Experts

---

[35] Luvell Anderson & Michael Barnes, *Hate Speech*, Stan. Encyclopedia Phil. (Jan. 25, 2022), https://plato.stanford.edu/archives/fall2023/entries/hate-speech/ [https://perma.cc/PDV8-W7DM].

[36] Emmie Hine, *Content Moderation in the Metaverse Could Be a New Frontier to Attack Freedom of Expression,* Philos. Technol. 36, 43 (2023), https://doi.org/10.1007/s13347-023-00645-4.

[37] Michael Karanicolas, *Even in a Pandemic, Sunlight is the Best Disinfectant: COVID-19 and Global Freedom of Expression*, 22 Or. Rev. Int'l L. 101, 102 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3726892.

[38] *See* Thi Tran, Rohit Valecha, Paul Rad, & H. Raghav Rao, *An Investigation of Misinformation Harms Related to Social Media During Humanitarian Crises, in* Secure Knowledge Management in Artificial Intelligence Era 167 (Sanjay K. Sahay, Nihita Goel, Vishwas Patil & Murtuza Jadliwala ed. 2019), https://link.springer.com/chapter/10.1007/978-981-15-3817-9_10.

[39] Janna Anderson & Lee Rainie, *More Potential Negatives of the Advancement of XR,* Pew Rsch. Ctr. (June 30, 2022), https://www.pewresearch.org/internet/2022/06/30/some-potential-negatives-of-the-advancement-of-xr/ [https://perma.cc/DMS2-3RGQ].

[40] *See, e.g.,* Lindsay Blackwell et al; *Classification and Its Consequences for Online Harassment: Design Insights from HeartMob,* 1 Proc. ACM Hum.-Comput. Interact. 1, 2 (Dec. 6, 2017), https://dl.acm.org/doi/abs/10.1145/3134659.

[41] Artur Pilacinski et al., *Phantom Touch Illusion, an Unexpected Phenomenological Eff[f]ect of Tactile Gating in the Absence of Tactile Stimulation,* 13 Sci Rep. (Sept. 18, 2023), https://doi.org/10.1038/s41598-023-42683-0 (suggesting these physiological responses are based not only on a user's vision but also a complicated combination of sensory inputs and internal perceptions).

[42] Heller, *supra* note 14, at 27.

[43] *See* Patsy Stevenson, *Sexual Assault in the Metaverse,* Byline Times, (Jan. 9, 2024), https://bylinetimes.com/2024/01/09/sexual-assault-in-the-metaverse/ [https://perma.cc/G6JY-LX3Y].

anticipate that these harms will only be exacerbated with the expected increase in haptic device use.[44] For instance, in the United Kingdom, law enforcement investigation of a "gang-rape" of a teenage girl's metaverse avatar yielded genuine manifestations of psychological trauma similar to that experienced by survivors of sexual assault in the physical world.[45]

In addition, the risk of harassment in XR is much greater due to the lack of "protectors." In the real world, although harassment occurs, safeguards like law enforcement or other agents of authority, clearer legal frameworks, and civic education are more established. These are by no means perfect solutions, but they provide at least some framework for prevention and redress for which there is no ready analogue in XR. Moderation structures are relatively ineffective and, to the extent that they exist, they lack the sort of sanctions that may prevent or inhibit this behavior from determined abusers.[46]

As a result of the challenges inherent in moderating XR content at scale, technology companies more generally have turned to personal moderation tools that enable users to shield themselves from unwanted behavior and disturbing content. These include the options to mute, block, or remove other users from a shared space, as well as activating a "space bubble," or virtual barrier that shields users from audio or "physical" contact. While these are effective strategies to help users control their own experiences in XR, they are ineffective at dealing with speech-related harms that create broader social costs, such as hate speech or misinformation.

II. Questions, Value Judgments, and Tradeoffs: Free Speech versus Safety

Any content moderation approach necessarily entails a restriction in individual freedoms and, to a certain degree, a judgment about the value of protecting open discourse versus preventing the individual and social harms caused by illegal and lawful but awful content discussed above. While this tension is at its most apparent in the case of rules which are imposed by States, even platform content guidelines require some sort of assessment of the values and community that the company wants to cultivate.

For categories of content that have been declared "illegal" in certain jurisdictions, this judgment reflects an understanding that the harms outweigh the benefits of a free flow of ideas — with the necessary caveat that the standard each jurisdiction employs to arrive at this conclusion varies drastically, just as the legislation itself varies. With respect to categories of "lawful but awful" content, the boundaries of regulation are murkier and more polarizing. However, both categories demonstrate a reflection of society and community values.

The question of who should regulate content is intrinsically tied into the nature of the content that is being regulated. One way to purportedly avoid free speech challenges to content moderation decisions is to shift the burden of such decision making onto private actors, which are generally not bound by the state action doctrine. In the United States, Section 230, enacted as part of the Communications

---

[44] Blackwell et al, *supra* note 40, at 4–6.

[45] Katherine Tangalakis-Lippert, *A Sexual Assault in the Metaverse Has Investigators Questioning the Future of Virtual Crime Prosecution,* Bus. Insider, (Jan. 7, 2024), https://www.businessinsider.com/police-investigate-digital-gang-rape-teen-vr-metaverse-horizon-worlds-2024-1 [https://perma.cc/QPZ4-3K8Z].

[46] *See* Emma Barrett & Steve Pettifer, *Online Safety: Child Abuse and Exploitation in eXtended Reality* (June 13, 2022), https://blog.policy.manchester.ac.uk/posts/2022/06/online-safety-child-abuse-and-exploitation-in-extended-reality/ [https://perma.cc/Y8ZQ-BBJX].

Decency Act, protects online communications platforms (including XR platforms) from liability for the content that users share on their platform.[47] Outside the United States, many democratic countries have intermediary liability laws in place to balance protecting free speech and safety considerations.[48] However, not all countries in which platforms operate have similar commitments to free expression. As a result, platforms themselves must take responsibility for making decisions about these trade-offs, including about compliance with local laws.

However, in light of the vast power private entities, such as social media platforms, wield in terms of limiting, controlling, and censoring speech, it has been argued that private actors are essentially analogous to governments, and communications on such platforms deserve First Amendment protections.[49]

This tension regarding whether social media platforms are "public spaces" for the purposes of free speech protections is already playing out in courts — the Supreme Court ruled in March 2024 that public officials who post about topics relating to their work on their personal social media accounts are acting on behalf of the government, and therefore can be held liable for violating the First Amendment when they block their critics.[50] On the other hand, in a set of cases filed against Florida and Texas statutes that aim to modify the internal policies and algorithms of large social media platforms by regulating how the platforms can promote, demote or remove posts, a tech industry trade group representing a wide range of social media platforms and online businesses, including Meta, Amazon, Airbnb and TikTok, contends that the platforms are not public forums.[51]

This assignment of burden is relevant not just for making the content moderation decision, but also for strategizing advocacy and seeking recourse. The question of what content should be moderated online, and what modalities should be used to accomplish this, implicates a wide range of questions concerning the value of free speech and associated tradeoffs. The idea that speech should be regulated to preserve online freedom for all citizens plays into the controversial idea of defensive democracy. This philosophy is exemplified by the right, as articulated by Karl Popper, "not to tolerate the intolerant,"[52] and thus ban rhetoric that threatens the civil exercise of democracy.

While European democracies have largely embraced the need to strengthen regulation over digital speech,[53] the appropriate scope of government, or even private platform, intervention remains controversial in American discourse.[54]

These controversies are likely to take on new dimensions as XR gains in popularity. On one hand, the imposition of regulations that curtail free expression could prove to be a serious hurdle to the growth

---

[47] U.S.C. § 230 (1996).

[48] Ashley Johnson & Daniel Castro, *How Other Countries Have Dealt With Intermediary Liability*, Info. Tech. & Innovation Found. (Feb. 22, 2021), https://itif.org/publications/2021/02/22/how-other-countries-have-dealt-intermediary-liability/ [https://perma.cc/9W4W-RTJ5].

[49] *E.g.*, Benjamin F. Jackson, *Censorship and Freedom of Expression in the Age of Facebook,* 44 N.M. L. Rev. 121, 134 (2014).

[50] Lindke v. Freed, 601 U.S. 187 (2024).

[51] *See* Moody v. NetChoice, LLC, 144 S. Ct. 2383 (2024).

[52] Karl Popper, The Open Society and Its Enemies (1962).

[53] Richard Youngs, *The Defensive Turn in European Democracy Support,* Carnegie Eur. (Mar. 14, 2024), https://carnegieeurope.eu/2024/03/14/defensive-turn-in-european-democracy-support-pub-91946 [https://perma.cc/Q5HT-DFCB].

[54] *See* Michael Signer, *America Does Have a Way to Save Itself,* Atlantic (April 29, 2023), https://www.theatlantic.com/ideas/archive/2023/04/us-defensive-democracy-authoritarianism/673878/ [https://perma.cc/9VZN-C7FK].

and adoption of a technology like XR, that's still in its nascent stage. On the other hand, current and potential users may also be driven away by a hostile virtual environment and proliferation of hateful and violent speech. Lawmakers are likely to face a steep learning curve adjusting to the technological differences between XR and social media, especially in terms of the challenges of effective moderation.

