ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

in cotutela con Università **KU Leuven**

DOTTORATO DI RICERCA IN

Law, Science, and Technology

Ciclo 38

Settore Concorsuale: 12/H3

Settore Scientifico Disciplinare: IUS/20

From the Physical World to a Mediated Reality: The Impact of Extended Reality on Fundamental Rights

Presentata da: ***Emmie Hine***

Coordinatore Dottorato

Professor Antonino Rotolo

Supervisore

Professor Luciano Floridi

Co-Supervisore

Professor Peggy Valcke, KU Leuven

Esame finale anno 2026

FROM THE PHYSICAL WORLD TO A MEDIATED REALITY

THE IMPACT OF EXTENDED REALITY ON FUNDAMENTAL RIGHTS

Emmie HINE

Supervisor(s):

Prof. Peggy Valcke

Prof. Luciano Florid

Members of the Examination Committee:

Prof. Frank Fleerackers

Prof. Federica Russo

Prof. Oreste Pollicino

Dissertation presented in partial fulfilment of the requirements for the degree of Doctor of Law

October 2025

"The Human Rights Council… affirms that the same rights that people have offline must also be protected online."

- Human Rights Council, 2012

The challenge for our generation is to reconcile these two forces. How do we protect liberty when the architectures of control are managed as much by the government as by the private sector? How do we assure privacy when the ether perpetually spies? How do we guarantee free thought when the push is to propertize every idea? How do we guarantee self-determination when the architectures of control are perpetually determined elsewhere?

- Lawrence Lessig, 1999 (Code: And Other Laws of Cyberspace)

Abstract

This dissertation investigates how immersive extended reality (IXR)—a spectrum encompassing aspects of virtual, augmented, and mixed reality—impacts fundamental rights and forces us to rethink how we consider fundamental rights in digital settings. As immersive technologies evolve into networked, commercially viable infrastructures, they increasingly function as privatized spaces that mediate users' perceptions, actions, and social relations. The thesis argues that these technologies are not merely new media but constitute fundamentally *mediated realities* that intensify both the opportunities and the risks associated with the digital age.

Adopting a sociotechnical and rights-based approach, the study explores how IXR's distinctive affordances reshape experiences of safety, privacy, and freedoms of assembly and expression. It advances three research questions: how IXR's structure influences user experience; how its affordances affect the exercise of fundamental rights; and how existing EU law addresses—or fails to address—these transformations. Through a combination of philosophical analysis, literature review, and doctrinal examination of the EU's digital governance framework (including the GDPR, Digital Services Act, Digital Markets Act, AI Act, and product safety legislation), the dissertation identifies gaps in current regulation and conceptualizes a new rights-based governance paradigm for digital environments.

The central claim of the latter line of thought is that as the degree of technological embodiment increases, so too should the responsibilities of private platform operators to uphold users' rights. IXR platforms act as reality-mediating infrastructures—spaces where control over embodiment, information flows, and participation effectively constitutes a form of governance. The thesis proposes a novel framework linking the degree of embodiment to a corresponding heightened duty of fair procedure, drawing analogies from public-function doctrines in constitutional and administrative law. This framework enables a proportional allocation of responsibility among state and corporate actors and offers guidance for adapting human rights and EU fundamental rights principles to immersive settings.

Ultimately, the dissertation argues that the transition from the physical to the mediated world should not entail a loss of rights. Instead, it demands the deliberate translation of established rights and liberties into the architectures of extended reality. By integrating insights from philosophy of technology, platform governance, and EU law, the thesis contributes both a theoretical account of mediated rights and a practical roadmap for rights-preserving governance in the age of immersion.

Publications and Academic Activities

First Author Publications

Hine, Emmie, & Floridi, Luciano. From No-Win to No-Lose: Legislating AI in US States. *Journal of AI Law and Regulation* (2025).

Hine, Emmie, & Floridi, Luciano. Winning the AI Race? The US AI Action Plan in Context. *Journal of AI Law and Regulation* (2025).

Hine, Emmie. Virtual Reality, Cyberspace, and Embodiment: A Historical Debate with Contemporary Resonance. *Virtual Reality* (2025).

Hine, Emmie, Cowls, Josh, & Floridi, Luciano. Assembly and Expression in Extended Reality: Transposing Human Rights Across Realities. *Interactive Entertainment Law Review* (2025).

Wilson, Claudia*, & **Hine, Emmie**.* US Open-Source AI Governance: Balancing Ideological and Geopolitical Considerations with China Competition. Policy paper with the *Center for AI Policy* (2025).

Hine, Emmie. AI laws in the US states are feeling the weight of corporate lobbying. *Nature Index* (2024).

Hine, Emmie. Governing Silicon Valley and Shenzhen: Assessing a New Era of Artificial Intelligence Governance in the United States and China. *Digital Society* (2024).

Hine, E., Novelli, C., Taddeo, M., Floridi, L. Supporting Trustworthy AI Through Machine Unlearning. *Science and Engineering Ethics* (2024).

Hine, E., Rezende, I.N., Roberts, H., Wong, D., Taddeo, M., Floridi, L. Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations. *Digital Society* (2024).

Ferruz, N.,* Zitnik, M.,* Oudeyer, PY.,* **Hine, E.**,* et al. Anniversary AI reflections. *Nature Machine Intelligence* (2024).

Hine, E., Yousefi, Y., Osivand, P., Brand, D., Kugler, P., & Chiara, P.G. The AI Act Grand Challenge shows how autonomous robots will be regulated. *Science Robotics* (2023).

Roberts, H.,* **Hine, E.,*** & Floridi, L. Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance. *Quo Vadis, Sovereignty? : New Conceptual Boundaries in the Digital Age of China* (2023).

Hine, Emmie. Content Moderation in the Metaverse Could Be a New Frontier to Attack Freedom of Expression. *Philosophy & Technology* (2023).

Contributing Author Publications

Rezende, I.N., **Hine, E.**, et al. Policing across and within metaverses: How immersiveness changes the role of police in cyberspace. *European Journal on Criminal Policy and Research* (2025).

Morley, J., **Hine, E.**, et al. Global Health in the Age of AI: Charting a Course for Ethical Implementation and Societal Benefit. *Minds and Machines* (2025).

Floridi, L., Buttaboni, C., **Hine, E.**, et al. Open-Source AI Made in the EU: Why it is a Good Idea. *Minds and Machines* (2025).

Sovrano, F., **Hine, E.**, Anzolut, S., & Bacchelli, A. Simplifying software compliance: AI technologies in drafting technical documentation for the AI Act. *Empirical Software Engineering* (2025).

Fratini, S., **Hine, E.**, Novelli, C., Roberts, H., & Floridi, L. Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models. *Digital Society* (2024).

Ganz, A., Camellini, M., **Hine, E.**, Novelli, C., Roberts, H., & Floridi, L. Submarine Cables and the Risks to Digital Sovereignty. *Minds and Machines* (2024).

Roberts, H., **Hine, E.**, Taddeo, M., & Floridi, L. Global AI governance: barriers and pathways forward. *International Affairs* (2024).

Conference Papers

Hine, Emmie, Cowls, Josh, & Floridi, Luciano. Assembly and Expression in Extended Reality: Transposing Human Rights Across Realities. Paper presentation and panel. *Proceedings of the International Congress: Towards a Responsible Development of the Metaverse* (2024).

Hine, Emmie. Extended Reality is a Fundamentally Mediated Reality. Paper presentation and panel. *Proceedings of A Metaverse for the Good* (2024).

Hine, Emmie. Governing Silicon Valley and Shenzhen: Assessing a New Era of Artificial Intelligence Governance in the US and China. *Proceedings of the Sixth AAAI/ACM Conference on Artificial Ethics, Intelligence, and Society* (*AIES '23).*

Pre-Prints

Hine, Emmie. Extended Reality as a Fundamentally Mediated Reality: XR Infrastructure and the Ethics of Experience. *Preprint* (2025).

Hine, E., Wong, D., Floridi, L. The Impact of Modern Big Tech Antitrust on Digital Sovereignty. *Preprint* (2025).

Floridi, L., Buttaboni, C., **Hine, E.**, et al. Agentic AI Optimisation (AAIO): what it is, how it works, why it matters, and how to deal with it. *Preprint* (2025).

Formisano, G.,* **Hine, E.,*** et al. Counter-Misinformation Dynamics: The Case of Wikipedia Editing Communities During the 2024 US Presidential Elections. *Preprint* (2024).

Editorial Contributions

Co-editor of *Business and Human Rights Journal* Special Issue, "AI, Business, and Human Rights" (2024 - present)

Guest editor of *Digital Society* Topical Collection, "The Situated Metaverse" (2023 - 2025)

Author of the Ethical Reckoner newsletter, a weekly tech-focused newsletter (2021 - present)

Ad-Hoc Manuscript Reviewing (2020-present)

Nature Machine Intelligence	FAccT '24 Committee Member	Information, Communication & Society	PLOS One
International Affairs	CAIP '23 Committee Member	Digital Society	The Journal of Digital Earth
Philosophy & Technology	AI & Society	Telecommunications Policy	Discover Artificial Intelligence
East Asia Forum	Minds & Machines	Political Science & Politics	Discover Psychology
Ethics & Information Technology	Business Ethics Quarterly	Asia Pacific Journal of Public Administration	Data & Policy
International Business Review	Res Publica	Heliyon	

Invited Talks and Panels

18th Community of Political Science and International Studies Conference (July 2025)
• *Open-Source Software and Open-Source AI: Lessons for Global AI Governance* (invited talk)

NY Tech Week (May 2025)
• *AI & the Social Contract* (invited panelist)

European Commission JRC Centre for Advanced Studies VirtueS Seminar (May 2025)
• *Regulatory aspects of virtual worlds and users' wellbeing* (invited speaker)

Envisioning Artificial Intelligence at Yale (May 2025)
• *AI Governance in the US, China, and EU: A Crash Course* (lightning talk)

Summit on State AI Legislation (March 2025)
• *AI Regulation: Considering Open Source* (panel moderator; also Summit Scientific Coordinator)

Centre for Information Policy Leadership (CIPL) Summit (March 2025)
• *Global AI, Data, and Technology Policy: Digital Sovereignty and Beyond* (panelist)

Bennett Institute for Innovation and Policy Acceleration launch event (February 2025)
• *How do we control AI for good?* (panelist)

Stereopsia (December 2024)
• *Safety, Ethics, and AI in Virtual Worlds* (fireside chat)

Metaverse Safety Week (December 2024)
• *International Human Rights Day Global Community Lab* (moderator and invited contributor)

Health Artificial Intelligence: Science, Technology, and Ethics (HASTE) Community Workshop (August 2024)
• *The State of State AI Legislation* (invited speaker)

ETUI-ETUCE Conference on AI at Work (February 2024)
• *Anticipating the Cognitive Impact of Extended Reality: Beyond Student Perspectives* (panelist)

Democrats Abroad UK (February 2024)
• *AI and Elections: What's in Store for 2024* (panelist)

Foundation Metaverse Europe (February 2024)
• *Virtual Environments, Real Responsibilities: Safeguarding Fundamental Rights in XR* (keynote speaker opposite MEP Axel Voss)

Metaverse Safety Week (December 2023)
• *Human Rights and Public Policy Roundtables* (invited contributor)

ICON-S Italy (October 2023)
• *AI Act Conformity Assessment Framework* (panelist)

DRAILS Workshop Series (September 2023)
• *Governing Silicon Valley and Shenzhen* (invited speaker)

Coursework

- Basic Course (Bologna)
- Legal Theory, Legal Reasoning, and General Research Methodology (Bologna)
- AI & Law (Bologna)
- Data Science for Legal Analytics (Bologna)
- Medical Ethics/Bioethics and Law (Bologna)
- LegalTech (Bologna)
- Big Tech and the Regulation of Digital Markets (Bologna)
- LXAI and YAI (Bologna)
- Foundations of Natural Language Processing (Bologna)
- Digital Ethics and Philosophy (Bologna)
- Proposal Writing Crash Course (Bologna)
- Leuven Global Law course (Bologna)
- Ethics and AI PhD Course (external)
- Vista Institute AI Agents & the Law course (external)

Additional Activities

- Co-Chair of Yale Digital Ethics Center Digital Vulnerabilities in the Age of AI, December 2025
- Scientific Coordinator of Yale Digital Ethics Center Summit on State AI Legislation, March 2025
- Invited to participate in Vista Institute AI & the Law Seminar, Washington, D.C., July 2025
- Accepted to Erasmus+ BIP on Social Rights, Lyons, December 2023
- Won AI Act Grand Challenge competition, August 2023
- Publishing Tech Reckoner newsletter

Acknowledgements

I write these acknowledgements on a plane about to take me across an ocean. It's a situation I've been in perhaps too often over the past three years—both for my sleep schedule and carbon footprint—and yet I am happy to be on this plane for several reasons. One is that I am en route to Brussels for a policy summit that I am looking forward to. Another is because I love a metaphor, and I think this trip represents two wonderful things about my PhD journey.

