UCLA Institute for Technology, Law & Policy

GOVERNING XR

EXECUTIVE SUMMARY

Developed by the UCLA Information Policy Lab.

Megan Bradley, Melodi Dincer, Gabriela Gura, Michael Karanicolas, Noah Keith, Angela Kim, Md Abdul Malek, Tammana Malik, Pablo González Mellafe, Maria Fernanda Muñoz, Walter Musgrave, Elizabeth Mzungu, Mahmut Ormanci, Noah Usman, and Chen Yan.

October 2024

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.

Executive Summary: 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.

Executive Summary: 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.

Executive Summary: 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.