III. Guiding Concepts for Effective Content Moderation in XR

A. Safety by Design

While the content moderation challenges that are set to manifest in XR environments bear some similarities to those that we see in traditional social media platforms, the dynamic and immersive XR environment, along with the inability of existing tools to handle these challenges, requires a fundamental reconceptualization of how content moderation is carried out. In particular, it requires a centering of design-centric models of content management.

Content moderation can occur through the intentional design of products, rather than specific regulations prohibiting categories of speech.[55] If content is moderated by the design of software and hardware, rather than by regulation, XR platforms can both protect freedom of expression and provide safe environments for use. This strategy of intentional design builds on Lawrence Lessig's proposals from Code 2.0, where he introduced the concept of "code" or technology as a regulator.[56] He argued the design of a technology (in this case, especially the design of software) can moderate the market, laws and norms and, ultimately, people's behavior.

Promoting safety by design has several advantages over the current moderation paradigm. Adopting a preventative and structural approach to online harms is both more efficient than focusing on tracking down instances of harmful content and it limits the need for human moderators to engage with shocking and damaging online content.[57] Traditional social media platforms are increasingly relying on structural solutions to limit the harm from online content, such as through imposing forwarding limits on messages to the public to stymie the virality of misinformation,[58] creating better labeling to identify official or satirical accounts,[59] and granting users more control over who can interact with them and how.[60] Many child protection codes rely heavily on design, for example by limiting interactions between children and adults, or placing stricter rules around permissible behaviors in circumstances where adults and minors engage with one another. Although the privacy challenges associated with age verification pose a major obstacle to these solutions in a social media context, the fact that XR is

---

[55] Katie Harbath, *Content Moderation Through Design*, Bipartisan Pol'y Ctr. (June 27, 2022), https://bipartisanpolicy.org/blog/content-moderation-through-design/ [https://perma.cc/UT9K-X3KM].

[56] Lawrence Lessig, The Code: Version 2.0 (2006).

[57] See Isaac Chotiner, The Underworld of Content Moderation, New Yorker (July 5, 2019), https://www.newyorker.com/news/q-and-a/the-underworld-of-online-content-moderation [https://perma.cc/G92H-UNUL].

[58] *E.g.,* Jay Sullivan, *Introducing a Forwarding Limit on Messenger,* Meta (Sept. 3, 2020), https://about.fb.com/news/2020/09/introducing-a-forwarding-limit-on-messenger/ [https://perma.cc/DX7Z-NS6F].

[59] *See, e.g.,* James Vincent, *Facebook Hopes Tiny Labels on Posts Will Stop Users Confusing Satire with Reality,* Verge (Apr. 8, 2021), https://www.theverge.com/2021/4/8/22373291/facebook-label-news-feed-page-posts-fan-satire-public-official [https://perma.cc/4CVR-K2NC].

[60] Perrino, *supra* note 2.

naturally more invasive (through verification paradigms that leverage types of biometric data) may help to mitigate these concerns.

Applying this paradigm to the XR realm will require careful and thoughtful engagement with the different forms of content-based harms that are likely to manifest in this environment. Design-based mitigation strategies that are intended to combat CSAM will likely vary from those targeted towards misinformation. However, the alternative, which involves regulating media platforms after dangers are well entrenched, is likely to be much less safe for users.

A preventative framework should center "safety by design" principles which emphasize accountability, transparency, and user empowerment in digital architecture.[61] This includes making reporting mechanisms easily accessible for minors, setting safety and security defaults to the strongest option possible, giving users more control over recommendation and communication features, offering in-platform education and resources to guide users on the standards for appropriate behavior, and proactively encouraging users to review platform settings.[62]

In addition to a fundamental strategic turn away from the growth-centric model of technological development, this approach will require substantial additional research to develop tools that are capable of grappling with the vast array of social and informational cues that manifest in an XR environment. In parallel to how automated enforcement has evolved in the context of traditional social media, it is likely that automated tools will be better suited to addressing some forms of problematic content than others. Harms in which context is less important, such as CSAM, will be easier to find and prevent than those which are heavily contextual, such as hate speech or abuse. Nonetheless, if these technologies are set into XR's architectural framework from the beginning, as opposed to being piloted after the technology has reached critical mass, they will be more likely to help shape the culture of XR platforms in a way that will help avoid the mistakes of the previous generation of social media.

B. Community Engagement

As a complement to the preventative, architectural approach, content moderation should prioritize models of behavioral regulation, employing a community-based approach to content moderation. Reddit and Wikipedia provide examples of how moderation may be hybridized between platform and community-driven approaches.[63] While Reddit has global content policies enforced by a centralized team, it also grants a great deal of autonomy and editorial discretion to subreddit (smaller communities within Reddit) moderators. These moderators tailor content policies to the specific needs of their subreddits, thus playing a key role in managing most of the platform's content. Reddit also allows for user moderation, by allowing all users in a subreddit to downvote comments or posts, which will block them from view or lead to their removal by the moderators.

To deal with the challenges of moderating at scale without effective automated structures, XR platforms will have to develop a decentralized approach, where there is company-wide code of conduct that

---

[61] Perrino, *supra* note 2.

[62] *Id.*

[63] *Case Study: Reddit,* New America, https://www.newamerica.org/oti/reports/everything-moderation-analysis-how-internet-platforms-are-using-artificial-intelligence-moderate-user-generated-content/case-study-reddit/ [https://perma.cc/37N9-R7WC]; *see also* Joel Khalili, *How Reddit Turned its Millions of Users into a Content Moderation Army,* TechRadar (June 22, 2021), https://www.techradar.com/news/how-reddit-turned-its-millions-of-users-into-a-content-moderation-army [https://perma.cc/KXL3-8599].

provides baseline standards, but where enforcement is mostly delegated to leadership teams responsible for their own sub-communities. These volunteers will need to be granted some degree of latitude for how norms are enforced, including the ability to adapt the rules, or add new ones, to suit their own specific contexts.

We can see initial signs of this in Meta's Metaverse, which has implemented a higher-level code of conduct for virtual experiences[64] and facilitates the creation of membership-based communities for like-minded individuals.[65] The creation of these "members-only" spaces remains optional; Meta's staff do not moderate these worlds, and membership is capped at 150 individuals per world. Creators are responsible for approving memberships, and designated "admins" within these closed communities handle the majority of content moderation tasks. Community-based moderation approaches such as platform user guidelines are generally applicable only to the "public spaces" on a platform. With many XR applications allowing for the creation of private/invite-only spaces, the need for moderation is further complicated by privacy concerns and the applicability of community rules to interactions within these spaces.

C. Who Polices XR?

While community-reliant methods are ideal for contained communities of relatively shared values, there is a dire need for reconsideration of how rules should be set and enforced in the context of XR. If XR becomes a more prevalent mode of engagement with the world, a place where we not only express and educate ourselves but also where we work, play, date, and carry out a variety of social activities, we will continue to encounter challenging questions regarding acceptable levels of enforcement and surveillance.

Few people want to live in a world which is teeming with abuse, sexual harassment, hate speech and misinformation. However, there are stark tradeoffs between safety and speech which most democracies accept as the price for living in a free society. If our society continues to adopt XR platforms and interfaces, this raises difficult questions as to whether the dominant regulatory paradigm should reflect the type of content enforcement that we see in social media, and which typically enforces standards more aggressively than the letter of the law, or the form of enforcement that we see in the real world, where speech-based enforcement is far less prevalent in most people's everyday lives. One necessary step towards reconciling these divergent enforcement paradigms is to update our legal frameworks to ensure they appropriately apply to XR harms.[66] Existing tort liability frameworks, for example, may need to be revised so that they adequately reflect how harm manifests in these contexts. Likewise, expectations about the speed and efficacy of content moderation will need to be adapted from text-based models of enforcement that regulators are familiar with. Hopefully, this emergent regulatory delta will give rise to a robust conversation about the type of XR world that we want and the tradeoffs between speech and safety that we find acceptable for these new technologies.

---

[64] *See Code of Conduct for Virtual Experiences,* Meta, https://www.meta.com/help/quest/articles/accounts/privacy-information-and-settings/code-of-conduct-for-virtual-experiences/ [https://perma.cc/HL6W-255F].

[65] *Members-only Worlds in Meta Horizon Worlds,* Meta, https://www.meta.com/help/quest/articles/horizon/explore-horizon-worlds/members-only-worlds/ [https://perma.cc/VL95-KRLX].

[66] *See, e.g.,* Ben Lang, *'Rec Room' Update Adds Private Lounge Space and Invite-Only Activities,* Road to VR (Dec. 23, 2016), https://www.roadtovr.com/rec-room-update-adds-lounge-space-invite-activities/ [https://perma.cc/V8PX-JXFF].

IV. Recommendations and Conclusions

The ever-increasing applications of XR provide a new array of possibilities for collaboration and social interaction, but also for new methods of harm and abuse. For all of their potential to connect people in exciting new ways, the immersive nature of these technologies also carry significant risks, such that users can exhibit psychological signs of sexual assault without ever having been touched, and that misinformation and hate speech can be circulated faster and more convincingly than at any prior point in human history.

In order to ensure safety on these new technologies, private actors, companies, users, and regulators should intentionally design XR products to effectively support safer and more trusted speech ecosystems and deploy community-centered approaches as innovative as the software that they intend to regulate.