First, there have been the research opportunities and the joy of doing that work. But this is not the place to discuss those. Rather, this is the place to discuss the second, more wonderful thing: the people. "It takes a village" is, at this point, incredibly cliched, but all the best cliches have a kernel of truth at their core, and this is truer than most. It took a global village to raise this PhD—over the course of the program, I lived in three countries and traveled to roughly eleven more—and the gratitude I express below bursts through borders of space and time.[1]

First, of course, I must (and want to) thank my family: my father Clarkson, my mother Laura, my brothers Nick and Sam, my sister-in-law Caroline, and my future sister-in-law Emma. I am fortunate to come from a family of writers, and having their examples of PR statements, Wall Street Journal articles, legal motions, and GQ features has been both instructive and motivating. They have also, of course, been excellent moral support, and I am grateful for what surely must be the hours they spent listening to me gripe in low moments. I also want to thank my grandparents Mema Sue, Grandpa Joe, and Meme, for their unwavering support, for keeping my IT support skills sharp, and also for being the first readers of my newsletter. Poppy, I think you would have liked it, too. And Uncle Chad—you would have loved the street art in Bologna. 💙

I am also immensely grateful to my supervisor, Luciano Floridi. He has been my mentor for the last five years, and as well as being my primary supervisor, is the primary reason I embarked on this PhD. I am thankful for every conversation we've had, whether about research, life, or both. He taught me about writing as a form of knowledge and power, and I know that will stay with me in all my future endeavors. He also ensured I had a VR headset as I embarked on this project, for which I am very appreciative.

Though I have known my co-supervisor, Peggy Valcke, for comparatively less time, I am also grateful to her for being a welcoming face in CiTiP, for bringing me into the fold of a wonderfully supportive research community, and for making sure I actually wrote a law thesis. The best supervisors allow their students to wander just enough before coming back to the path, and both Luciano and Peggy have indicated interesting hills and tussocks to explore while also pointing the way ahead.

There is a wonderful circle of badass women in academia who inspired me every day, and each of them deserve acknowledgement and many accolades:

- Dr. Julia Andreasen - the first doctor of our generation in our family. Inspirationally committed to ice and science education. The first person I would call if stuck in a tent in Antarctica.
- Dr. Jess Morley - who's always hitting her marks. Grateful to have witnessed several eras and can't wait to see the next—long live the walls we crashed through ✨
- Dr. Allison Wong - climber and chemist extraordinaire. The only person I would take an EasyJet full of bachelor partygoers to Spain for.
- Happily-not-Dr. Isabella Huang - climber and technologist extraordinaire who showed me that *not* getting a PhD is an equally valid option, and to view academia with a critical eye.
- The future Dr. Renée Sirbu - who also helped me keep things in perspective, who climbed and cooked and kvetched with me. We're never defeating the allegations #BetaTesters4ever

[1] Names are in alphabetical order unless there's a reason for them not to be.

There are so many other people that I owe so many thanks to—Alessandra (for sweaters, tea, voice notes, and life advice), Holly (for constant inspiration and Downton Abbey enthusiasm), Nadav (for hosting, climbing, and memes), Nur (grateful for the trauma of Bologna housing for bringing us together), Yasi (for her sage PhD advice and always making me feel welcome), Zoë (for sea cliff and Central Park adventures). My Doughty crew: Ally, Ariel, Charlotte, Emily, Jared, Jackson, Matt, and RB. The Belgium crowd: Clara, Marie and Freija, Patrick, Stella. The New Havenites: Abi, Julia, Justin. The broader DEC research universe, a wonderful community of friends and collaborators including: Abra Ganz, Claudia Wilson, Claudio Novelli, David Wong, Huw Roberts, Isadora Neroni Rezende, Jakob Mökander, Josh Cowls (to whom I also owe thanks for much life advice and the excellent example his dissertation provided), Mariarosaria Taddeo, and Martina Camellini. Abby—I can't believe that this journey started with me not knowing you. Who would have thought that a chance meeting of a present and future Connecticutian in Bologna would result in such marvelous adventures and a beautiful friendship? Dolly—from Williams to Linnaean Street to NYC, you've been there for it all. Mike—This journey started with me quitting the company (and team) we both worked at, but our friendship persevered. I'm grateful for every meal (and owe you several), every sail, and every piece of advice.

Another wonderful community has been my PhD cohort. Alessandro, Ali, Cecilia, Emilia, Giovanni, Giovanni, Margherita, and Thay—thank you for the support, the salons, and for "attending CIRSFID every day." We all went through a lot of life during this PhD. Thay (again)—it was a privilege to see my friend embark on the journey of a lifetime with her person in Brazil.

Provided there's no orchestra to play me out, I also want to thank all my climbing gyms for keeping me sane, and though I've been diplomatic in other sections, here I will single out one in particular: Ascent. I've been a climber for most of my life, and Ascent is fantastic as a gym, but the most extraordinary as a community. Katie, Nate, the Gays Off Belay crew, and everyone else who makes Ascent such a special place—thank you.

I've been fortunate to participate in several fellowships over the course of my PhD. I'm grateful to have worked with some wonderful people, including from the Future Impact Group the ever-patient Nick Caputo and the incredibly dedicated Luke Dawes; the wonderful Talos Network team of Antonia Briel, Carolin Basilowski, Chiara Gerosa, David Conrad, Francesca Sheeka, and Stephen Robcraft; and the Internet Law & Policy Foundry team. I'm grateful to all of them for their guidance and helping me explore new research horizons.

A few other necessary acknowledgements:

- Ariell Bachman and Kiran Subhani - If Luciano taught me that writing can be a form of power, they taught me that writing can be a form of coping.
- Ted Bach, for setting the standard for bosses in my very first job, and for supporting me inevitably leaving for a PhD even though he thought it would be a year later.
- My first thesis supervisor, Dan Barowy, for teaching me how to be a researcher.
- My laptop. It's been through a lot. Hold on, we're almost there. (As I edit, we're now down a shift key)
- Wooster Square Park, site of breakups, breakdowns, a few picnics, and many cherry blossoms.
- The various iterations of my house; some are thanked more than others.
- Trains, in this order: Belgian NMBS/SNCB, TrenItalia, MetroNorth, Italo, Amtrak (at least you exist).
- The joy of stamps (but only the 2-euro ones, not the 16-euro ones).
- Melatonin (and TimeShifter (not sponsored, I promise)).
- Liege waffles, piadine, and tigelle (aka the European carbs I can never hope to recreate).

- All my newsletter readers. Writing the Ethical Reckoner—now Tech Reckoner—helped keep me sane when I felt like I couldn't write another word of academic prose, and I'm forever flattered that hundreds of people want to read my words.

This has been a great many words—I've deplaned and am now on a Belgian train (and now I'm editing this on an English train)—but they have been perhaps the most gratifying ones of the thesis to write. My yearbook quote my senior year of high school was: "Somewhere, something incredible is waiting to be known." (And somehow I was surprised I went on to grad school?). Jesting aside, I have learned many wonderful things over the course of the PhD, but the most important one has been how wonderful my people and communities are. If you read nothing else of this thesis, read this:

Thank you for being part of my communities. You have gotten me through this, and I am immensely grateful for you.

What is waiting to be known next? We'll find out.

Table of Contents

Index of Tables

Index of Figures

Part I: Introductory Remarks

Chapter 1: Introduction

In 1962, Morton Heilig built a peculiar machine: a swivel chair mounted to a platform, facing a large box that engulfed the user's head. Inside the box was a set of sensory wonders—a stereoscopic color display, scent diffusers, fans, and a stereo-sound system. Users could experience a motorcycle ride through Manhattan, a bicycle ride through Brooklyn, or several other immersive experiences. He called this machine the Sensorama (Lanier 2017, 38–39).

Six years later, Harvard professor Ivan Sutherland created the "ultimate display" (Sutherland 1965): a head-mounted device attached to a mechanical arm, festooned with wires to monitor motion and eye movement. The seeming precarity of the ceiling mount inspired the joking name "Sword of Damocles,"[2] but Sutherland preferred "Stereoscopic-Television Apparatus for Individual Use" (Werner 2024). The whole device had the vague appearance of orthodontic headgear for the upper part of the face. It was neither practical nor commercially viable—nor was the Sensorama. And yet the Sensorama, as one of the first immersive multimodal systems, and the Sword of Damocles, the first extended reality (XR) headset, are the grandparents of today's virtual reality (VR), augmented reality (AR), and mixed reality (MR) systems.

1.1. Background and Rationale

These early experiments proved the concept of immersive, computer-mediated environments, and it is the descendants of these original systems that are the subject of this dissertation. XR technology has

[2] Cicero told the story of powerful but miserable ruler Dionysius II of Syracuse. A courtier, Damocles, remarked how wonderful his life must be. Dionysius seated him on a golden couch, had him waited on hand and foot, and fed him the most lavish food, but when Damocles glanced up, he noticed a sword dangling above his head, hung from a single thread of horsehair (Cicero 2007, 487). The myth is widely interpreted as being about the precarity of "the fortunes of men who hold power" (The Editors of Encyclopaedia Brittanica 2025b) and the impossibility of happiness when "perpetually menaced by some alarm" (Cicero 2007, 489).

advanced significantly in the last eight decades and become networked, allowing them to become commercially viable products. However, as with many technologies—including artificial intelligence (AI)—XR has experienced a number of "summers" and "winters." In summer, expectations grow, new technology emerges, and revolutionary change seems imminent. In winter, expectations are tempered, investment cools, and attention moves to other topics (Floridi 2020a). Extended reality (XR) recently experienced a very hot summer—the so-called "metaverse" craze—with the global XR market growing 24.9% in 2022 to $25.2 billion (Alsop 2022), before economic headwinds and technological difficulties led some major companies to scale back their XR ambitions (Miller 2023; Lü 2023; Whelan and Flint 2023; Thorbecke 2023). However, the entries of major technology companies into the market and increased consumer attention to AR devices indicates a possible imminent market upswing.

Typically defined as including virtual reality (VR), augmented reality (AR), and mixed reality (MR), XR is becoming more widespread as a variety of new devices enter the market, including from some of the world's largest technology companies, suggesting another upswing may be on the horizon. New devices (from AR glasses to gaming VR headsets and high-end MR devices) are entering the market, including offerings by some of the world's largest tech companies, and XR is increasingly being used in a range of domains. Gaming and entertainment remain the leading sectors for VR adoption but it is worth noting that education, healthcare, professional training, and industrial design have also embraced immersive technologies in recent years (Pratt 2024). For example, VR simulations now aid therapy and mental health treatment, VR and AR assist with surgical training and medical visualization, and immersive platforms are used for skills training in fields like aviation and emergency response (Slater et al. 2020). Enterprise uses (virtual meetings, architectural visualization, data modeling) and artistic or cultural applications are expanding as well (Slater et al. 2020). XR presents new opportunities for new, different, and better experiences across many sectors, including education, healthcare, and entertainment (Floridi 2022), fueling a sense that these technologies could transform how we learn, communicate, and interact.

1.1.1. XR Realism

Crucially, the appeal of XR lies in its ability to produce experiences that feel real, and this thesis accepts part of David Chalmers's position of virtual realism—that is, that virtual experiences are real (Chalmers 2022, 80). Even if one does not accept the other part of his argument (that virtual *entities* are real), one can still acknowledge that virtual experiences are real experiences. Consider online video meetings: Zoom meetings are still meetings and impart knowledge and instill emotions in attendees (provided they are paying attention!). Modern XR systems surround users with interactive, stereoscopic environments that engage multiple senses and track user movements to enable natural interaction. Virtual environments can elicit the subjective impression of presence in the scene (Slater 2009). According to Slater (2009), presence involves two intertwined illusions: the place illusion (feeling physically in the virtual world) and the plausibility illusion (feeling that the virtual events are actually happening). When both occur, users tend to respond to virtual situations and stimuli as if they were real, even while knowing intellectually that they are not (Slater 2009). Chalmers (2022) critiques the assertion that VR always creates "illusions," arguing that the place and plausibility illusions should be thought of as senses of being in a place (physical or virtual) and "the sense of plausibility" (Chalmers 2022, 152–53). Still, the point remains that XR can create feelings of situatedness and experience that feel real, even if they are not mimicking physical places.