Privacy & XR

Gabriela Gura
Md Abdul Malek
Walter Musgrave
Mahmut Ormanci

Introduction

The buzz around data privacy began to intensify in the 2010s as technology developers increasingly prioritized "big data" capabilities.[1] Widespread adoption of the internet, smartphone devices, and social media platforms began to ring alarm bells about the collection, use, and protection of personal data. Since then, and fueled by some notable privacy scandals,[2] policymakers and stakeholders worldwide have developed privacy regulations that are just now getting their arms around the challenges posed by unchecked tech innovation that relies on the mass accumulation of data.[3] As this chapter will detail, however, the tech industry is rapidly developing XR technologies that pose new challenges to existing privacy regulations.

XR differs meaningfully from prior technologies, requiring novel policy approaches to preserve data privacy. When it comes to data practices, XR is unique in its:

- **Scope** — the *amount* of data that XR can collect.
- **Scale** — the *range* of different kinds of data (biometric, geolocation, personal identifiers, etc.) that XR can collect.
- **Real-time data collection** — how XR collects all the above-mentioned data in real-time.
- **Bystander effects** — how bystanders are also affected by XR data collection.
- **Aggregation** — how all this data is packaged both on- and off-device to create profiles of users to predict behavior and/or to sell to third parties.

This chapter will proceed in four sections. Section I explores the ways that XR dataflows collect, store, and compile information. Section II describes how current XR data practices further surveillance capitalism. Section III analyzes how existing privacy regulations could tackle these issues and their limitations. Section IV imagines how privacy-enhancing technologies could be incorporated into

---

[1] Big data refers to the new data processing and storage capabilities that incentivized mass collection of personal data. *See* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics,* 11 N.W. J. Tech. & Intell. Prop. 239, 240 (2013); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms,* 55 B.C. L. Rev. 93 (2014); Katherine J. Strandburg, *Monitoring, Datafication and Consent: Legal Approaches to Privacy in the Big Data Context,* in Privacy, Big Data and the Public Good: Frameworks for Engagement (2021); Gil Press, *A Very Short History of Big Data,* Forbes (July 17, 2019, 11:32 AM), https://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/ [https://perma.cc/M3HK-GUSH].

[2] Alvin Chang, *The Facebook and Cambridge Analytica Scandal, Explained with a Single Diagram,* Vox (May 2, 2018), https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram; Kate O'Flaherty, *Google+ Security Bug — What Happened, Who Was Impacted And How To Delete Your Account,* Forbes (Oct. 9, 2018), https://www.forbes.com/sites/kateoflahertyuk/2018/10/09/google-plus-breach-what-happened-who-was-impacted-and-how-to-delete-your-account/?sh=27872aa66491.

[3] *See* Julien Tromeur, *Reality Check: How is the EU Ensuring the Data Protection in XR Technologies,* Digit. Constitutionalist (Jan. 25, 2024), https://digi-con.org/reality-check-how-is-the-eu-ensuring-data-protection-in-xr-technologies/.

XR systems to minimize the risk of privacy violations. Finally, Section V provides concrete policy recommendations, including data minimization and purpose limitation, user consent, data access and control mechanisms, privacy-enhancing technologies, and broader antitrust protections.

I. How XR Devices Collect and Process Data

Before we consider the privacy implications of XR, it is important to understand how and why data is collected, processed, and stored by XR companies. XR and its accompanying data collection capabilities differ in important ways from non-XR technologies such as smartphones, computers, cameras, and other data-driven devices.

First, XR devices collect immense amounts of data, both in scope and scale. A single XR device must collect and process immense quantities of data to create socially and psychologically immersive experiences for users.[4] This data includes highly accurate recordings of a person's surroundings, their biometric information, geolocation, and other demographic information, especially when they interact with the device using an avatar.[5] When someone puts on an XR headset, for example, inward-facing cameras scan their pupils, outward-facing cameras take pictures of their surroundings, microphones record their voice, and gyroscopes analyze their movements.[6] Non-XR devices can collect similar forms of data as well. The main difference is that for XR devices to function properly, they *must* collect all this data.[7]

Second, besides collecting all these different types of data to create immersive experiences, XR devices aggregate data both on the device itself and on external servers. The aggregation does not only happen at a single point in time but on a continuous basis as users operate XR devices.[8] This data does not often remain in one place under the control of one entity, however. It is typically processed further, both on and off the device, depending on the situation.[9] While raw sensor data is sometimes transmitted off the device to its manufacturer to improve existing device functions, a specific app on an XR device might separately capture data that flows to the developer's own servers. As with other devices, when people use XR, they enable several layers of data collection and processing both on- and off-device, by the device manufacturer as well as any other developers whose applications and features they access through the device.

---

[4] Brittan Heller, *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law,* 23 Vand. J. Ent. & Tech. L. 1 (2020), https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/1/.

[5] *Id; see also* Zhihui Zhang, Josep M. Fort, & Lluis Giménez Mateu, *Facial Expression Recognition in Virtual Reality Environments: Challenges and Opportunities,* 14 Frontier Psych. (2023), https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2023.1280136/full.

[6] Jeff Shepard, *What Sensors Are Used in AR/VR Systems?,* Sensor Tips (May 19, 2022), https://www.sensortips.com/featured/what-sensors-are-used-in-ar-vr-systems-faq/.

[7] *Id.*

[8] Indeed, as Brittan Heller has cautioned:

> Immersive technology is not limited to static measurements or images because sensors track how users move over a period of time. Furthermore, it constantly records changes in the environment and how that change may impact the user's condition over time. It is not just the user's real identity, which is mostly already known by the platforms of immersive experiences from his or her financial information and account information. Instead, it is a new quality of information that is comprised of the user's real identity combined with their reactions to particular stimuli — indicating what someone uniquely may think and like and want.

Heller, *supra* note 4, at 28.

[9] *Id.*

Third, XR devices pose a privacy risk not only to users but also to bystanders who are unwittingly caught in their data collection range.[10] With a growing market for XR devices meant for daily use, such as the Apple Vision Pro, bystanders who have not consented to the capture of their information are now vulnerable to privacy violations from any direction.

XR devices must store and process a wealth of information to function, and yet control over these sizeable dataflows tends to lie with manufacturers and developers, not users or others whose information gets captured by XR tech. While the scale and scope of data is different than with non-XR technologies, the lack of user control and agency over data is nothing new. This level of non-user access to intimate data can create diverse harmful scenarios for data subjects. The wealth of information stored and processed by XR devices can make them prime targets of hackers and other bad actors wanting to access this data.[11] Data breaches are common occurrences with existing devices, so we might expect more of this to happen as XR use grows.[12] One manufacturer's poor security practices or irresponsible privacy policies could give a multitude of parties, including criminals and overreaching governments, improper access to treasure troves of highly sensitive information.

But the dangers to data privacy go beyond bad actors and data insecurity. Seemingly benign third-party access requests, whether from developers, government agencies, or app developers, could ultimately infringe on users' autonomy and dignity rights, especially when they are unaware and do not consent to such requests. If users cannot control their own XR dataflows or have ways of monitoring and contesting them, they are vulnerable to data exploitation by commercial and state actors who see opportunities for profit and power in the reams of sensitive, real-time data generated by XR devices.

II. XR as a Surveillance Mechanism

In the current technology ecosystem, there is a genuine risk that XR data may be used to surveil both users and non-users of these devices. Non-immersive technologies and digital services are already designed to capture as much human behavior as possible and transform it into profitable data insights that determine where to target ads, where to serve content, and where to maximize user engagement, keeping people glued to their devices as unwitting participants in a personalized panopticon.[13]

Surveillance capitalism is the "unilateral claiming of private human experience as free raw material for translation into behavioral data."[14] Google was the first to understand that it could capture large amounts of behavioral data — in excess of what was necessary to run its search engine — and sell the

---

[10] *See* Drew May, *Do VR Headsets Give Bystanders Enough of a Heads Up?,* Samuelson-Glushko Can. Internet Pol'y & Pub. Int. Clinic (June 21, 2024), https://www.cippic.ca/articles/do-vr-headsets-give-bystanders-enough-of-a-heads-up#.

[11] *Hacking the Metaverse,* LSU Media Ctr. (Nov. 8, 2022), https://www.lsu.edu/mediacenter/news/2022/11/virtualreality_safety_metaverse_cybersecurity_hacks.php.

[12] *Who's Hacked? Latest Data Breaches and Cyberattacks,* Cybercrime Mag. (2024), https://cybersecurityventures.com/intrusion-daily-cyber-threat-alert/.

[13] *See* Thomas McMullan, *What Does the Panopticon Mean in the Age of Digital Surveillance?,* Guardian (July 23, 2015, 3:00 PM), https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham.

[14] John Laidler, *High Tech Is Watching You,* Harv. Gazzette (Mar. 4, 2019), https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/. For more reading, see Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (2018).

data to advertisers.[15] Google also knew, however, that the average consumer would likely not consent to this collection, repackaging, and selling of their data,[16] so its methods were initially undetectable.[17] Now, both the private and public sectors actively benefit from surveillance capitalism.[18] While policymakers and stakeholders worldwide seem to just be catching up with appropriate legislation to deal with the privacy nightmare that surveillance capitalism poses, XR threatens to upend this progress.

A. Commercial Surveillance

As described above, XR devices' highly specific and personal data capture fills companies' data repositories which they can then repackage and sell to the robust data broker industry.[19] XR manufacturers and developers have the potential to create a commercial surveillance system of unprecedented proportions that advertisers and other private companies can exploit for profit.

Advertisers were Google's original target buyers when Google discovered that it could sell behavioral data beyond the scope of the services it provided to users.[20] Behavioral data refers to information that is collected about how users interact with digital products, services, or platforms.[21] This data provides insights into users' actions, preferences, habits, and patterns of behavior, both online and offline.

While pre-XR data collection has already raised plenty of privacy concerns, the characteristics and functions of previous devices have placed limits on the kinds of data that internet, gaming, and social media companies can distribute or sell. However, with the emergence of XR headsets, tech companies can now access biometrics such as body posture, eye gaze, pupil dilation, haptics, facial expressions, skin color, and even instances where a user blushes.[22] XR headsets can also collect more precise geolocation data than previous technologies since they operate on a continuously recording camera to integrate virtual worlds with a user's surroundings.[23] Aggregation of all this data gives tech companies a more complete picture of users' daily lives, which makes the information more valuable.

---

[15] Laidler, *supra* note 14.

[16] *Id.*

[17] *Id.*

[18] Surveillance capitalism has allowed the data broker industry to become very lucrative, where data brokers pay private data companies for data and then resell it to third companies, which are often advertisers. This has become an avenue through which private companies can derive profit in addition to their regular services. The public sector, too, benefits from surveillance capitalism since government entities can subpoena or request data from companies that have become more and more sophisticated in their data collection.

[19] *See generally Data Brokers,* EPIC, https://epic.org/issues/consumer-privacy/data-brokers/ (last visited May 1, 2024); Last Week Tonight, *Data Brokers: Last Week Tonight with John Oliver,* YouTube (Apr. 10, 2022), https://www.youtube.com/watch?v=wqn3gR1WTcA.

[20] Laidler, *supra* note 14.

[21] *What Is Behavioral Data and Data Analytics?,* Indicative, https://www.indicative.com/resource/what-is-behavioral-data-and-behavioral-analytics/ (last visited May 6, 2024).

[22] While IoT smart devices, especially wearables like Apple Watches and Fitbits, started the trend towards biometric data collection and aggregation with non-biometric data to inform analytics, XR has the additional layer of being able to capture surroundings and external stimuli. Alyson Klein, *VR Devices Collect 'Intimate' Data, Lack Private Protections. Should Schools Invest?,* EducationWeek (Nov. 18, 2022), https://www.edweek.org/technology/vr-devices-collect-intimate-data-lack-privacy-protections-should-schools-invest/2022/11.

[23] Mobile-based data, conversely, is more limited since cameras do not need to run continuously to operate a phone or computer. However, with XR, cameras need to be on always to create the extended reality. This continuous feed builds a more detailed environment than traditional mobile devices.

In 2022, Common Sense Media conducted a study in which privacy researchers reviewed the most popular VR headsets in the market to understand the scope of their privacy protections.[24] Researchers found that "[a]ll of the VR devices state[d] in their privacy policies that they can use sensitive biometric data collected in virtual reality for commercial purposes that include selling their data to third parties, sending users third-party marketing communications, displaying targeted advertisements, tracking users across other sites and services over time, and creating advertising profiles for data brokers."[25] Newer VR devices marketed for everyday life, like the Apple Vision Pro, will further increase privacy risks since these headsets often capture bystanders as well.[26]

XR headsets can allow private advertisers or any private party seeking to use the data for profit to surveil individuals' daily lives to an unimaginably invasive degree. This kind of monitoring, which leads to users being fed highly personalized and targeted advertisements, deprives consumers of control over personal data and can result in heightened security risks, manipulation, and discrimination at the hands of private companies.

The extent of the commercial surveillance apparatus will depend largely on the amount of competition in the XR space. Like existing platforms, virtual worlds are digital multi-sided platforms with strong network effects that can enable a few players to dominate this space.[27] Thus, if strong ex-ante antitrust measures are not incorporated in the XR space, it is likely that a few platforms will have unique access to their users' personal data, making the entry or expansion of competitors more difficult and further centralizing the control of users' data.[28] With tech companies like Meta and Google already dominating the XR space, it is expected that they will persevere in gaining more power in this space to entrench their dominance in adjacent advertisement-related markets.

B. Government Surveillance

XR data collection also creates a treasure trove of information for governments to use (or misuse) as they please. If more XR headsets meant for daily use, like the Apple Vision Pro, continue to expand into the market, these devices and their data become a powerful tool, especially as they are integrated into government-run surveillance units and by companies turning over their data in public-private partnerships.

Law enforcement and military agencies are prime candidates for XR data surveillance and often have specific procurement budgets to use to license these products. In China, for example, police forces are using AR glasses in combination with artificial intelligence and facial recognition software to help officers identify suspects in real time.[29] The U.S. Army announced in 2020 that it would invest in

---

[24] These VR headsets are the Microsoft Hololens 2, HP Reverb G2, HTC Vive Cosmos Elite, PlayStation VR, Meta Quest 2 (formerly Oculus Quest 2), Valve Index, and Primax Vision 5K Super. These devices make up close to 100 percent of the marketplace for VR. Alyson, *supra* note 22.

[25] Privacy of Virtual Reality: Our Future in the Metaverse and Beyond, Common Sense Media (2022), https://www.commonsensemedia.org/sites/default/files/research/report/privacy-of-virtual-reality-our-future-in-the-metaverse-and-beyond.pdf.

[26] Apple Vision Pro, Apple, https://www.apple.com/apple-vision-pro/.

[27] Robin S. Crauthers, *Antitrust: Into the Metaverse,* Wilson Sonsini Goodrich & Rosati, https://www.wsgr.com/en/insights/antitrust-into-the-metaverse.html (last visited Sep 12, 2024).

[28] *Id.*

[29] Bernard Marr, *How Augmented & Virtual Reality Is Used in Law Enforcement and the Military,* Bernard Marr & Co. (Oct. 11, 2021), https://bernardmarr.com/how-augmented-virtual-reality-is-used-in-law-enforcement-and-the-military/.

40,000 pairs of MR goggles equipped with thermal and low-light sensors to more quickly identify friends from foes.[30] In Russia, law enforcement is also adopting AR glasses equipped with facial recognition technology.[31] Russia's prior history of using facial recognition cameras may indicate that the glasses will be used to curb dissent in addition to being used as public safety tools.[32]

In some cases, governments can even access private XR data without direct access to the devices.[33] Many tech and data companies have their own procedures for cooperating with government requests without the need for formal protocols, such as subpoenas, warrants, or court orders. Across the U.S., these privately designed procedures are called legal requests, and they allow the government to access device and account data, financial identifiers, and data sought in relation to an emergency.[34] In the EU, the adoption of the GDPR has restricted how public authorities can use legal grounds to request personal data.[35] However, in the U.S., and in other countries without comprehensive data privacy rules, governments are still able to coopt individuals walking around with XR devices as unwitting agents of civilian surveillance.

Privacy concerns with government legal requests will be amplified by XR technology. First, with legal requests that involve emergencies, the term "emergency" itself remains an overbroad term that can be defined very flexibly for the benefit of law enforcement. There is no standard definition or criteria across the industry to validate whether a government request concerns a genuine emergency. Apple, for example, requires that emergency requests within the U.S. "relate to circumstances involving imminent danger of death or serious physical injury to any person."[36] However, when filling out a request form, there is no real vetting process outlined (other than Apple may, not will, reach out to a supervisor to confirm the emergency's details) to verify whether the emergency is indeed one of the nature that Apple requires it to be.[37] This means that government entities can embellish details or be

---

[30] Kyle Mizokami, *'Mixed Reality' Goggles Will Give U.S. Army Soldiers Super Vision,* Popular Mechanics (Feb. 13, 2020), https://www.popularmechanics.com/military/a30898514/mixed-reality-goggles-army/. The Integrated Visual Augmentation System (IVAS) is a helmet-mounted combined night vision/thermal augmented reality and situational awareness tool derived from the Microsoft Hololens. The IVAS is set to hit its final testing phases in 2024. Todd South, *Army's Mixed Reality Device Nears Fielding with Final Testing in 2024,* Army Times (Dec. 29, 2023), https://www.armytimes.com/news/your-army/2023/12/29/armys-mixed-reality-device-nears-fielding-with-final-testing-in-2024.

[31] *Russia to Arm Police with AR Face Recognition Glasses by 2020,* Moscow Times (May 24, 2019), https://www.themoscowtimes.com/2019/05/24/russia-to-arm-police-with-ar-face-recognition-glasses-by-2020-a65720.

[32] Lena Masri, *Facial Recognition Is Helping Putin Curb Dissent with the Aid of U.S. Tech*, Reuters (Mar. 28, 2023), https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/. Russia's surveillance camera system before the AR goggles, dubbed Smart City, "was touted by city officials as a way to streamline [the city's] public safety systems. In recent years, however, its 217,000 surveillance cameras, designed to catch criminals and terrorists, have been turned against protestors, political rivals, and journalists." Masha Borak, *Inside Safe City, Moscow's AI Surveillance Dystopia,* Wired (Feb. 6, 2023), https://www.wired.com/story/moscow-safe-city-ntechlab/.

[33] Matt O'Brien, *How Big Tech Created a Data "Treasure Trove" for Police,* Denver Post (June 26, 2021), https://www.denverpost.com/2021/06/26/big-tech-data-police/.

[34] An emergency is commonly defined as relating "to circumstances involving imminent danger of death or serious physical injury to any person." *Apple Transparency Report, Government and Private Party Requests,* Apple, https://www.apple.com/legal/transparency/pdf/requests-2022-H1-en.pdf.