Immersive XR also enables a sense of body ownership and embodiment: users can look down and see a virtual body in place of their own, with head-and-hand tracking creating synchronous movements, leading the brain to accept the virtual body as "yours" (Slater 2021; Chalmers 2022, 153–56). A corollary to these is that multi-user XR sessions create an sense of co-presence—the feeling of sharing a space with others whose avatars are perceived as real actors (Slater 2021; Poeschl and Doering 2015). These qualities—immersion, presence, embodiment, and co-presence—set XR apart from traditional media like television or PC interfaces. XR can induce stronger psychological and physiological reactions than watching a screen, precisely because the experience is more lifelike. Research has shown, for instance, that VR and even AR scenarios can trigger emotional and behavioral responses akin to those in an equivalent real-world situation (Yeh et al. 2018; Eckhoff et al. 2020; Martens et al. 2019; Slater and

Sanchez-Vives 2016); applications from phobia therapy to work training leverage this realism on the premise that the more a virtual experience is perceived as real, the greater its impact (Slater et al. 2020; Freeman et al. 2017). Though research on AR and MR is more nascent, they also possess these characteristics, with AR inducing feelings of anxiety at a similar level as VR in one experiment (Yeh et al. 2018). Furthermore, an AR device could make a user feel present in a different environment or embodied in a different body through overlays, and AR experiences have been shown to influence people's behavior in the physical world (Miller et al. 2019). Thus, we must be concerned about the impact of technologies across the XR spectrum.

1.1.2. Private Platform Power

IXR is infrastructural and transnational. Choices by a small number of platform and hardware firms organize what is perceptible and actionable, thereby distributing power and responsibility in ways that existing legal regimes only partially anticipate. Recent flurries of antitrust efforts in the US and EU have targeted many US Big Tech companies (Hine, Wong, et al. 2025), reflecting a growing consensus that the social and economic influence of technology firms should be curtailed (Friederiszick 2025). Although motivations and enforcement mechanisms differ, it is this same market power that gives technology firms control over human rights, which will be explored further in the next section.

It is critical to acknowledge that business already have a responsibility to uphold human rights, as recognized by the UN Guiding Principles on Business and Human Rights (United Nations Human Rights Office of the High Commissioner 2011a) (henceforth the Guiding Principles, also often called the Ruggie Principles). However, the Ruggie Principles lack an enforcement mechanism. Additionally, when it comes to XR, platforms not only have negative obligations to avoid infringing on human rights, but are involved in positively promoting them by designing the affordances of devices and platforms that impact what kinds of assembly and expression are possible and permissible, raising questions of legitimacy around human rights governance. This will be discussed further in subsequent chapters; I mention it here both to justify my assertion that businesses possess human rights obligations, but also to underscore the necessity of determining an approach to reifying their obligations.

1.1.3. Rights Recalibrations in Emerging Technologies

The increasing realism and adoption of XR raises urgent questions about its broader societal implications. History has shown that new communications technologies—from the printing press to the Internet—can unsettle legal and ethical frameworks. A brief genealogy illustrates how successive communications technologies have precipitated doctrinal and normative recalibrations in the protection of fundamental and human rights. The print revolution redistributed epistemic authority by lowering the cost and increasing the persistence and portability of texts, weakening clerical and monarchical controls over knowledge and catalyzing nascent commitments to freedom of expression and freedom of conscience; states experimented with licensing and prior restraint while theorists articulated anti-censorship principles (Eisenstein 1980). The emergence of instant photography, mass newspapers, telegraphy, and the telephone then made personal intrusion qualitatively easier and more scalable, prompting the formulation of a modern right to privacy in Warren and Brandeis's "right to be let alone" and, later, a jurisprudential shift from property-based to expectation-based conceptions of communications privacy (from *Olmstead* to *Katz*), developments that resonate with contemporary protections of correspondence and private life (e.g., Art. 8 of the ECHR) (Brandeis 1890).

With broadcast radio and television, the one-to-many architecture and ubiquity of the medium made questions of incitement, dignity, and equality acute; the International Criminal Tribunal case against Rwanda's Nahimana et al. ("The Media Case") crystallized how broadcast affordances can ground criminal responsibility for direct and public incitement to genocide, underscoring positive state duties to prevent catastrophic rights violations (MacKinnon 2004). The rise of computing and networked databases in turn produced the modern data protection project, from fair-information principles and the OECD Guidelines to the EU's constitutionalization of data protection in primary and secondary law, culminating in the GDPR (OECD 2013). The Internet reconfigured expression and assembly in digital environments: courts and legislators rejected broadcast analogies for online speech (e.g., *Reno v. ACLU*[3]), international bodies affirmed that the "same rights" apply online and offline (Human Rights Council 2012), and European jurisprudence developed novel balances between privacy and expression (e.g., the "right to be forgotten" in *Google Spain*[4]). Subsequent mobile and platformized communications enabled continuous inference about location, association, and behavior, provoking limits on state and corporate surveillance (e.g., cell-site tracking in *Carpenter*;[5] the invalidation of general data-retention regimes in *Digital Rights Ireland*[6] and *Tele2 Sverige*;[7] European Court of Human Rights scrutiny of bulk interception in *Big Brother Watch*[8]). Finally, algorithmic and biometric systems (e.g., face recognition and emotion inference) have revived concerns about non-discrimination, due process, and informational self-determination in public and semi-public spaces; courts have constrained live facial recognition deployments[9] and EU law now treats biometric and certain automated-decision contexts as specially protected (GDPR Arts. 9, 22).

XR is no exception. If virtual environments feel authentic—even if not to the extent of the physical world—and impact how people think and behave, then actions in XR can carry real consequences. Harms experienced in immersive digital spaces may affect users in ways analogous to harms in the physical world. For example, a violent or harassing encounter in a highly immersive VR setting can provoke genuine trauma or fear (Blackwell et al. 2019). Likewise, the blurring of reality could lead to cognitive or identity confusion—issues anticipated by Madary and Metzinger (2016) in their "code of ethical conduct" for VR. They warn that prolonged exposure to realistic VR might have unforeseen negative effects on individuals' perceptions or social behavior (e.g., desensitization or difficulty

---

[3] (*Reno v. ACLU, 521 U.S. 844* 1997)
[4] (*Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* 2014)
[5] (*Carpenter v. United States* 2018)
[6] (*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* 2013)
[7] (*Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis* 2016)
[8] (*Big Brother Watch and Others v. the United Kingdom* 2021)
[9] (*Bridges, R (On the Application Of) v South Wales Police [2020] EWCA Civ 1058* 2020)

distinguishing virtual from real experiences). As Floridi (2015) observed, our on- and offline lives are merging into an "onlife" continuum. XR accelerates this convergence by making virtual interactions more embodied and immediate, to the extent that they can approach similar levels as offline life. This heightened immersion is precisely why we must scrutinize XR's impact on human rights and fundamental freedoms now, at an early stage. Even if immersive digital experiences do not become equivalent to physical reality, the rights we consider fundamental in the physical world are still at stake, and to a greater degree than non-immersive platforms—which we already agree carry fundamental rights implications.

1.1.4. The US Development and EU Regulatory Landscapes

This thesis primarily addresses XR developments in the US. Although other countries, including China, South Korea, and Japan also have active XR industries, including all global XR developments would render the scope of this dissertation overly broad. Additionally, US companies are embedded in the ecosystem of technology companies and structures of power that this dissertation is concerned with investigating. Finally, addressing development in a liberal democratic context means that I can analyze uses that are more relevant for policymaking in a similar political context.

Related to this, I address my policy recommendations to EU legislators because they are moving towards proactive regulation of XR, which could also have significant implications for other jurisdictions' governance. In only one year, the EU moved from releasing an EPRS briefing on the "metaverse" and proposing a "metaverse amendment" to the forthcoming Artificial Intelligence Act (Bertuzzi 2022) to hosting Citizens' Panels and launching a regulatory initiative aimed at developing a non-legislative framework to uphold EU values in "virtual worlds" (Joint Research Centre 2023). The regulatory initiative's strategy on "Web 4.0 and virtual worlds" calls on the EU to be an early mover in development and regulation (European Commission 2023a). To analyze whether current legislation is fit for purpose, the Committee on the Internal Market and Consumer Protection (IMCP) published the European Parliament's first draft motion on "virtual worlds" highlighting risks and urging "fitness checks" to see how existing legislation is coping with new developments (Grady 2023; IMCP 2023), while the Committee on Legal Affairs (JURI) published a report on policy implications of virtual worlds (JURI 2023) and the European Commission Joint Research Centre published a report on the challenges of "next generation virtual worlds" (Torres et al. 2023). "Virtual worlds" were also included in the European Commission President von der Lyon's "next wave of frontier technologies" that she asked the incoming Tech Commissioner to prioritize in late 2024 (Grady 2024). Although recent policy statements have slowed down, XR seems to be embedded in the EU emerging technology regulatory landscape.

Alongside these Commission activities, the Council of Europe has also been actively examining the human rights implications of emerging technologies, including algorithmic manipulation, the impact of digital platforms on freedom of expression, and the governance of artificial intelligence through initiatives like its Framework Convention on AI (Council of Europe 2024; Committee of Ministers 2022; 2019). Additionally, in a report on "Enhancing Legal Frameworks at the National and International Level" for emerging technologies, specifically invokes the need to enhance legal frameworks for the governance of XR, particularly protection from harmful content and enhancing privacy and data protection laws to prevent harmful nudging and manipulation (Vinders 2023). This broader European attention underscores the recognized need for rights-based governance frameworks for technologies like IXR.

Inevitably, many of my policy recommendations will also apply to other XR applications, including non-immersive proto-metaverse platforms and potentially even non-AR smart glasses. However, non-immersive technologies have been around for longer and thus are better regulated than emerging immersive technologies; including threats and legal analysis specific to them would render the scope of the thesis overbroad.

This dissertation reflects the state of EU law as of mid-October 2025. On 19 November 2025, the European Commission published the Digital Omnibus proposals (European Commission 2025c; 2025b), which propose amendments to several instruments discussed in this dissertation, including the

GDPR, ePrivacy Directive, and AI Act. These proposed modifications are not addressed in this analysis, and readers should be aware that the legislative landscape may evolve as these proposals progress.

This is an integrated thesis, meaning that the substantive chapters (Chapters 3-6, and components of Chapter 7) are based on peer-reviewed journal articles. Section 1.4 provides an overview of the chapters and where they have been previously published. In this dissertation, I tie the individual chapters with shared research questions, a common conceptual scaffold (infrastructure and embodiment), and cross-referenced methods and findings. The introduction articulates the throughline so that each chapter reads both independently and as part of a coherent whole.

1.2. Key Concepts and Research Questions

This thesis advances the novel concept of immersive extended reality (IXR). XR is a spectrum that includes virtual reality (VR, when users are immersed in a virtual environment, often with a headset), augmented reality (AR, where virtual information is overlaid on the physical world), and mixed reality (MR, which encompasses both AR and the use of the physical world to augment the virtual)[10] (Milgram and Kishino 1994). Within this spectrum, IXR encompasses immersive VR and MR environments. It includes experiences such as social "metaverse"[11] platforms, VR games, and work environments, but excludes non-immersive experiences such as "desktop VR" and "smartphone VR." It also comprises aspects of MR/AR where users are "immersed" in a sensory context wholly mediated by a device, such as using glasses that overlay information onto the user's field of vision.[12] This narrowed focus is because IXR experiences are of special moral significance: as discussed above, their increased realism and immersiveness create similar psychological and physiological responses as experiences in the physical

[10] The definition and utility of the term "mixed reality" is much debated, to the extent that some question if it should even be considered a separate concept (Grady 2025),

[11] Definitions of the "metaverse" vary, but one widely accepted one is from Ball (2022): "A massively scaled and interoperable network of real-time rendered 3D virtual worlds that can be experienced synchronously and persistently by an effectively unlimited number of users with an individual sense of presence, and with continuity of data, such as identity, history, entitlements, objects, communications, and payments" (22)

[12] I use "IXR" as a generic term throughout or when referring to concerns across IXR, "XR" when referring to XR-specific literature, and "VR," "AR," and "MR" when referring to aspects of those specific areas.

world, indicated both by academic studies of VR and AR (Yeh et al. 2018; Eckhoff et al. 2020; Martens et al. 2019; Slater and Sanchez-Vives 2016) and reports of trauma in victims of sexual harassment and assault in VR (Farrant 2024). While some workplace XR examples are considered, purely industrial systems are out of scope, as are defense-focused systems due to the specificity of the moral debate around defense technology.

At a high level, this thesis is about governance: of platforms and of platform companies, performed by platform companies and governments. The term "platform" broadly refers to "online, data-driven apps and services" (Gorwa 2019) while "platform organization" or "platform company" refers to the entity that deploys a platform, whether a company or other entity. It is key to note that "platforms" are thus not just immersive social "metaverse" platforms, but also XR apps, app stores, and experiences. Governance is, broadly, "all processes of governing, whether undertaken by a government, market, or network, whether over a family, tribe, formal or informal organization, or territory, and whether through laws, norms, power, or language" (Bevir 2012, 1). I consider both platform self-governance and platform governance. Platform governance is "the layers of governance relationships structuring interactions between key parties in today's platform society, including platform companies, users, advertisers, governments, and other political actors" (Gorwa 2019). Platform self-governance is "a subset of platform governance which concerns the rules and procedures that platform operators adopt and implement with respect to their users' activity, behaviour, and content" (Cowls 2023). In the broader area of platform governance, the political actors involved that I am considering in this thesis are EU institutions.

The inquiry centers on consumer IXR[13] in liberal-democratic contexts and uses the European Union as the primary legal forum for doctrinal analysis. Essentially, regulation is "a form of institutionalised norm enforcement" (Black 2020). In this thesis, those institutions are EU policy bodies, and regulations are European regulations and directives. In the EU, most laws are made via the ordinary

[13] This is primarily meant to scope out military and healthcare uses of IXR, which are more specialized, but does at times include educational and work uses, which rely on consumer-available devices.

legislative procedure: the European Commission proposes an act after preparatory work under its Better Regulation guidelines (European Commission 2021a), which requires assessing the potential economic, social, and environmental impact of new initiatives. The European Parliament and the Council of the EU then co-legislate—often reconciling positions in trilogue meetings—before adopting an identical final text (European Union, n.d.-b). Once adopted, regulations apply directly, while directives bind Member States as to results and must be transposed into national law by a deadline (Art. 288, Treaty on the Functioning of the European Union (TFEU)).[14] The legislature can empower the Commission to issue delegated acts to amend or supplement non-essential elements (TFEU Art. 290) and implementing acts to ensure uniform application (TFEU Art. 291). Final texts are published in the Official Journal of the European Union, and interpretation and enforcement are overseen—together with national authorities—by the Court of Justice of the EU, which ensures the uniform application of EU law (European Union, n.d.-a).

Throughout this thesis I refer to "fundamental rights" in the context of extended reality. It is important to clarify this terminology. The term "human rights" generally denotes the inalienable rights and freedoms to which all people are entitled by virtue of being human—as articulated in international instruments like the Universal Declaration of Human Rights (United Nations General Assembly 1948a). The UDHR's 30 articles enumerate civil, political, economic, and social rights (such as the rights to life, privacy, free expression, assembly, and education) that have since been codified in binding treaties and national constitutions. The term "fundamental rights" is often used in European law to describe the subset of human rights that are guaranteed by EU law and domestic constitutional law (European Union Agency for Fundamental Rights 2013). For example, the Charter of Fundamental Rights of the EU and the European Convention on Human Rights secure many of the same rights as the UDHR (Charter of Fundamental Rights of the European Union 2012; European Court of Human Rights 2022), but within the EU legal order these rights have a special, justiciable status. In practical terms, this thesis treats "fundamental rights" as equivalent to basic human rights, with an emphasis on those rights recognized

[14] (Consolidated Version of the Treaty on the Functioning of the European Union 2016)

and protected under European law. I will draw on human rights language and jurisprudence—e.g., the rights to privacy, data protection, freedom of expression, freedom of assembly, nondiscrimination, etc.—but frame them as fundamental rights questions in the context of digital/virtual environments. The choice of wording signals my focus on rights that have legal force (especially in the EU setting) and reflects the EU's perspective that its digital policy should be grounded in fundamental rights (European Commission 2022a). It also implies a constitutional dimension: this thesis is interested in how immersive platforms may need to be constrained or shaped to uphold the kind of core values found in constitutional democracies.

While XR undoubtedly touches a wider constellation of rights (including the right to health and the right to education, UDHR Arts. 25–26), this dissertation narrows its analysis to safety, privacy, and the freedoms of assembly and expression for three reasons. First, these four rights are the ones most directly and ubiquitously transformed by immersion itself—that is, by IXR's core affordances of presence, embodiment, co-presence, and pervasive sensing—regardless of sector or use case. By contrast, health- and education-related impacts are typically context-specific (clinical VR, curricular AR, etc.) and mediated by pre-existing sectoral regimes (e.g., medical-device, patient-safety, and professional-standards frameworks for healthcare or Member-State education law and pedagogy for schooling), which would require a different analytic frame and risk diluting the horizontal argument developed here. Second, the chosen rights map onto the thesis's governance focus: they sit at the intersection of platform governance and EU horizontal instruments (e.g., data protection, platform accountability, product safety/cybersecurity), enabling a tractable assessment of how general EU law travels into IXR (see Section III; Ch. 5–6). Third, following the Hohfeldian distinctions used in Part III (Hohfeld 1917), safety and privacy function here as predominantly multital claim-rights against many others (Chapter 5), whereas assembly and expression are privileges/liberties to be actively exercised (Chapter 6). That pairing lets the analysis address both "freedom-from" interferences heightened by immersion and "freedom-to" participate in embodied publics. None of this denies the importance of other rights; rather, it treats them as downstream or derivative of the four core areas (e.g., accessibility and nondiscrimination in education are addressed via the platform-level duties and design choices examined in Ch. 3–6). Where appropriate, the Recommendations (Ch. 7) point to sector-specific adaptations, while other chapters maintain a horizontal rights analysis consistent with the dissertation's overall scope.

1.2.1. Research Questions

With these concepts established, we can now turn to the research questions that drive this thesis. I address three research questions (RQs), united by one overarching research question (ORQ).

ORQ: How does the rise of IXR technology affect our conceptualization of fundamental rights in digital spaces?

This broad question asks how immersive technologies force us to reconsider how we think about the protection of fundamental rights in other, non-immersive digital settings. The immersiveness of IXR technologies underscores how the fundamental rights we value in the physical world are increasingly implicated by emerging technologies and the need for a framework to highlight how we can think about the protection of fundamental rights across digital settings.

RQ1: What does the structure of IXR services mean for individual user experiences?

This question is essentially technological and experiential. It probes how IXR systems are built (including hardware, software, platforms, and content ecosystems) and how those structural features shape the way users experience reality. For example, if a few corporations provide the dominant XR platforms, what implications does that have for a user's agency, equality, or safety in those environments? RQ1 sets the stage by describing the infrastructure and design of XR and its embedded values, which in turn affect rights (e.g., a closed, proprietary XR platform might limit who can participate or what they can do, affecting freedom of expression or equality). RQ1 is primarily addressed in Chapters 3 and 4 through a socio-technical analysis of XR architecture and embodiment.

RQ2: What are the positive and negative impacts of IXR on fundamental rights?

This is the core rights analysis. It asks, in a general sense, how IXR helps or hinders the enjoyment of fundamental rights. On the positive side, IXR might enhance certain rights: for instance, it could enable new forms of education and expression, support freedom of assembly by allowing people to gather virtually, or even further equality by enabling experiences across physical limitations. On the negative side, IXR could introduce or amplify risks: threats to user safety (harassment, psychological harms), intrusions on privacy (through extensive data collection and surveillance), new avenues to distort reality and spread misinformation (implicating rights to truth and autonomy), or novel forms of discrimination and exclusion in virtual spaces. RQ2 will be answered by examining specific rights—notably the rights to safety, privacy, and the freedoms of expression and assembly—and evaluating how immersive features of XR amplify familiar issues or create new ones. This analysis (in Chapters 5 and 6) will draw on both scholarly literature (for hypothesized impacts) and empirical evidence available about XR in practice.

RQ3: How does the extant EU legal regime address the fundamental rights impacts of IXR?

This question shifts to a legal perspective, querying to what extent current EU laws and regulations already cover or mitigate the fundamental rights implications identified in RQ2. I survey the existing digital governance framework in the EU—including horizontal laws like the GDPR, DSA, Digital Markets Act (DMA), Product Liability and Safety directives, the EU Charter of Fundamental Rights, and sector-specific regulations—to see if and how they apply to XR scenarios, highlighting gaps or mismatches in the legal regime. RQ3 essentially asks: if IXR were to become mainstream tomorrow, do we have the legal tools in place to safeguard fundamental rights in those environments, or are we overlooking important aspects?

RQ3.5: How should this legal regime adapt?

Having identified likely gaps or shortcomings in the current framework (through RQ3), the follow-up question considers normative and policy proposals: what adaptations, new regulations, or governance mechanisms are needed to better protect fundamental rights in XR? I label this RQ3.5 because it flows naturally from RQ3's analysis of gaps. It is slightly less formal than the other questions, providing a bridge to the policy recommendations in Chapter 7.

These research questions are interrelated and build on one another. RQ1 provides context about XR technology and user experience, which informs RQ2's exploration of impacts on rights. RQ2's findings about benefits and risks set the stage for assessing legal readiness in RQ3. Finally, RQ3.5 engages with forward-looking solutions, circling back to the overarching question of protecting rights in mediated reality. Thus, this thesis has a theoretical component (in Part 1, corresponding to RQ1), a legal component (in Part 2, corresponding to RQs 2-3), and a normative component (in Parts 2 and 3, focusing on RQ3.5 and the ORQ). In the Conclusion, I will reconnect these sub-questions to ensure that the overarching question is answered and the thesis' central argument is brought into focus.

1.3. Epistemology, Methodology, and Limitations

Before summarizing the chapters that address these questions, this section explains the epistemological stance and methodologies adopted in this research, as well as my positionality and the thesis's scope and limitations.

1.3.1. Epistemological Stance

This research takes a sociotechnical perspective that is both legal/policy-oriented and critically informed. By sociotechnical, I mean that technology (in this case, XR) is understood not as a deterministic force but as embedded in social contexts and shaped by human decisions. Sociotechnical approaches examine not just what the technology can do, but who builds and controls it, who uses it and for what purposes, and how those social dynamics influence outcomes. Although its theoretical underpinnings have "faded into the background" of governance discussions (Cowls 2023, 20), a sociotechnical approach aligns with approaches in science and technology studies (STS) and internet governance scholarship, which emphasize that technical architecture and governance norms co-evolve (Musiani et al. 2020). Musiani (2020, 85) argues that "STS-informed Internet governance research relies on understanding governance as a normative system of systems, and it acknowledges the agency, often discreet yet pervasive, of both human and nonhuman actors and infrastructures." This thesis, particularly Chapters 3 and 4, discusses the "system of systems" and uncovers the agency of individual actors, particularly when said agency is constrained by other actors.

My focus on fundamental rights anchors the analysis in normative questions—what should be done to ensure technology aligns with ethical and legal principles—but remains cautious about claims of innovation exceptionalism. By that, I mean the tendency to view a new technology as so novel that it falls outside existing rules or that it should be given a free pass from regulation to flourish. XR is certainly innovative, but it is not *sui generis* in a way that nullifies society's core values. I approach XR with the belief that existing principles of human and fundamental rights remain relevant, even if the methods of implementation need adjustment. In other words, new technology does not require abandoning our hard-won rights frameworks; rather, it challenges us to adapt and apply them intelligently. I also reject the "innovation-regulation" dichotomy—the premise that any regulation will quash technological progress—which is currently heavily emphasized in AI regulation (Hine and Floridi 2025). Bradford (2024) argues that this is a "false choice," comparing the US and EU to reveal that it is not the presence or absence of regulation that impact technological innovation, but instead due to factors like market structure, access to capital, punitive bankruptcy laws, and immigration policies. Thus, I maintain that governments can regulate XR without risk of destroying a nascent industry, provided the regulations are well-crafted.

The epistemology at play is ultimately problem-oriented and reformist: it assumes that through critical analysis we can identify problems and suggest regulatory or design interventions. It also assumes that law and policy can effectively guide technological development—a premise supported by prior observations from, for example, data protection and platform regulation, and one that underpins the

EU's proactive posture on digital governance. Thus, this thesis is supportive of regulation as not only necessary to protect rights but also as a positive force to shape technology for social good. At the same time, the analysis is wary of knee-jerk or poorly tailored regulation; it advocates thoughtful, evidence-based interventions (hence the emphasis on mapping harms and evaluating current laws first).

1.3.2. Methodological Approach

The dissertation employs a combination of methods corresponding to the different sub-questions and disciplinary angles. A significant portion of the work involves reviewing existing literature—from computer science, psychology, philosophy, law, and policy—on IXR and its implications. For the theoretical chapters, a narrative literature review was used to synthesize key debates and concepts. For the rights impact analysis (Chapters 5 and 6), I conducted targeted literature searches on XR and the specific rights. To capture risks from the broad range of literature relevant to safety and privacy in IXR, Chapter 5 employs a narrative literature review. To construct taxonomies of freedoms of assembly and expression and capture the scant and specialized literature about XR and freedoms of assembly and expression, Chapter 6 uses semi-systematic literature reviews. The relative merits and drawbacks of each are discussed in the respective chapters. In general, this dissertation takes a pragmatic approach to the future development of XR technology, excluding excessively speculative discussion to avoid distracting from its policy-oriented goals.