[35] Esther van Duin, *GDPR in the Public Sector: The Biggest and Smallest Changes,* Deloitte, https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-in-the-public-sector.html.

[36] *Apple Transparency Report, Government and Private Party Requests,* Apple, https://www.apple.com/legal/transparency/pdf/requests-2022-H1-en.pdf.

[37] *Emergency Government/Law Enforcement Information Request,* Apple, https://www.apple.com/legal/privacy/le-emergencyrequest.pdf.

vague in ways that push companies to overshare.[38]

Tech companies often have a tendency to be extremely cooperative with law enforcement.[39] The government is often allowed access to non-content data such as user names, addresses, and contact information, even if it is encrypted.[40] Tech companies also store and can, in some cases, access and share user content from emails, texts, photos, videos, contact lists, calendars, and documents.[41] Apple has stated that it will even voluntarily release personal data "if Apple believes in good faith that [there] is a valid emergency."[42] In 2022, which is the latest available year of Apple's Transparency Report, Apple provided data for 87% of its emergency requests within the U.S.,[43] and 90% of emergency requests worldwide.[44] Now, with XR headsets that store highly accurate data about your surroundings, hands, eyesight, and appearance,[45] the groundwork is laid out for these requests to become a bounty of biometrics and highly accurate geolocation data.

The lack of a proper vetting process means that tech companies have been subject to data hacks where cybercriminals pose as government officers and acquire data through fraudulent emergency information requests.[46] XR's constant and vast data collection leaves even more highly personal data vulnerable to these kinds of cyberattacks going forward.

III. Solutions and Limitations of Existing Privacy Regulations

Transparency is the common band-aid solution that many companies promote as a response to mounting privacy concerns. Many tech companies release transparency reports that provide a lot of insight into how a company is using user data. However, the problem remains that knowing how a company uses user data leaves little recourse to challenge whether that data should be collected, stored, or distributed in the first place.

While XR presents novel challenges to existing information privacy regimes, these challenges are in magnitude, not in kind. The core issue, which remains consistent across data-based technologies, is that users lack awareness and control over their own data, and do not benefit from its financial value. Luckily, this means that law and policymakers interested in protecting data privacy in the XR space will not be starting from scratch. This Section applies the foundational principles which animate

---

[38] The government also often cites national security or other reasons not to share more details about an ongoing investigation when making these requests, which limits how specific they can be (and means requests are often over-broad and nonspecific).

[39] Jack Nicas, *What Data About You Can the Government Get From Big Tech?,* N.Y. Times (June 14, 2021), https://www.nytimes.com/2021/06/14/technology/personal-data-apple-google-facebook.html.

[40] *Id.*

[41] *Id.*

[42] *Apple Transparency Report, Government and Private Party Requests,* Apple, https://www.apple.com/legal/transparency/pdf/requests-2022-H1-en.pdf.

[43] *Government Information Requests — Apple (US),* Apple, https://www.apple.com/legal/transparency/us.html.

[44] *Emergency Requests,* Apple, https://www.apple.com/legal/transparency/emergency-requests.html.

[45] *Apple Vision Pro Privacy Overview,* Apple, https://www.apple.com/privacy/docs/Apple_Vision_Pro_Privacy_Overview.pdf.

[46] William Turton, *Tech Giants Duped Into Giving Up Data Used to Sexually Extort Minors,* Bloomberg (Apr. 26, 2022), https://www.bloomberg.com/news/articles/2022-04-26/tech-giants-duped-by-forged-requests-in-sexual-extortion-scheme?embedded-checkout=true.

much of existing privacy regulations — the Fair Information Privacy Principles (FIPPS).[47] Meaningful protections to ameliorate privacy risks that will inevitably emerge from XR must come from the angle of data minimization and propose limitations, as well as empowering individual participation in decisions concerning their own dataflows.

A. Data Minimization and Purpose Limitation

Data minimization is the principle by which data processing companies should be "limiting the collection, use, transfer, and retention of personal information to that which is reasonably necessary."[48] With XR, data collection is reasonably necessary when it is directly related to fulfilling a consumer's requests regarding their use of the XR device.[49] Purpose or use limitation requires companies not to disclose, share, or use personal data of others for purposes other than those they communicate to users, except with user consent or as required by law.

Despite these decades-old principles, many tech companies engage in secondary data collection uses, primarily for advertisement purposes and by sharing it with government agencies, that are often disconnected from the company's main service. These secondary data practices fall outside the scope of data minimization, as they are not reasonably necessary for the functioning of the device, and are additional uses of data to increase shareholder value.

Globally, existing privacy laws can serve as models to protecting privacy against the kinds of incursions XR facilitates. These laws have the dual function of protecting XR users against both commercial and government surveillance, since a significant amount of government surveillance relies on private sector data collection.

Europe

The most influential framework for regulating privacy in the private sector is the EU's General Data Protection Regulation (GDPR), which went into effect in May 2018.[50] Importantly, the GDPR imposes its privacy principles on any organization worldwide that collects data related to people in the EU.[51]

The GDPR establishes strong data minimization principles for data collection and access by private and government entities. Article 5 (c) states that personal data shall be "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed."[52] In the same line, Article 5 (b) also establishes the principle of purpose limitation, which states that personal data shall

---

[47] *Fair Information Privacy Principles (FIPPS),* Fed. Priv. Council, https://www.fpc.gov/resources/fipps/.

[48] Sara Geoghegan, *Data Minimization: Limiting the Scope of Permissible Data Uses to Protect Consumers,* EPIC (May 4, 2023), https://epic.org/data-minimization-limiting-the-scope-of-permissible-data-uses-to-protect-consumers/.

[49] *Id.*

[50] *What is GDPR, the EU's new data protection law?,* GDPR.EU, https://gdpr.eu/what-is-gdpr/ (last visited May 1, 2024).

[51] The size and scale of the EU incentivizes every company that wants to be a global player to need to figure out how to comply with GDPR. *Id.*

[52] *Id.*

be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."[53]

These principles are complemented by the GDPR's establishment of lawful ways to process data from data subjects in Article 6.[54] Based on this Article, the main purposes by which tech companies are justified in processing personal data are with the consent of data subjects, that the processing is necessary for the performance of a contract, or that it is necessary for the purpose of the legitimate interests they are pursuing. Notably, all these justifications place limitations on the processing of data for secondary purposes like advertising. For example, companies cannot justify their processing based on the necessity of their legitimate interests when such interests are overridden by the fundamental rights and freedoms of the data subject.[55] Since it is unlikely that companies will be able to process vast troves of personal data for advertising purposes without infringing on data subjects' rights to dignity and autonomy, this justification cannot be used by companies to legally validate their surveillance practices.

At the same time, in a 2022 decision, the European Data Protection Board (EDPB) established that tech companies like Meta cannot use their contract obligations as a legal justification under the GDPR for processing data for advertising purposes either.[56] According to the EDPB, Meta's Terms of Service do not provide for any contractual obligation binding the company to offer personalized advertising to its users, which shows that, at least from the users' perspective, this kind of processing is not necessary to perform the contract.[57]

Together with the limitations placed by the GDPR to obtain meaningful consent, which we explain below, these principles and their application by European authorities already raise questions as to the legality of processing personal data to advance tech companies' behavioral advertising models. Considering that XR headsets currently available on the market (such as the Apple Vision Pro or the Meta Quest) collect highly sensitive data and are not meant for advertising or surveillance, tech companies that trade in the EU will potentially violate the GDPR if they choose to process XR data for commercial surveillance purposes.

Another European regulation intertwined with XR is the EU AI Act (AI Act),[58] which the European Parliament formally adopted in 2024. The AI Act works in tandem with the GDPR and would apply to XR products that incorporate AI. The AI Act creates different regulations for different AI systems, which reflect their degree of risk.[59] The Act bans certain "unacceptable risk" AI programs, including "biometrical identification and categorization of people".[60] Since most of the data collected by XR

---

[53] Art. 5 GDPR — Principles relating to processing of personal data, General Data Protection Regulation (GDPR), https://gdpr-info.eu/art-5-gdpr/ (last visited Sep 12, 2024).

[54] Art. 6 GDPR — Lawfulness of processing, General Data Protection Regulation (GDPR), https://gdpr-info.eu/art-6-gdpr/ (last visited Sep 12, 2024).

[55] Art. 5 GDPR — Principles relating to processing of personal data, *supra* note 53.

[56] *Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR),* Euro. Data Prot. Bd., https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-32022-dispute-submitted_en (last visited Sep 12, 2024).

[57] *Id.*

[58] The EU Artificial Intelligence Act, https://artificialintelligenceact.eu.

[59] *EU AI Act: First Regulation on Artificial Intelligence,* Euro. Parliament (June 8, 2023), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence#next-steps-7.

[60] *Id.*

devices is biometric, this may limit XR companies' ability to incorporate AI systems into their platforms or the processing and collection of data they enable.

United States

In the U.S., where most XR companies operate, there is no comprehensive and up-to-date federal privacy law, though several attempts have been made to fill this void. The American Data Privacy and Protection Act (ADPPA), which was introduced in 2022, aimed to provide U.S. consumers with foundational data privacy rights. The ADPPA established "a duty of loyalty on covered entities, including a data minimization limitation that prohibits [an] entity from collecting, processing, or transferring covered data unless it is reasonably necessary and proportionate."[61]

However, this bill failed to advance, in part because of the limitations it placed on its private right of action.[62] Despite this, its provisions could become law by being included in another bill in the future.[63] Like the GDPR, a bill like this would limit secondary uses of data that enable private and government surveillance. Yet, the ADPPA data minimization practices relied on a reasonableness standard. As different entities argue different notions of what form of data processing is "reasonable" in various contexts, that provision could be applied inconsistently across XR devices and services. Future legislation wanting to revive the ADDPA provisions should be hesitant to adopt a reasonableness standard that risks protecting commercial interests at the expense of meaningful consumer privacy.

The California Consumer Privacy Act (CCPA) and other similar state laws give consumers more control over the personal information that businesses collect about them.[64] Although the CCPA is commonly known as a GDPR-style law, it has significant limitations in comparison to the GDPR that may affect the level of protection for U.S. users of XR. For example, while the GDPR provides that the processing of personal data will only be lawful if one of the Article 6 grounds is fulfilled, the CCPA does not set a list of grounds that businesses must follow before collecting, selling, and disclosing personal information. In fact, the CCPPA "only provides for a posteriori mechanism, namely allowing customers to opt out of the sale and disclosure of their personal information or to ask for erasure of the information."[65]

The CCPA is not the only state-level data protection regulation that could apply to XR. The Illinois Biometric Information Privacy Act (BIPA) helps ensure that individuals are in control of their biometric data and requires informed consent before private companies can collect the data.[66] The law also prohibits companies from selling or otherwise profiting from collected biometric data. However, the law only applies to "biometric identifiers," which it defines as "scans" such as fingerprints and eye scans that can be used to identify the user. It is unclear whether much of the biometric information that XR devices collect to function — such as eye-tracking and bodily motion data — would fall under the

---

[61] Geoghegan, *supra* note 48.

[62] Bill Tolson, *Still No Federal Data Privacy Law: What Happened to the ADPPA?,* Smarsh (Dec. 1, 2023), https://www.smarsh.com/blog/thought-leadership/no-federal-data-privacy-law-what-happened-ADPPA (last visited Sep 12, 2024).

[63] *Id.*

[64] California Consumer Privacy Act (CCPA), State of California - Department of Justice - Office of the Attorney General (2018), https://oag.ca.gov/privacy/ccpa (last visited Sep 12, 2024).

[65] *Comparing Privacy Laws: GDPR v. CCPA,* Euro. AI All. https://futurium.ec.europa.eu/en/european-ai-alliance/open-library/comparing-privacy-laws-gdpr-v-ccpa (last visited Sep 12, 2024).

[66] 740 Ill. Comp. Stat. Ann. 14/15; *Biometric Information Privacy Act*, ACLU, https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa (last visited Sept. 12, 2024)

law, so long as they are not used to identify an individual user.[67] If more states adopt similar biometric data laws to protect the privacy of individuals in the XR space, they should specify that the information collected by XR devices falls under the definition of biometric data.[68]

Additionally, California's Age-Appropriate Design Code Act (ADCA) presents interesting strategies for XR regulation and privacy. Passed in September 2022, ADCA applies to websites and online services that are "likely to be accessed" by users under 18 years of age. Before offering an online service to the public, a business that qualifies must complete a Data Protection Impact Assessment (DPIA), which addresses how the service uses children's personal information and the risks to children, and whether and how the service collects or processes sensitive personal information of children.[69] Many XR platforms likely fall under the ambit of ADCA. However, the Northern District of California — applying intermediate scrutiny — recently held that the DPIA provision likely violates the First Amendment and enjoined the Act.[70] The Ninth Circuit, on appeal, applied First Amendment strict scrutiny to the DPIA provision and affirmed the injunction.[71] Thus, it is unlikely that this form of mandatory disclosure is consistent with the First Amendment.

Compared to Europe, the United States faces a long road to effective privacy protection in the XR space. Without a federal privacy law and with various state laws facing significant limitations to safeguard users' privacy rights, it is likely that the advertising-centered business model of tech companies will be replicated in the XR space. Because of the scope and scale of data collection enabled by XR devices, policymakers in the U.S. should seize the momentum created by XR technologies to introduce new legislation to prevent harmful surveillance in the virtual world. Laws that set a higher bar for XR data practices could establish protections that flow down to non-immersive technologies similarly producing, processing, and profiting from personal data.

B. Empowering Individual Participation

Alongside using privacy values such as data minimization and purpose limitation to address surveillance, there are benefits to democratizing data policy by empowering users to engage more actively in governance decisions.[72] Such empowerment is a valuable strategy to protect users against potential misuse or exploitation.[73] It is possible to define two crucial tenets of individual participation for protecting data privacy in XR spaces: consent management, and meaningful access and control.

Rethinking Consent Management

Human autonomy plays a pivotal role in promoting consumer well-being,[74] making consent essential in

---

[67] Daniel Berrick & Jameson Spivack, *Understandsing Extended Reality Technology & Data Flows: Privacy and Data Protection Risks and Mitigation Strategies,* Future of Priv. F. (Nov. 17, 2022), https://fpf.org/blog/understanding-extended-reality-technology-data-flows-privacy-and-data-protection-risks-and-mitigation-strategies/.

[68] XRA, https://xra.org/public-policy/biometric-data/.

[69] Cal. Civ. Code § 1798.99.31

[70] NetChoice, LLC v. Bonta, 692 F. Supp. 3d 924, 951 (N.D. Cal. 2023), *aff'd in part,* 2024 WL 3838423 (9th. Cir. 2024).

[71] NetChoice, LLC v. Bonta, No. 23-2969, 2024 WL 3838423 (9th Cir. Aug. 16, 2024).

[72] *Protecting Privacy,* Univ. of Va. (2024), https://research.virginia.edu/irb-sbs/protecting-privacy.

[73] For an excellent piece on data stewardship and fiduciary relationship, see Sarah Rosenbaum, *Data Governance and Stewardship: Designing Data Stewardship Entities and Advancing Data Access,* 45 Health Serv. Rsch. 1442 (2010).

[74] Gary Burkhardt et al., *Privacy Behaviour: A Model for Online Informed Consent,* 186 J. Bus. Ethics 237 (2023).

the XR world.[75] Obtaining consent is a "continuous process."[76] Rather than being a single event of mere disclosure or notice, meaningful consent must involve a mechanism for providing clear, transparent, and understandable information about the data life cycle, including the collection, use, retention, and sharing of data.

According to the GDPR, consent must be freely given, specific, informed, unambiguous, and reversible.[77] This means that consent should be free from jargon-heavy and obscure terminology with clear communication, user-friendly interfaces, and consent records. This enables users to gain necessary "knowledge and awareness" about purposes, data types, and their implications.[78] This ongoing consent process also involves "minimizing the potential for coercion or undue influence and providing the [user] sufficient time to consider participation as well."[79] Otherwise, obtaining consent may result in "consent desensitization or fatigue," making users disinterested or leaving them feeling powerless when faced with consent requests.[80]

Design Justice advocates argue that the concept of "notice and consent" in digital contexts is fundamentally flawed because it is overly individualistic, placing an unrealistic burden on individuals to understand and navigate complex data practices.[81] This model also fails to account for the systemic power imbalances and structural inequities that can undermine meaningful consent.[82]

The immersive virtual worlds and the depth of personal data involved present unique privacy challenges because "XR environments can generate high-fidelity records of our behaviors, mental states, and trait-level dispositions" that go far beyond what a regular person could witness and observe in the real world.[83] This data trove is continuously generated and retained, creating a heightened risk of profiling, manipulation, and covert exploitation compared to isolated public imagery. Likewise, unlike

---

[75] In the UK and the EU, disclosed personal data may be processed under several legal bases, one of which is consent. Regulation 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), art. 51, 2016 O.J. (L 119) 33 (EU); Data Protection Act, 2018 (Act No. 12/2018) (UK).

[76] Sara Manti & Amelia Licari, *How to Obtain Informed Consent for Research,* 14 Breathe 145 (2018).

[77] Regulation 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 O.J. (L 119) 33 (EU). However, for more on the contextual nature of consent, see Helen Nissenbaum, *A Contextual Approach to Privacy Online,* 140(4) Daedalus 32 (2011).

[78] Data collected in this way can be used to track patterns, which can identify sensitive medical data (e.g., eye tracking) for individuals that could be used to discriminate during job interviews, access financial information, or other activities that currently use biometric data for identity authentication when this data is stored and sold to third parties. While this may be a helpful feature for some, the implications on user privacy, and ultimately safety, should be communicated clearly.

[79] Sara Manti & Amelia Licari, *How to Obtain Informed Consent for Research,* 14 Breathe 145 (2018).

[80] Burkhardt et al., *supra* note 74.

[81] Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies (2018).

[82] Sasha Costanza-Chock, Design Justice: Community-Led Practices to Build the Worlds We Need (2020). Additionally, researchers like Helen Nissenbaum and Solon Barocas have questioned the applicability of traditional informed consent frameworks in contexts where data flows and potential uses are often unpredictable and can evolve over time. They argue for a broader consideration of contextual integrity and the need to align data practices with societal norms and expectations. *See* Solon Barocas & Helen Nissenbaum, *Big Data's End Run Around Anonymity and Consent, in* Privacy, Big Data, and the Public Good 44 (Julia Lane, Victoria Stodden, Stefan Bender, & Helen Nissenbaum eds., 2014).