To address RQ3, I performed a doctrinal analysis of relevant EU legal instruments (Bhat 2020). This involved identifying EU laws and regulations that might apply to IXR. I analyzed the text of these laws, regulatory guidance, and interpretations to infer how they may cover IXR scenarios. Part of this analysis is comparative—that is, assessing IXR-specific risks against existing legal provisions. I also considered soft law and ethical frameworks (like the EU's Declaration on Digital Principles or the UN Guiding Principles on Business and Human Rights) as a backdrop for evaluating companies' responsibilities. Since IXR is emerging, there is not yet dedicated EU legislation, so my legal analysis is somewhat innovative, anticipating how to interpret current law for a new domain. Doctrinal legal analysis has been criticized as excluding "sociological understanding" of the function of legal systems (Bhat 2020), which is critical to my analysis and broader theoretical argument. This is why it forms only one part of my methodological structure, complementing my broader analysis.

Rather than conducting a formal Human Rights Impact Assessment (HRIA) for XR (Salcito et al. 2013), the thesis adopts a broader Governance, Ethical, Legal, and Social Implications (GELSI) approach to assess the impacts of immersive technology. The GELSI framework encourages a holistic analysis, going beyond just legal compliance to incorporate ethical considerations, governance structures, and social context (Ghioni et al. 2023). I integrate GELSI thinking especially in Part III of the thesis, which means that my rights analysis (Chapters 5–6) is informed by universal human rights principles (as laid out in the UDHR) and considers ethical concerns, legal frameworks, and social implications. This comprehensive approach, while less systematic than a HRIA, is more suitable for this project. HRIAs are best suited for established, specific instances of technologies with clear and actionable impacts. In other words, it might be appropriate if assessing a specific IXR product, but not the class of technologies as a whole. They are also aimed towards corporate compliance (Salcito et al. 2013), but the goal of this thesis is not to help companies ensure compliance with existing law—it is to help shape the law that they will later be doing HRIAs to ensure compliance with.

In analyzing the possible risks and opportunities for human rights, I use the Universal Declaration of Human Rights (UDHR) as a baseline definition of freedoms of assembly and expression. This is intended to make my analysis applicable across legal and political regimes, rather than situating it in any one specific legal system. The UDHR rights form the "universally desirable" traits in my ethical pluralist stance (Ess 2006), which holds that within those universal traits, there is room for interpretation across cultural and legal contexts. Objections exist; for example, China has called out the UDHR as a Western neo-colonialist construct (Zhao 2015). However, it voted in favor of it and, in fact, played a large role in shaping its provisions (Zhao 2015; Will 2008), as did countries in Latin America (Glendon 2003; Obregon

2009). Though a necessarily imperfect standard, as an international document adopted by the UN and its 193 Member States, it is a sensible yardstick with considerable legitimacy.

It should be noted that empirical research (e.g. user surveys, experiments in VR) was not within the scope of this dissertation. I rely on existing empirical studies where available, but much of the argument is built from theoretical and legal analysis. This is appropriate for research questions centered on conceptual and legal understanding, but it means some conclusions (especially on potential impacts) are predictive. Wherever possible, I have tried to bolster these with real examples and studies.

1.3.3. Positionality and Ethical Limitations

It is important to acknowledge my positionality and how it impacts the limits of this study. Due to my educational and research backgrounds, I approach IXR as a technologist, social scientist, and legal scholar. I am genuinely intrigued and excited by the potential of IXR as an accessibility technology and to facilitate work and education. However, as someone happy with her work setup and not inclined to gaming or social media in general, I am only an occasional VR user. I have not spent vast amounts of time in social virtual reality, nor do I have an AR device. On the one hand, not being a heavy IXR means I maintain a degree of outsider objectivity; I am perhaps less susceptible to the novelty bias or enthusiasm that early adopters might have. On the other hand, it also means I must be careful to fully understand the user experience through secondary reports and interviews, since I cannot draw on extensive personal usage. I have attempted to mitigate this by engaging with qualitative accounts of XR experiences and even anecdotal evidence of user interactions, especially around sensitive issues like virtual harassment. Still, a more immersive personal exposure could have provided additional insight, so this is a self-acknowledged limitation.

In terms of social identity, I identify with some communities that are marginalized in IXR, but certainly not all of them. This positionality informs my sensitivity to certain issues—for example, how embodiment in virtual spaces might differently affect those who face harassment or bias in physical reality. It perhaps leads me to question narratives from primarily able-bodied, white, male tech evangelists, whose excitement about IXR's potential may overlook how women or LGBTQ+ users might encounter particular risks (such as gender-based harassment in VR). My standpoint strives to be inclusive: I ask whose perspectives are missing in the design of XR and whose rights might be disproportionately impacted if we are not careful. While I strive for academic neutrality in tone, I openly approach the topic with a rights-based, equity-focused lens. This means I am inclined to highlight dangers of XR for marginalized groups. Some might view this as a bias toward skepticism about technology, but I would frame it as a critical corrective to innovation hype. My goal is not to diminish the real positive possibilities of XR; indeed, I discuss positives like increased accessibility for disabled persons via virtual mobility, or the freedom for queer individuals to express themselves in avatar form. However, I remain cautious and grounded in the reality that technology often reproduces societal power imbalances unless deliberately checked.

1.4. Overview of Argument and Structure

In summary, this dissertation argues that IXR technologies are reconfiguring the environment in which fundamental rights are exercised, in ways that demand both conceptual and regulatory adaptation. On one hand, IXR has the potential to enrich human experience and augment the exercise of rights—for instance, by enabling new forms of expression and assembly that transcend physical constraints. On the other hand, IXR's unique affordances intensify certain risks and create novel modes of interference with rights, blurring lines between physical harm and virtual harm, eroding privacy through intrusive sensors, concentrating unprecedented control over impactful digital environments in the hands of private companies, and challenging our legal notions of responsibility in digital contexts. The thesis contends that many fundamental rights principles do carry over into IXR, but the application of these rights in IXR is not straightforward. Moreover, the current EU legal framework, while comprehensive in general digital regulation, has significant gaps when faced with IXR's distinctive challenges. Importantly, because IXR platforms function as reality infrastructures—essentially privatized spaces that mediate user interactions—they exercise a quasi-governance power. This calls for a reconceptualization of the duties of IXR providers: the dissertation will ultimately argue that as immersion increases, so too should the responsibilities of platform operators to respect and protect users' rights. In parallel, the state's role must evolve to set boundaries and standards for these new environments, treating them not merely as products or services, but as spaces where fundamental rights are at stake. Ultimately, the thesis makes the case that moving from the physical world to a mediated reality should not mean a loss of rights, but rather a deliberate effort to carry our rights into the virtual realm through thoughtful governance.

Chapter 3 argues that IXR creates a fundamentally mediated reality—one that exists only through and is shaped by its technological infrastructure. Using Star's infrastructure studies framework (Star 1999), I examine how platform organizations, hardware companies, devices, and users participate in and are constrained by this infrastructure. Unlike physical infrastructure, which regulates behaviors, IXR infrastructure is constitutive of the reality it enables. Through analysis of technical capabilities, accessibility considerations, and user experiences, I demonstrate how the current development of IXR infrastructure embeds inequality into virtual experiences in novel ways. The quality of one's extended reality experience—from visual fidelity to interaction capabilities—becomes directly tied to purchasing power and corporate priorities in ways that transcend typical digital divides. This suggests an urgent need to consider new governance frameworks as IXR technologies become more prevalent. This chapter addresses RQ1 and contributes to infrastructure studies by examining how private control of reality-constituting infrastructure differs from traditional infrastructure, while advancing XR scholarship through a novel theoretical framework for understanding virtual experiences as fundamentally mediated.

Chapter 4 continue the exploration of RQ1 by critically examining the evolution of digital embodiment within cyberspace and VR, analyzing how the narratives surrounding embodiment differ from the experiences of marginalized communities. Narratives of Cartesian disembodiment abounded in the discourse but overlooked that there was no true disembodiment in cyberspace, just anonymity coupled with an assumed identity that was often that of the white, male majority. Early proponents of VR saw it as an inherently embodied phenomenon, but this was supplanted by a dualist narrative that dominated pop culture and academia. As cyberspace evolved from text-based to pictorial, it was acknowledged that bodies impacted online experiences, but many insisted that this should not matter. In today's cyberspace-VR merging, dominant players insist that the body should be celebrated, but this does not come coupled with measures to ensure that they are. This chapter reveals how virtual experiences reflect societal biases, despite narratives to the contrary, foregrounding how the dominant developers of cyberspace and VR have impacted the experiences of marginalized users of both.

The thesis begins to address RQs 2 and 3 in **Chapter 5**, which outlines safety and privacy harms associated with IXR (RQ2) and analyzes to what extent the existing EU framework for digital governance—including the General Data Protection Regulation, relevant product safety legislation, ePrivacy Directive, Digital Markets Act, Digital Services Act, and AI Act—addresses these harms (RQ3). This analysis then lays the groundwork for the recommendations in Chapter 7.

Chapter 6 explores freedoms of assembly and expression in the context of IXR. I outline possible risks and benefits of IXR to the freedoms of assembly and expression. Building on the theoretical framework established in Chapters 3 and 4, it outlines how privately owned XR companies are granted government-like powers over key fundamental rights. Finally, it assesses how specific pieces of EU legislation apply to freedoms of assembly and expression in IXR.

Building on legal analysis from Chapters 5 and 6, **Chapter 7** synthesizes the findings to make policy recommendations, thus addressing RQ3.5. Finally, the **Conclusion** ties the previous chapters together to address the ORQ. Based on the premise that with increased embodiment comes increased responsibility to ensure human rights are upheld because those rights become closer to their physical equivalents, it advances a new framework by which to consider fundamental rights in digital settings. To clarify the level of responsibility that platforms have in immersive contexts, I offer a novel interpretation of the ideas behind the public function and fair procedure doctrines that incorporates the level of embodiment of a given platform to determine the extent to which freedoms of assembly and expression are implicated. The conclusion likely reflects on the broader societal challenge: ensuring that as we enter increasingly mediated realities, our "architectures of control" are aligned with liberty, privacy, self-determination, and other core values rather than undermining them (Lessig 1999, 220). In short, mediated reality should not become a wild west of rights, but rather an opportunity to reaffirm and adapt rights for the digital age.

Chapter 2: Literature Review

This chapter reviews the key bodies of literature that inform my inquiry into XR and fundamental rights. It synthesizes scholarship across XR and cyberspace ethics, the philosophy of technology, platform governance, business and human rights, and the current state of consumer XR. Together, these domains provide a conceptual and contextual foundation for understanding XR's emergence as a fundamentally mediated reality and its human rights implications. The review highlights major debates and developments in each area, with a focus on historical XR and cyberspace literature, postphenomenological approaches to technological mediation, the governance of digital platforms (especially XR platforms), corporate responsibility for human rights (anchored in the Universal Declaration of Human Rights and the UN Guiding Principles on Business and Human Rights), and the contemporary landscape of consumer XR. I identify notable gaps in the literature, underscoring how this thesis will contribute to bridging them. In what follows, Section 2.1 outlines historical XR ethics literature; Section 2.2 examines philosophical frameworks of technology and mediation as they relate to platforms and XR; Section 2.3 discusses platform governance, including the nascent issue of XR platform governance; Section 2.4 addresses business and human rights, covering enforcement theories and the intersection of technology platforms with fundamental rights; and Section 2.5 reviews the current state of consumer XR. Note that to minimize repetition, chapter-specific literature is discussed in the relevant chapters. Though there is some topical overlap, this chapter focuses on situating the dissertation in the wider literature landscape.

2.1. XR and Cyberspace Ethics

As I discuss in Chapter 4, XR ethics are situated in a long history of research on cyberspace and VR. XR has generated a rich discussion about ethics and impacts, dating back to the earliest days of VR. Even in science fiction and early futurist speculation, thinkers foresaw that virtual environments could blur the line between illusion and reality, raising novel moral questions (Slater 2021). By the 1990s, as rudimentary

VR systems emerged, commentators were already worrying about issues like addiction to virtual worlds, escapism, "virtual" crimes, and identity deception in cyberspace (Schroeder 2007). Early academic work began to sort through these speculations in a more grounded way. For instance, Ralph Schroeder's early research on multi-user virtual environments (circa 2007) noted that many ethical and social questions "had not so far received systematic attention" (Schroeder 2007). He argued that discussions must tie closely to the technology's actual capabilities and uses, rather than dystopian hype (Schroeder 2007), much of which was inspired by sci-fi (see Chapter 4). Schroeder distinguished between instrumental VR systems (e.g., experimental or training simulations) and internet-based social VR platforms,[15] noting that each posed different challenges—the former requiring research ethics guidelines and the latter needing norms for appropriate and desirable uses in society (Schroeder 2007). This hinted that VR ethics would span both the lab and the living room, from how researchers design safe virtual experiments to how everyday users behave in shared virtual worlds. This thesis, as discussed, primarily focuses on the latter, but many of its insights apply to the former as well.