[83] Michael Madary & Thomas K. Metzinger, *Real Virtuality: A Code of Ethical Conduct Recommendations for Good Scientific Practice and the Consumers of VR-Technology,* 3 Frontiers Robotics AI 3 (2016).

fleeting public snapshots, XR's repurposable data corpus,[84] combined with other data sources, could be adversely more consequential in profound ways.

A traditional understanding of privacy, rooted in data protection and consent management concepts, might not be commensurate with the novel challenges posed by the seamlessly blended physical and virtual world that XR enables. This requires a shift from a narrow focus on data privacy to a broader understanding of privacy as a fundamental enabler of personal autonomy, self-expression, and the freedom to explore and experiment without fear of unwanted surveillance, manipulation, or exploitation.[85]

While GDPR's strict requirements to obtain meaningful consent from data subjects may guard against infractions upon the above-mentioned privacy values, the applications of these rules in the XR space are not straightforward. Because of this, some have argued that the GDPR should be revisited and tailored to the XR space by clarifying the application of its principles to biometric data in the Metaverse and VR interactions.[86]

For example, Article 9 of the GPDR states that the processing of biometric data for the purpose of uniquely identifying a natural person is prohibited.[87] However, it is not clear what types of biometric data could uniquely identify an individual, as this depends on how companies process and aggregate this data with other identifiers. For example, Meta's 'Oculus Privacy Policy' seems to view hand-tracking data as not uniquely identifying users because this data is deleted after processing, and its processing is linked with identifiers different from the user's ID account.[88] In this way, "the intent behind data processing emerges as a significant criterion in determining whether such data should be categorized under Article 9", which makes it extremely hard to evaluate companies' compliance with these rules.

The problem is that tech companies can easily rearrange their processing schemes of biometric data to identify individual users. A study found that a VR system correctly identifies 95% of users when trained on less than 5 minutes of tracking biometric data, like head movement, per person.[89] Adapting the GDPR to the XR space should reconsider biometric data as being able to uniquely identify individuals by default, as opposed to making it dependent on companies' original processing purposes.

Additionally, a company can only process biometric data under Article 9 by obtaining explicit consent from the data subjects, which is a stricter type of consent than the one required for processing non-sensitive data. According to the EDPB, explicit consent must be an express statement; therefore, "ticking a box that says 'I hereby consent to process [...]' followed by the relevant data will comply with the

---

[84] A repurposable data corpus is a collection of data that can be reused, repackaged, and repurposed across various XR applications or experiences, and is possible because of XR's data scope, scale, and aggregation capabilities.

[85] Theories such as Helen Nissenbaum's 'contextual integrity' and Woodrow Hartzog's notion of 'privacy as an affordance,'or the idea of "data sovereignty, rationalize such reconceptualizing the privacy in terms of individual participation. *See* Helen Nissenbaum, *A Contextual Approach to Privacy Online,* 140(4) Daedalus 32 (2011); Hartzog, *supra* note 81.

[86] Vasilis Xynogalas & M R Leiser (Mark), *The Metaverse: Searching for Compliance with the General Data Protection Regulation,* 14 Int. Data Priv. Law 89, 105 (2024).

[87] Art. 9 GDPR — Processing of special categories of personal data, General Data Protection Regulation (GDPR), https://gdpr-info.eu/art-9-gdpr/ (last visited Sep 12, 2024).

[88] Xynogalas & Leiser (Mark), *supra* note 86 at 95.

[89] Mark Roman Miller et al., *Personal Identifiability of User Tracking Data During Observation of 360-Degree VR Video,* 10 Sci. Rep. 1 (2020).

GDPR."[90] The problem is that XR devices collect many different categories of biometric data, making it nearly impossible for users to assess the importance of giving explicit consent for each category. Considering that even GDPR's template for privacy notices seems unnecessarily lengthy and may be easily ignored,[91] XR technologies could make consent requirements even less meaningful than they already are.

At the same time, it is difficult to assess which types of data are truly necessary to enable the full XR experience, challenging the GDPR's notion of "freely given" consent.[92] While it is true that biometric data can boost XR functionality to personalize users' experience (e.g., utilizing head movements and eye tracking for analytics purposes),[93] this does not mean that technological efficiency and monetization justify personal privacy trade-offs.[94] Consider the theory of "contextual integrity," which emphasizes the need to respect the norms and expectations of privacy in different contexts, even in the face of potential benefits or efficiencies.[95] For example, a video game user could consent to the collection and processing of their real-time head movement and eye-tracking while playing a game that requires them to look at certain targets and make head movements, but the same user may not consent to the same eye-tracking and head movement data being used to advertise an eyewear subscription product. In addition, unchecked data exploitation and sacrificing privacy for the sake of a better XR video game, floating apps, or a slightly more accurate map may normalize invasive practices that can chill freedom of expression and individual autonomy, inflicting long-term societal harm for short-term gains.[96]

Meaningful Access and Control

The question of "who owns your data?" is complex. Still, consumers excited about XR have legitimate expectations that tech companies will design platforms where they can exercise their own "control, autonomy, and identity."[97] Users should have access to their personal data collected during their interactions with XR applications, including usage history, preferences, and biometric data stored in account settings or profile information.[98] Even in multi-user VR experiences, users should be able to control the "visibility" of their identity and personal information to other participants through privacy settings or permissions.[99]

---

[90] Xynogalas & Leiser (Mark), *supra* note 86 at 97.

[91] Christine Utz et al., *(Un) informed Consent: Studying GDPR Consent Notices in the Field, in* Proceedings 2019 ACM SIGSAC Conf. on Computer Comm'ns Security 973 (2019).

[92] Xynogalas & Leiser (Mark), *supra* note 86 at 97.

[93] It is aptly argued that "when this information is necessary for functionality or quality of services, transparency and disclosure around how and why inferred information is used can ensure users understand the data practices in place." *See* Ellysse Dick, *Balancing User Privacy and Innovation in Augmented and Virtual Reality*, Info. Tech. Innovation Found. (Mar. 2021), https://www2.itif.org/2021-ar-vr-user-privacy.pdf.

[94] Marcel Becker, *Privacy in the Digital Age: Comparing and Contrasting Individual Versus Social Approaches Towards Privacy,* 21 Ethics Info. Tech. 307 (2019).

[95] Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (2009).

[96] Zuboff, *supra* note 14.; Hartzog, *supra* note 81.

[97] Kentbye, *XR Ethics: An XR Ethics Manifesto,* Voices VR (Nov. 5, 2019), https://voicesofvr.com/844-xr-ethics-an-xr-ethics-manifesto/.

[98] De Guzman et al., *Security and Privacy Approaches in Mixed Reality: A Literature Survey,* 52 ACM Computing Surveys 1 (2019).

[99] Divine Maloney et al., *"Talking Without a Voice": Understanding Non-Verbal Communication in Social Virtual Reality,* 4 Proceedings ACM on Human-Computer Interaction 1 (2020).

In a technical sense, since remaining anonymous in an XR context remains a near impossibility,[100] policy choices should extend beyond merely adopting the data minimization principle, as discussed earlier. Two additional rights that will be essential to achieving meaningful user control over personal data are the "right to be forgotten" and the "right to delete". By exercising these rights, users should be able to control health and activity data from MR fitness tracking devices, purchase history and personal preferences from VR shopping applications, medical records, and health information from MR healthcare applications, and gaming history and achievements from VR gaming platforms.[101]

The right to be forgotten was entrenched in EU legislation by the European Union Court of Justice in May 2014. However, there is no equivalent right in the U.S.[102] In the XR space, the right to be forgotten may be applied to outdated or irrelevant information regarding users' profiles, social interactions, and user-generated content shared within VR social networking platforms.[103] Finally, the right to delete is established by GDPR's Article 17 and may be used to remove personal data from devices or platforms' internal records.[104] In the U.S., this right is recognized by the CCPA and other similar GDPR-style state laws, but elsewhere the right to delete is a dead letter.

IV. Privacy By Design for XR

Considering the limitations of existing legislation to protect privacy in XR ecosystems, certain technological innovations can mitigate some of these privacy risks. For example, privacy-enhancing technologies (PETs) like differential privacy may ensure that individual user information cannot be easily re-identified or inferred.[105] Privacy-preserving techniques like end-to-end encryption, jammers, or blurring vision can protect sensitive data collected in XR environments during transmission and storage.[106] End-to-end encryption ensures that only intended users can read data being exchanged or created, preventing any intermediaries, even private tech companies, from accessing the data.[107] A jammer, on the other hand, is a device specifically designed to interfere with radio noise or signals.[108]

---

[100] Minderoo Centre for Technology and Democracy, Securing the Metaverse: Addressing Harms in Extended Reality (2023); *see also* Daniel Berrick & Jameson Spivack, *Unpacking the Privacy Implications of Extended Reality,* Tech Pol'y Press (Apr. 4, 2023), https://www.techpolicy.press/unpacking-the-privacy-implications-of-extended-reality/.

[101] Guo Freeman & Divine Maloney, *Body, Avatar, and Me: The Presentation and Perception of Self in Social Virtual Reality,* 4 Proceedings ACM on Human-Computer Interaction 1. *See also* Konstantina Kilteni et al., *The Sense of Embodiment in Virtual Reality,* 21(4) Presence: Teleoperators Virtual Env'ts 373 (2021).

[102] Right to Be Forgotten, Free Speech Ctr., https://firstamendment.mtsu.edu/article/right-to-be-forgotten/ (last visited Sep 12, 2024).

[103] Case C-131/12, Google Spain, SL, Google Inc v. Agencia Española de Protección de Datos, EU:C:2014:317.

[104] Mel Slater et al., *The Ethics of Realism in Virtual and Augmented Reality,* 1 Frontiers Virtual Reality 1 (2020).

[105] Daniel Berrick & Jameson Spivack, *Understanding Extended Reality Technology & Data Flows: Privacy and Data Protection Risks and Mitigation Strategies,* Future Priv. F. (Nov. 17, 2022), https://fpf.org/blog/understanding-extended-reality-technology-data-flows-privacy-and-data-protection-risks-and-mitigation-strategies/.

[106] For example, Google uses powerful face and license plate blurring technologies to protect people's privacy in Street View imagery. This technology automatically blurs identifiable faces and license plates contributed by Google users. The "Report a Problem" function allows users to request extra blurring for their faces, registration plates, entire residences, cars, or bodies. *See Google-Contributed Street View Imagery Policy*, Google (2024), https://www.google.com/streetview/policy/.

[107] *See* Mitchell Telatnik, *What Is End to End Encryption?,* Built In (Mar. 28 2023), https://builtin.com/articles/end-to-end-encryption.

[108] *An Introduction to Jammers,* JEM Eng'g., https://jemengineering.com/blog-an-introduction-to-jammers/ (last visited May 7, 2024).

In theory, jammer technology could be adapted to jam visual and audio signals that an XR device picks up in certain environments. Blurring vision could work similarly to immediately blur faces or other visual data that a user doesn't want to be shared.

These privacy-enhancing techniques like jammers and blurring can protect both users and bystanders,[109] even without requiring any action on their part.[110] Jammers might prevent an XR device from accurately capturing or transmitting certain data types, such as biometric or environmental data. While this technology may interfere with XR technologies' data collection capabilities, the onus should be on XR developers to navigate any negative impacts on functionality. As a public policy matter, companies should not be able to release products for mass commercial use that infringe so deeply on privacy. Rather, they should bear a responsibility to find solutions within their technological abilities to ameliorate privacy risks before putting products in market.

Likewise, blurring can reduce or obscure the visual fidelity of bystanders or non-consenting individuals in the XR environments. This could involve real-time image processing algorithms that detect human figures or faces in the device's field of view and apply a blurring effect to those areas. The goal is to protect the privacy of individuals who have not consented to be recorded or observed by XR devices, ensuring that their identity and actions remain anonymous.[111] Additionally, biometric data may also be stored locally on the internal storage or memory of XR devices like VR headsets or AR glasses without being transmitted or synced to any external servers or cloud services[112] or, alternatively, in the cloud/servers but associated with the individual user's account,[113] separate from other users' data.[114] As a non-technical solution, defining consent in XR requires a broader understanding of societal context, including societal awareness and regard for XR tools in public spaces.[115]

All of these built-in privacy-enhancing technologies are part of the concept of data protection by design and by default, which is also mandated by the GDPR in Article 25 and stems from broader GDPR principles like data minimization and purpose limitation. Given that Article 25 broadly refers to the implementation of "appropriate technical and organizational measures" to achieve privacy by design, however, it is ultimately up to the companies to decide which measures to embed in their systems' architecture.

EDPB's recent guidance and further interpretations of GDPR's recitals to actual industry practices can further clarify the minimum necessary privacy-enhancing technologies XR makers must implement to comply with privacy-by-design requirements. On the other hand, privacy by design could also be accomplished by following industry technical standards. To ensure that these standards incorporate

---

[109] Berrick & Spivack, *supra* note 105. *See also* Matthew Corbett et al., *BystandAR: Protecting Bystander Visual Data in Augmented Reality Systems,* 21 MobiSys '23: Proceedings 21st Annual Int'l Conference on Mobile Systems, Applications Services 370 (2023).

[110] Franziska Roesner et al., *Security and Privacy for Augmented Reality Systems,* 57 Comm'ns ACM 88 (2014).

[111] *See* Daniel Berrick & Jameson Spivack, *Unpacking the Privacy Implications of Extended Reality,* Tech Pol'y Press (Apr. 4, 2023), https://www.techpolicy.press/unpacking-the-privacy-implications-of-extended-reality/.

[112] Ellysse Dick, *Balancing User Privacy and Innovation in Augmented and Virtual Reality,* Info. Tech. Innovation Foundation (Mar. 2021), https://www2.itif.org/2021-ar-vr-user-privacy.pdf.

[113] *Id.*

[114] Jaybie A. de Guzman et al., *Security and Privacy Approaches in Mixed Reality: A Literature Survey,* 52 ACM Computing Surveys 1 (2019).

[115] Tobii has developed a VR framework that includes transparency features for obtaining user consent but lacks in providing context. *See* Ewa Luger & T. Rodden, *Terms of Agreement: Rethinking Consent for Pervasive Computing*, 25(3) Interacting with Computers 229 (2019).

strong privacy-by-design mechanisms, governments should explore intervening or overseeing the technical-standard-setting process led by tech companies.

V. Recommendations and Conclusions

Data minimization, purpose limitation, consent, meaningful access and control to personal data, and privacy by design will be key principles to ameliorate the inevitable data harms posed by XR. Although most of these principles are already contained in the EU's GDPR, policymakers and authorities must stress the importance of enforcing these laws in the XR space while also addressing their limitations. Building off decades of missed opportunities to protect personal data with earlier technologies, advocates must push U.S. law and policymakers to act now before virtual privacy harms become commonplace, as just another risk of doing business for tech companies in a new space.

A. Data Minimization and Purpose Limitation

Given that this will be the most important aspect to prevent XR companies from advancing their advertising and surveillance powers, authorities should focus on enforcing and carefully overseeing compliance with purpose limitation and data minimization requirements, including those found in the GDPR, to the XR space. Considering that XR headsets currently available on the market collect highly sensitive data and are not meant for advertising or surveillance, tech companies that trade in the EU may be infringing upon the GDPR if they further process the information for commercial surveillance purposes.

In contrast to Europe, the U.S. lacks a federal privacy law, and its most protective privacy state laws, such as the CCPA, BIPA, and ADCA, face significant limitations in ensuring users' privacy rights in the XR space. Policymakers in the U.S. should seize the momentum created by XR technologies to introduce new legislation to prevent harmful surveillance in the virtual world. This includes restricting government access to XR data without legal process to protect citizens' Fourth Amendment rights in their personal information.

B. Consent

While companies must obtain meaningful consent from users under the GDPR, the application of these rules in the XR space are not straightforward. Because of this, some aspects of the GDPR should be revisited and tailored to XR. For example, the quality of biometric data that is uniquely capable of identifying individuals should not depend on companies' original processing purposes but be presumed by default every time biometric data is processed in the XR space. Additionally, policymakers should address the limitations of giving meaningful consent. For instance, legislators could take advantage of the immersive qualities of the XR space to create new user-friendly ways to give meaningful consent and, when needed, easily revoke it.

C. Access and Control Mechanisms

Users should be able to review, edit, or delete their data and settings to manage privacy preferences and permissions within XR environments. These should include both the right to delete XR data and the right to be forgotten within XR platforms and applications. XR companies should also take steps now to ensure user data is portable. While this is already required by EU legislation, as discussed in the interoperability section, companies should work on making their interfaces technically compatible

through open and common technical standards from the outset. Doing so will help companies comply with EU data portability requirements and build resilience in their ecosystem.

D. Privacy-Enhancing Technology

To comply with the GDPR's requirements of privacy by design and privacy by default, XR companies should integrate built-in privacy-enhancing technologies like end-to-end encryption, jammers, or vision blurring in their XR ecosystems. Given that the GDPR leaves the decision on which measures to incorporate up to companies, EDPB's guidance or further specifications of GDPR's recitals should specify which privacy-enhancing technologies will serve as a minimum for companies to legally comply with privacy-by-design requirements in the XR space. Additionally, governments should oversee and participate in the standard-setting process to ensure that companies are building privacy-by-design mechanisms into their ecosystems' architecture. Not doing so could impair the feasibility of implementing these technical measures in the future.

E. Antitrust Measures

Privacy concerns will not only stem from the unprecedented scale and range of data collection enabled by XR technologies but also from the main tech players' ability to aggregate this data and use it to entrench their market power in adjacent advertisement-related markets.

To tackle XR privacy issues, authorities will need to enforce existing antitrust laws to prevent and sanction big tech's conduct raising artificial barriers to entry in the XR space. This will prevent a handful of providers from centralizing all the XR data collected. Antitrust investigations might address these issues by focusing on several behaviors the same companies have committed to entrenching their market power in existing digital markets. This includes exclusivity requests by XR with certain content providers, requirements that users use certain VR devices to access specific virtual spaces, self-preferencing of their own XR content, refusals to grant access to a virtual space to other providers, or even just raising entry barriers through data accumulation.[116] Authorities will also need to prevent companies like Meta and Alphabet from leveraging the market power they already have in existing social media platforms and advertising markets to achieve a dominant position in the XR space in the first place.

Finally, interoperability standards will be pivotal to avoid XR companies locking their users in their proprietary systems and raising barriers to entry in different ecosystems. As proposed in the interoperability section, beyond enforcing existing mandatory interoperability rules (e.g., DMA), to achieve interoperability, governments must intervene in the standard-setting process to introduce interoperability through open and common technical standards.

---

[116] Crauthers, *supra* note 27.