A core insight from decades of VR research is that immersive simulations can feel real to our brains and bodies, which makes the experiences exciting and enthralling, but also ethically fraught. Presence, immersion, and interactivity combine to create more realistic and satisfying VR experiences (Mütterlein 2018); AR possesses these factors but to a lesser degree. Decades of interaction studies show that social interaction in VR tend to mimic those of the physical world, requiring us to consider the implications of those norms (Han and Bailenson 2024). Mel Slater, a leading VR psychologist, explains that VR uniquely generates powerful "illusions" of reality which traditional media cannot. These include the feeling of presence—the sense of actually being inside the virtual world, which includes the illusion of being in a place and that events are plausibly occurring (Slater 2021). VR can also produce a body ownership illusion; when users see a virtual body moving in sync with their real movements from a first-

[15] Major social VR platforms include Meta's Horizon Worlds, VRChat, Rec Room, AltspaceVR (discontinued in 2023), Spatial, Neos VR (discontinued in 2025), Resonite, and ChilloutVR.

person perspective, they often feel that "this is my body" (Parshall 2022). And in networked VR, users experience co-presence, the illusion of truly sharing a space with other people's avatars (Slater 2021).

The body ownership illusion deserves more extended discussion, as the foundational work on virtual embodiment builds upon earlier research on the "rubber hand illusion," in which synchronous tactile stimulation of a visible rubber hand and a participant's hidden real hand induces a sense of ownership over the rubber hand (Botvinick and Cohen 1998). Slater and colleagues extended this principle to full-body ownership in virtual reality, demonstrating that when participants view a virtual body from a first-person perspective and experience visuomotor synchrony—seeing the virtual body move in correspondence with their own movements—they develop a perceptual illusion that the virtual body is their own, even when it differs substantially from their physical body (Sanchez-Vives et al. 2010; Slater et al. 2010). This "body ownership illusion" occurs rapidly and reliably, suggesting that the brain's body representation is remarkably plastic and amenable to technological manipulation.

Crucially, virtual embodiment is not merely a perceptual curiosity; it produces measurable changes in cognition, attitudes, and behavior. The "Proteus Effect," first identified by Yee and Bailenson (2007), describes how the characteristics of one's avatar influence subsequent behavior—participants embodied in taller avatars negotiated more aggressively, while those in more attractive avatars engaged in greater self-disclosure. In immersive VR, these effects are amplified. Banakou et al. (2013) found that embodying adults in child-sized virtual bodies altered their perception of object sizes and induced implicit attitude changes associated with childhood. More strikingly, Banakou et al. (2018) demonstrated that embodying participants in a virtual body resembling Albert Einstein improved their performance on cognitive tasks, with the effect most pronounced for participants with lower self-esteem—suggesting that virtual embodiment can temporarily reshape self-concept in ways that affect cognitive functioning.

Because of these various illusions, participants can undergo authentic-seeming emotional and cognitive experiences. This power is dual-use. XR experiences can alter users' attitudes or behavior, intentionally or unintentionally, raising questions about behavioral influence and autonomy. Clinical applications have leveraged this for good (for example, VR exposure therapy for phobias (Freeman et al.

2017)). Additionally, VR has been used as an "empathy machine," with studies finding that embodying someone of a different race, age, or ability can increase empathy and reduce biases (Bujić et al. 2020). It should be noted that critics of the "empathy machine" narrative note that evidence for impact on pro-social behavior is lacking and that VR is not a silver bullet to increase empathy (Sora-Domenjó 2022; Balcerak Jackson and Balcerak Jackson 2024), and that other forms of media can have similar effects (Balcerak Jackson and Balcerak Jackson 2024). Regardless, XR does show impact on attitudes and beliefs. Peck et al. (2013) found that embodying light-skinned participants in dark-skinned avatars significantly reduced their implicit racial bias as measured by the Implicit Association Test. Banakou et al. (2016) replicated and extended this finding, demonstrating that the bias reduction persisted for at least one week after a single brief exposure—a durability that few other bias-reduction interventions have achieved. These studies, alongside work by Maister et al. (2015) and others, suggest that virtual embodiment engages the same neural and psychological processes involved in physical self-representation, with corresponding effects on social cognition.

However, researchers like Slater warn that the same mechanism could be misused; just as VR can be used to reduce bias, a VR scenario could instill new prejudices or harmful mindsets if designed unethically (Slater 2021). Thomas Metzinger and Michael Madary, in a 2016 paper, warned that immersive simulations could have "psychological effects that last after leaving the virtual environment," and called for a proactive "code of ethical conduct" for VR to address risks like false memories, desensitization, or shifts in one's self-perception (Madary and Metzinger 2016). In short, XR's realism is a critical distinguishing factor. Actions and events in virtuality can impact users as if they were real, forcing us to reconsider how we define harm, consent, and responsibility in these mediated worlds.

The literature has also safety and privacy concerns. This includes both physical safety and mental welfare. Physical safety has been a concern with VR since the early days. As discussed in Chapter 5, concerns initially focused on the physical effects of VR because headsets could weigh four kilograms—sometimes requiring external supports—and could cause severe discomfort (Wilson 1996; Costello 1997). Unlike traditional screen media, VR and AR pose physical risks because they involve movement in real space while one's attention is in a virtual layer; a widely-publicized case in Moscow involved a man who, blinded to his surroundings, fell through a glass table and died (Paton 2017).). There have also been high-profile cases of sexual harassment with significant mental health impacts. A well-known early incident was the virtual groping of a female player in a 2016 VR game, who described the assault in visceral terms and noted "I'm still thinking about it" a week later (Belamire 2016). Her testimony sparked a debate on sexual harassment in VR and underscored that attacks on one's avatar can feel so real that they require serious moderation and design responses (Parshall 2022). (In fact, after a similar report in 2021, Meta introduced a mandatory 4-foot personal boundary around avatars in its Horizon Worlds to prevent virtual unwanted contact, although it later allowed users to turn them off (Perez 2022).) The EU's Horizon Europe fund is also sponsoring research into harassment in XR through the META-TOO project ("THE PROJECT" 2024). Privacy was not a major focus on early XR development and research (Lanier and Biocca 1992), but now is the focus of several works, including (Renieris 2023), which outlines the possibility of biometric data abuse. Building on this existing literature and concerns, Chapter 5 elaborates on the safety and privacy risks of contemporary XR, synthesizing existing literature to provide a policy-relevant mapping of risks.

Literature has also emerged regarding content moderation, although this was not anticipated in early literature prior to the rise of platformization. As immersive platforms grow, they inherit all the content governance and moderation risks of the internet—including hate speech, disinformation, and graphic content—but magnified by immersion. A violent or pornographic experience in VR can be far more intense and potentially disturbing than on a 2D screen, leading scholars to argue for new content rating systems and ethical design that gives users fair warning and control. Madary and Metzinger specifically recommended increasing awareness of possible impacts and conducting research into mechanisms to minimize lasting negative effects (Madary and Metzinger 2016). Moderating user-generated content and behavior in shared XR spaces also poses novel challenges because what needs to be moderated is real-time and not easily standardizable, unlike static 2D content. Companies are experimenting with tools like personal safety bubbles, muting/banning features, and even AI-driven content filters for virtual environments; these are discussed more in Chapter 4. However, getting this right is difficult. Over-policing could infringe on freedom of expression, while under-policing leaves users vulnerable to abuse.[16] The ethical imperative is to foster virtual communities that are inclusive and safe. This involves setting behavioral norms, providing users with agency to block or escape harmful interactions, and possibly devising new laws for crimes that are purely virtual but feel very real (a subject of ongoing debate in legal and ethics circles).

This dissertation's fundamental rights framework can be seen as a continuation of Elizabeth Renieris's call to use human rights as a backstop against datafication and commodification in her book *Beyond Data: Human Rights at the Dawn of the Metaverse*. She argues that:

> We must move beyond a limited application of human rights that emphasizes narrowly conceptualized rights to privacy and free expression over and above all others—- an application historically shaped by globally dominant Western technology companies and viewed through an outdated ICT lens. (Renieris 2023, 171–72)

She acknowledges, as does this thesis, that as physical and virtual worlds blur, we cannot separate "physical" rights from "virtual" rights. This thesis is in part an elaboration on the mission to "start from the perspective of people rather than from the vantage point of data, technology, commerce, or the market" (Renieris 2023, 172). Her book focuses primarily on data protection; this thesis builds on her data privacy work and incorporates other forms of privacy in Chapter 4 and examines other rights in Chapters 5-7.

From the work of early VR ethicists to the latest discussions of the metaverse, it is clear that immersive technology forces society to revisit old ethical questions in a new light. The historical literature on XR ethics converges on a common conclusion: we must treat immersive technologies with the same seriousness as real life. The early XR ethics literature provides a roadmap, but it also highlights that we are entering technologically novel territory. In the coming years, ensuring that virtual worlds remain

[16] For a discussion of policing criminal behavior in XR, see Appendix 6.

respectful of our rights will be an essential part of the broader quest to marry technology with ethics in the digital age.

2.2. Philosophy of Technology and Mediation in Platform Studies

The philosophy of technology offers critical insights into how digital platforms and XR mediate human experience. A central concept in this area is technological mediation—the idea that technologies are not neutral tools but actively shape perceptions, actions, and social relations. Contemporary scholars building on postphenomenology (notably Ihde and Verbeek) argue that technology mediates the relationship between humans and the world, co-constructing our experience of reality (Ihde 1990; 2015; Verbeek 2016; 2012). Rather than a human subject and a technological object interacting at arm's length, postphenomenology views human–technology–world relations as intertwined; the subject and the world are mutually constituted through technological mediation. In VR, for example, the user's sense of presence, embodiment, and even identity are profoundly shaped by the design of the virtual environment and interface (Vindenes and Wasson 2021; Murray 1999). By embodying users in avatars and immersing them in designed worlds, VR technologies illustrate how mediation goes beyond transmitting information—they actively reconfigure the user's situated experience of self and world (Vindenes and Wasson 2021). AR likewise mediates experience by overlaying digital elements onto physical environments, blurring the boundary between the "real" and the virtual. In sum, philosophy of technology provides a vocabulary for understanding XR as a transformative mediating layer in human experience; this is elaborated upon in Chapters 3 and 4.

Within platform studies, a related strand of scholarship examines how digital platforms serve as mediating infrastructures of social life. Early work on "platform" concepts in media and software studies (e.g., Bogost and Montfort (2009)) has evolved to treat major online platforms (social media, content-sharing sites, etc.) as structuring environments that shape user behavior and social interaction (Plantin et al. 2018). Platforms mediate not only content delivery but also the very possibilities of action and connection through their technical design and policies. Key features identified in platform studies include affordances and constraints set by the platform, algorithmic curation, and the connection of heterogeneous actors (including users, advertisers, and third-party developers) (Plantin et al. 2018). Notably, scholars have drawn parallels between platforms and infrastructure, observing that large platforms increasingly function as essential societal infrastructure for communication and information, while infrastructures (like telecom networks or cloud computing) are becoming more platform-like (Plantin et al. 2018). Plantin et al. (2018) describe a convergence where platform studies and infrastructure studies meet: platform companies achieve a quasi-infrastructural status (ubiquitous, reliable, taken-for-granted), and infrastructures adopt platform-like modularity and openness.

In particular, my infrastructural view of XR (advanced in Chapter 3) owes a debt to Lawrence Lessig's 1999 "Code: And Other Laws of Cyberspace" (Lessig 1999) (and its 2006 follow-up, "Code 2.0" (Lessig 2006)), known for the aphorism "code is law" (Lessig 1999, 6). He argues that code forms the law of cyberspace. At the time, it was still debated whether the "Net" *should* and *could* be regulated. Lessig argued for both, but noted that regulation in virtual settings is more than just law as passed by legislatures; "code is a regulator in cyberspace because it defines the terms upon which cyberspace is offered" (Lessig 2006, 84). This resonates with this thesis's argument that the infrastructure of XR shapes both social and sensory experiences, which carries corresponding moral significance. Indeed, Lessig asks: "How do we protect liberty when the architectures of control are managed as much by the government as by the private sector?" (Lessig 1999, x–xi). With the evolution of technologies and market structures, this thesis can be thought of as a response to the question, "How do we protect liberty when the architectures of control are managed *much less* by the government than by the private sector?" It also points out that as digital technologies have developed, we have been asking similar questions about what they mean for society and governance. XR amplifies these questions because of the immersion and intensified psychological impacts that make interactions more morally salient, but it is a continuation, not a phase shift. The theoretical development of considering platforms as infrastructure is important for XR, which can be seen as both a platform (in the sense of software ecosystem and content environment) and an infrastructure for mediated experience.

Building on traditions from phenomenology and science and technology studies (STS), researchers have also explored how embodiment and identity are mediated in digital realms. Decades before today's VR, cyberspace theorists debated whether going online enabled escaping one's embodied identity or instead replicated real-world biases. As discussed in Chapter 4, cyber-utopian views hoped the internet would be a disembodied realm of pure mind, but feminist and critical theorists countered that offline power structures (gender, race, disability, etc.) reassert themselves in virtual interactions. Contemporary XR, with its visually and physically immersive avatars and environments, makes embodiment central: users feel present in a body schema within the virtual world, and this can both empower (e.g., enabling new perspectives) and marginalize (e.g., exposing users to avatar-based harassment). The literature, as discussed in Chapter 4, traces a historical arc from text-based virtual worlds, where identity play was constrained by text and imagination, to graphical social VR where one's avatar appearance and voice can closely parallel (or deliberately contrast with) one's physical traits. Postphenomenology contributes the insight that mediated embodiment in XR is not "virtual" in the sense of trivial or inconsequential—on the contrary, virtual experiences can loop back to affect one's physical-world attitudes and sense of self. For example, studies have shown that embodying people in avatars of a different race or age in VR can measurably shift their real-world biases or empathy. Such findings reinforce the notion that XR environments are continuous with "real" life in their impact, aligning with Floridi's concept of the "onlife" condition in a hyperconnected era—the merging of online and offline into a single, hybrid reality. In Floridi's terms, we increasingly live onlife, where digital systems are woven into the fabric of everyday existence, dissolving the old dichotomy between virtual and real (Floridi 2015; Ess 2015). XR is perhaps the epitome of onlife: a realm where the distinction between physical presence and digital presence is blurred by design.

In summary, the philosophy of technology and platform studies literatures provide a framework to recognize XR as a mediating technology that actively shapes human experience rather than passively transmitting it. XR platforms function as architectures of perception and action, built upon layers of corporate-controlled infrastructure that define what is possible in a given immersive world. This theoretical perspective underscores why XR raises unique ethical and rights-related questions: if our sensory, social, and even identity experiences are conditioned by privately designed systems, issues of power and inclusion come to the fore. A notable gap is that, despite rich theory on mediation and some nascent discussions of XR as infrastructure, there has been limited explicit linkage of these concepts to fundamental rights. Few studies have yet connected postphenomenology or mediation theory with a legal-human-rights analysis of XR's design (though calls to accompany technological development with critical scrutiny are growing (Floridi 2015)). This thesis helps fill that gap by applying mediation theory to interrogate how XR's design might enhance or diminish basic rights such as equality, privacy, and autonomy. By reframing XR as a "fundamentally mediated reality," I set the stage for asking how its architectures might be governed or designed in alignment with human rights values.

2.3. Platform Governance

As digital platforms have become central nodes of communication and social life, questions of how they are governed have become paramount. Platform governance refers to the frameworks and practices through which the operators of platforms (and, increasingly, governments and other stakeholders) set rules and norms for behavior, content, and participation online. A substantial body of literature has emerged around how major platforms like Facebook, YouTube, and Twitter moderate content, enforce policies, and exercise power over users—essentially functioning as private regulators of speech and interaction. Scholars have pointed out that these companies perform a kind of governance role traditionally associated with states (Plantin et al. 2018). For instance, companies establish community standards and use a combination of algorithms and human moderators to remove disallowed content, which has direct consequences for users' freedom of expression and exposure to harm. These governance decisions are often opaque and driven by corporate interests, prompting debates about accountability and transparency.

Over the past decade, key trends in platform governance include the professionalization of content moderation (and the subsequent dissolution of many trust and safety (T&S) teams) (Moran et al. 2025; Patja et al. 2023), the development of appeals mechanisms (like Facebook's Oversight Board) (Edelson 2024), and external pressure from governments and civil society for platforms to better address issues such as disinformation, hate speech, and election interference (for a detailed discussion of this, see Appendix 6). At the same time, platforms have resisted being characterized as publishers or traditional media, in part to avoid legal liability for user-generated content. In the US, the legal backdrop of Section 230 of the 1995 Communications Decency Act[17] has given platforms broad immunity from liability for third-party content while allowing them discretion to moderate as they see fit (Kim and Mellafe 2024). This immunity is often credited with enabling the rise of social media platforms, but it also places the onus of governance on the private companies themselves, since government regulation of lawful online speech is limited by both law and the First Amendment.

The literature highlights a divergence between the US and Europe in regulating platforms. The US has historically taken a hands-off approach—relying on industry self-regulation and the market, with the government intervening only in specific areas like child sexual abuse material or intellectual property. The EU, by contrast, has increasingly legislated responsibilities for platforms in the interest of protecting users' rights and societal values. A salient development is the EU's Digital Services Act (DSA),[18] adopted in 2022, which imposes due diligence obligations on "very large online platforms" (VLOPs) for managing systemic risks including impacts on fundamental rights. The DSA requires VLOPs to conduct risk assessments (not unlike human rights impact assessments) for issues such as dissemination of illegal content, manipulation that affects elections or public security, and harms to civic discourse and rights, and to put in place mitigation measures. This reflects a trend of embedding human rights principles into platform governance at the regulatory level (Belic et al. 2024).

[17] (S.314 - 104th Congress (1995-1996) 1995)

[18] (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) 2022)

Additionally, European regulators and courts have been more willing to balance platform freedoms with user rights—for example, the "right to be forgotten" ruling requiring Google to de-list certain personal data upon request (a privacy right versus platform's free expression).[19] Complementing the EU's legislative efforts, the Council of Europe has also issued guidance, such as its Recommendation CM/Rec(2022)13 on the impacts of digital technologies on freedom of expression, emphasizing principles like transparency, user remedies, and the need to protect against arbitrary restrictions by platforms (Committee of Ministers 2022). The "Brussels effect" is often cited, where EU tech regulations (from data protection to platform accountability) set *de facto* global standards due to large platforms complying globally with the strictest rules, or *de jure* laws from other governments adopting similar standards (Bradford 2020). Some scholars, however, caution against viewing the European model as an unalloyed success; they argue that even rights-based EU regulations have limits and can entrench the power of big platforms if not complemented by deeper rethinking of platform power structures (Belic et al. 2024). Nonetheless, from a comparative perspective, the EU literature emphasizes public oversight and rule of law in platform governance, whereas US discourse often emphasizes free speech and innovation, only recently shifting to discuss reform (e.g., proposals to amend Section 230 or impose transparency requirements).

2.3.1. XR Platform Governance

Extended reality platforms—including, but not limited to, social VR worlds and multiplayer AR games—bring new dimensions to platform governance debates. On one hand, they inherit many of the challenges seen in traditional online platforms (content moderation, user behavior policies, data governance); on the other hand, XR amplifies these issues with its heightened immersion and embodiment. Early studies and reports on social VR environments have observed significant incidents of harassment, abusive behavior, and even sexual assault (unwanted groping of avatars, etc.) in immersive platforms (Outlaw 2018). The

[19] (*Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* 2014)

level of immersion in XR can make harmful interactions feel intensely real to users; one victim of a VR sexual harassment attack found her "real heart racing" from the virtual assault (Nix 2024). As discussed earlier, psychologically and physiologically, users are more vulnerable to harm because the virtual experience engages their senses and bodily presence in ways flat-screen social media do not (Martens et al. 2019). This places a premium on effective safety measures and moderation in XR. However, moderating XR is notably complex. Unlike text or images that can be algorithmically scanned for keywords or hashes, XR involves real-time 3D interactions, gestures, voice chat, and spatial behavior, which are far more difficult to automatically monitor without invasive data collection; this is discussed more in Chapter 4 and Appendix 5.

Some work has analyzed XR platform governance. The Institute of Electrical and Electronics Engineers (IEEE) issued a report arguing for a global approach to the governance of metaverse platforms (Stephens 2022). Gray et al. (2024) assess governance on social VR platforms, focusing on content and conduct risks and calling for proactive government regulation to protect users and ensure platforms prevent harms, rather than reactively respond to harms. Saghafi and Angelopoulos (2025) address the specific governance challenges of VR human-like AI interactions, and Blackwell et al. (2019) was an early look at harassment in social VR. Most existing literature focuses on "social VR" (which has significant overlap with the concept of the "metaverse"). Karanicolas et al. (2024) is an exception in that it addresses the privacy concerns of AR systems, but this thesis's treatment of immersive AR is overall a contribution to the literature.

While there is limited literature applying traditional platform governance studies to XR, the literature identifies a range of governance *tools* being developed for XR: technical safety features (personal "bubbles" or safe zones that a user can activate to create space around their avatar, the ability to mute, block, or "ghost" other users so they become invisible, etc.), as well as community guidelines and human moderation akin to what exists on traditional platforms (S.B. et al. 2024). Major XR platforms have begun to implement some of these controls. For example, Meta's *Horizon Worlds* has a code of conduct and allows users to mute or distance themselves from others to counter misbehavior. Community moderation is another strategy: VR platforms can empower trusted users to act as moderators in communal spaces or allow community-run instances with their own rules (similar to how Reddit entrusts subreddit mods with the governance of their communities) (Kim and Mellafe 2024). Analysis suggests XR governance will likely require a multi-layered approach, combining top-down enforcement of minimum standards by the platform with bottom-up community management for specific worlds or groups (Kim and Mellafe 2024). As discussed further in Appendix 5, it is likely that that no single entity can monitor all behavior on an IXR platform with one single method—thus, platforms must enlist both design and social mechanisms.

A notable point in XR governance discussions is the role of architecture or design as regulation. Building on Lessig's dictum that "code is law," commentators argue that XR developers can build safer environments by design before bad behavior occurs (Kim and Mellafe 2024). For instance, the platform could prevent certain interactions: age-gating rooms so that children are not mingling with unknown adults (to preempt grooming or inappropriate contact) or requiring identity verification such that users cannot hide behind total anonymity when abusing others. Automated filtering of virtual content (e.g., blocking graphic violence or sexual content) is theoretically possible if the system can recognize those elements in real time, though this is an evolving technical challenge. Prevention-by-design—a form of pro-ethical design (Floridi 2016)—has advantages: it is proactive and can reduce the burden on after-the-fact moderation. However, over-reliance on design restrictions might also limit the openness and spontaneity that make XR platforms attractive; it raises the risk of over-moderation or privacy violations. Thus, XR governance needs to strike a balance between safety and user freedom, an aim I try to strike in my recommendations in Chapter 7.

Legal frameworks are only beginning to grapple with XR. In the US, current laws (like Section 230) apply to XR platforms much as they do to any online service, meaning platforms are generally shielded from liability for user actions but also largely responsible for policing their spaces. This has led to suggestions that initially, governance of "lawful but awful" conduct in XR (e.g., bullying that is not illegal per se) will rely on platform self-regulation more than government intervention (Kim and Mellafe

2024). In Europe, it is plausible that the DSA's provisions will eventually encompass large XR platforms, obliging them to assess risks such as harassment or content impacts on rights. Yet, concrete regulatory guidance specific to XR (for example, how to handle virtual crimes or protect children in VR) is still nascent, meaning that XR platforms are still largely self-regulated.

XR platform governance is an emerging field at the intersection of tech policy and design. Early research underscores that the immersive nature of XR heightens both the stakes and the challenges of content moderation and user safety. Harassment can feel more visceral and damaging, but detecting and preventing it is harder given new interaction modalities. The literature to date suggests combining technical safeguards, user empowerment tools, and community norm-setting to address these issues. A gap in the literature, however, is the relative scarcity of comprehensive studies on governance models tailored to XR—most writings so far are conceptual or extrapolate from 2D platform experiences. There is, for instance, little empirical research yet on what governance strategies best reduce harm in social VR or how users perceive the trade-offs of safety versus privacy in those spaces. This thesis contributes to filling that gap by examining XR governance through a rights-oriented lens, asking how principles of fundamental rights (like non-discrimination, freedom of expression, and dignity) can inform the rules and design of XR platforms. It also highlights currently under-explored questions such as the accountability of XR providers for user experiences and the governance of emergent behaviors unique to immersive settings, proposing an embodiment and rights-grounded governance framework in Chapter 8. By situating XR governance within platform governance debates, I argue that XR should not remain a lawless frontier but rather can learn from the hard lessons of social media—ideally before it reaches the scale of billions of users. Part III of this dissertation will specifically address governance questions around safety and privacy (Chapter 5) and freedoms of assembly and expression (Chapter 6) in XR, building on the foundation laid here.

2.4. Business and Human Rights

The expansion of powerful technology companies has prompted extensive discussion on business and human rights (BHR), an interdisciplinary field that examines the duties of corporations with respect to internationally recognized human rights. Traditionally, human rights law was state-centric: states bear obligations to uphold rights like those in the Universal Declaration of Human Rights (United Nations General Assembly 1948b), whereas private actors were not direct duty-bearers under treaties. However, as multinational corporations' activities began to have global human rights impacts, advocacy and scholarship in the late 20th and early 21st centuries pushed for mechanisms to hold businesses accountable (McCorquodale 2024, 7–13). Early intergovernmental efforts included the OECD Guidelines for Multinational Enterprises and the ILO Tripartite Declaration (1977), later updated to reflect the UNGPs, while the UN Sub-Commission's 2003 "Norms" ultimately failed to gain UN endorsement (McCorquodale 2024, 10–12).

Against this backdrop, the Human Rights Council endorsed the UNGPs' three-pillar Framework: states' duty to protect, corporate responsibility to respect (operationalized through human rights due diligence), and access to remedy (Special Representative of the Secretary-General 2008). This culminated in the United Nations' adoption of the Guiding Principles on Business and Human Rights (UNGPs) in 2011 (United Nations Human Rights Office of the High Commissioner 2011a), after years of work by UN Special Representative John Ruggie (Davis 2012). The UNGPs rest on three pillars—Protect, Respect, and Remedy—which delineate that (1) states have a duty to protect human rights (including against abuses by third parties like companies), (2) companies have a responsibility to respect human rights (i.e., to avoid infringing on rights through their operations and to address harms they are involved in), and (3) there should be greater access to effective remedy for victims of business-related abuses (through judicial or non-judicial means). The UNGPs are a soft-law instrument: they are not legally binding, but they have been widely endorsed and have set expectations for corporate conduct globally. They call on companies to implement human rights due diligence—an ongoing process to identify, prevent, mitigate, and account for how the company addresses its human rights impacts.

The corporate responsibility is framed as a standard of expected conduct—"doing no harm" through proactive due diligence to identify, prevent, and address adverse impacts—rather than a freestanding body of hard law. Illustrative catastrophes such as the 1984 Bhopal disaster—where 45 tons of toxic methyl isocyanate leaked from an insecticide plant due to insufficient safety procedures, killing 15,000-20,000 people and causing health problems for an estimated 500,000 more (The Editors of Encyclopaedia Brittanica 2025a)—crystallized the problem: transnational corporate structures and forum challenges produced accountability deficits that BHR seeks to narrow.

2.4.1. Theories of Enforcement and Corporate Accountability

A persistent challenge in the BHR field is the enforcement gap: how to move from principles to practice in corporate behavior and accountability for harms (Floridi 2019). The literature discusses several approaches, often in combination, to enforce human rights standards for businesses.

The first is voluntary compliance and self-regulation. Many companies have adopted human rights policies or joined initiatives like the Global Compact or Global Network Initiative (for tech firms) (Global Network Initiative, n.d.; "UN Global Compact" 2025), pledging to uphold certain rights. While these can be important, critics note that without external enforcement, such commitments may serve more as blue-washing or ethics-washing if not accompanied by transparency and independent oversight (Floridi 2019). Indeed, analyses of corporate human rights reporting have found they are often superficial or selectively disclosed (Chambers and Vastardis 2021). This has led scholars to argue that relying on the market to police corporate reports is insufficient (Chambers and Vastardis 2021).

When voluntary guidance falls short, litigation and legal liability step in. In some jurisdictions, affected parties have tried to sue companies for human rights abuses—for example, using tort law or statutes like the US Alien Tort Statute (ATS).[20] However, significant hurdles both legal and practical often prevent success, including jurisdictional issues, high costs, and difficulty proving causation. Additionally,

[20] (Alien's Action for Tort 1948)

the US Supreme Court in recent years narrowed the scope of the ATS for corporate cases (Farbstein 2023). There have also been lawsuits in home countries of multinationals for abuses in foreign subsidiaries—for example, UK and Canadian courts have seen cases on environmental and labor harms (Neely and Smit 2025; Baker and Cutifani 2025; Dodge 2020)—with a few notable victories but many challenges remaining. Litigation alone thus provides patchy enforcement at best.

In the past decade, some national laws have emerged requiring companies to report on human rights or take due diligence steps. Examples include the 2017 French Duty of Vigilance Law[21] which requires certain large firms to actually conduct due diligence to prevent human rights and environmental harms, backed by potential civil liability, and Germany's 2021 Supply Chain Due Diligence law,[22] which requires enterprises over 1,000 people to establish risk management systems to protect human rights, with failure to comply punished with significant fines. In 2024, the EU Directive on Corporate Sustainability Due Diligence[23] went into effect, aiming to set a baseline of human rights due diligence across member states. These laws mark a trend of turning what was a voluntary guideline (due diligence per the UNGPs) into a legal obligation.

Yet scholars have pointed out limitations. Many early laws emphasize disclosure and transparency over substantive performance, and enforcement mechanisms are weak or unclear. For instance, Rachel Chambers and Anil Yilmaz-Vastardis observe that early transparency laws effectively outsourced enforcement to civil society and consumers, as states did not create robust oversight bodies or penalties for non-compliance (Chambers and Vastardis 2021). Without government oversight, many companies simply ignore the reporting requirements or provide vague assurances, undermining the effectiveness of such legislation (Chambers and Vastardis 2021). The authors argue that the state should reassert a key role in monitoring and sanctioning compliance, rather than leaving it entirely to private actors (Chambers

[21] (LOI N° 2017-399 Du 27 Mars 2017 Relative Au Devoir de Vigilance Des Sociétés Mères et Des Entreprises Donneuses d'ordre (1) 2017)
[22] (Gesetz Über Die Unternehmerischen Sorgfaltspflichten in Lieferketten 2021)
[23] (Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on Corporate Sustainability Due Diligence and Amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859 (Text with EEA Relevance) 2025)

and Vastardis 2021). Newer laws like the French Duty of Vigilance Law hint at this by allowing NGOs to sue companies for not having adequate vigilance plans, but these are still evolving.

There is ongoing debate about a binding international treaty on business and human rights. Since 2014, a working group at the UN has been negotiating a potential treaty that could impose obligations on transnational corporations (OHCHR, n.d.-a). However, progress is slow and positions divided; objections include that states may use the treaty to offload their own human rights responsibilities and that the exclusion of purely national corporations would leave significant governance gaps (Loizides 2016). No treaty is in place as of 2025. If one were adopted, enforcement would depend on national implementation and international monitoring—a significant political hurdle.

In certain sectors, multi-stakeholder initiatives (MSIs) play a role in enforcement-like functions through their standards-setting role. For example, the Fair Labor Association and Ethical Trading Initiative set labor standards and conduct audits in supply chains ("Home - Fair Labor Association," n.d.; "Home | Ethical Trading Initiative," n.d.), while the aforementioned Global Network Initiative sets free expression and privacy standards for ICT companies with some independent assessment. These bring some external review, but participation is voluntary and coverage limited to willing companies.

In summary, enforcement theories converge on the idea that a mix of measures is needed—combining binding regulations with incentives and transparency. The literature highlights that we are seeing a gradual move from pure voluntarism toward more coercive mechanisms (like mandatory due diligence). Still, a gap remains between policy and practice, and many communities affected by corporate human rights abuses have yet to see effective remedies. This thesis engages with that gap by considering how these enforcement challenges manifest in the context of XR and digital platforms—domains that until recently were not central in BHR discussions. The XR industry might face similar issues (e.g., a VR platform causing psychological harm or enabling rights abuse) without clear accountability pathways. Thus, one contribution here is to investigate the largely uncharted territory of business and human rights in XR, asking what enforcement of human rights norms might look like for immersive tech companies.

2.4.1. Technology Platforms and Human Rights

Technology platforms—from social media networks and search engines to e-commerce and now XR environments—have become influential actors in the realization (or infringement) of human rights. Multiple rights can be affected by platform practices: freedom of expression and information (through content policies, algorithmic curation, or censorship), privacy (through data collection and surveillance-based advertising models), equality and non-discrimination (through algorithmic bias or disparate impacts on marginalized groups), freedom of assembly (through online groups and now virtual gatherings in XR), and even the right to security and bodily integrity (insofar as online harassment or coordinated violence can lead to physical harms). The UDHR and subsequent human rights treaties enshrine these rights universally, and there is a growing consensus that the private sector must play a role in upholding them in digital spaces (Jørgensen 2019). Policymakers, civil society, and international bodies have increasingly framed digital platform issues in human rights terms (Belic et al. 2024)—for example, describing internet access as linked to the right to freedom of expression, or content moderation as needing to respect freedom of expression while protecting people from discrimination and violence. The UNGPs provide the high-level framework: platforms as companies have a responsibility to respect all internationally recognized human rights. In practice, this means they should have policies and due diligence processes to avoid infringing on users' rights and to address any harms that occur. Indeed, companies like Meta, Google, and Microsoft have publicly affirmed their commitment to human rights and in some cases publish human rights impact assessments (HRIAs) for certain products or policies (Ugarte 2024).

Despite these commitments, the literature offers a critical perspective on how effective a human rights-based approach to platform governance has been so far. One line of critique is that human rights discourse, when adopted by companies, can be somewhat selective or instrumental. Platforms may highlight rights that align with their business model (e.g., "free expression" to encourage specific groups to use the platform) while giving less weight to others (e.g., privacy, equality) until pressured; the literature expresses concerns that corporate human-rights-preserving methods like human rights impact assessments (HRIAs) may be ineffective at best and "ethics-washing" to make practices appear more ethical at worst (Latonero 2018). There is also the structural issue that human rights law evolved to constrain state power, not the diffuse, privatized power of platforms (Wodajo and McDonald 2024; Golia 2024). The conventional human rights legal regime can struggle to address situations where platforms create conditions leading to human rights abuses without direct state action. For instance, Facebook's involvement in the spread of hate speech that fueled ethnic cleansing against the Rohingya in Myanmar is often cited (Amnesty International 2022). A private platform contributed to gross human rights violations, but accountability was hard to achieve since international human rights law binds Myanmar more directly than it binds Facebook. Another concern is that the human rights framework itself, being very general and often focused on minimal state obligations, may not be fully adequate to capture the positive duties we might want platforms to uphold. Human rights law requires states to protect individuals from abuses (including by private actors), but it does not straightforwardly require a social media company to, say, provide a safe online environment—unless domestic laws translate that duty. We are left with gaps between aspirational calls for platforms to follow human rights standards and the lack of legal force or precise standards to hold them to account.

Nevertheless, progress is being made in integrating human rights into platform governance. The UN B-Tech initiative (launched by the Office of the High Commissioner for Human Rights) provides guidance on applying UNGPs in the tech sector, including case studies and recommendations for how companies can embed human rights due diligence into development of new technologies (Office of the United Nations High Commissioner for Human Rights 2024). We also see cross-pollination in regulatory regimes: the EU's Digital Services Act, as mentioned, implicitly pushes platforms toward human rights thinking by naming fundamental rights among the risks to assess and mitigate. The UN Global Digital Compact (a UN initiative aiming to set principles for digital cooperation) explicitly reaffirms the application of international human rights law in digital contexts ("Global Digital Compact" 2024). Similarly, the Council of Europe's Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law represents a major step towards creating binding international standards for AI development and deployment grounded in fundamental rights principles (Council of Europe 2024). Various "Internet Bills of Rights" have been proposed by civil society, seek to articulate how existing rights translate to the digital environment (De Minico 2015). Furthermore, civil society and user advocacy have invoked human rights in campaigns—for example, Access Now's initiatives on digital rights or the Ranking Digital Rights project which evaluates tech companies on criteria derived from rights to expression and privacy (Ranking Digital Rights 2025; Access Now, n.d.).

The UN has increasingly emphasized that digital technologies, while empowering, also pose serious human rights challenges. As UN Secretary-General António Guterres notes, we must "better curtail harmful use of digital technology" while also "better unleash its power as a democratizing force and an enabler" (OHCHR 2022). In practice, this means recognizing that the same human rights that people enjoy offline apply fully online. The UN has affirmed that existing international rights treaties—largely drafted before the digital era—still "exist online as they do offline and have to be respected in full" (UN Secretary-General 2020). Digital tools can advance free expression, access to information, and civic participation, but they are equally used for "surveillance, repression, censorship, and online harassment," often targeting vulnerable groups and human rights defenders (UN Secretary-General 2020). The UN warns that new technologies like facial recognition, algorithmic profiling, and digital identification systems are already "used to violate and erode human rights, deepen inequalities and exacerbate existing discrimination" if left unchecked (UN Secretary-General 2020). In short, the UN's position is that technology must not be a pretext to undermine fundamental rights.

To uphold this principle, the UN has taken concrete steps to integrate human rights safeguards into technology governance. In 2012, the Human Rights Council passed a landmark resolution declaring that "the same rights that people have offline must also be protected online," making clear that freedom of expression and other rights extend to the internet (United Nations General Assembly Human Rights Council 2012). Following global surveillance revelations, the UN General Assembly affirmed "the right to privacy in the digital age" and urged states and companies to ensure that digital surveillance and data collection comply with international human rights law (United Nations General Assembly 2014). High

Commissioner reports have explored how to apply human rights norms to emergent areas like artificial intelligence and social media content moderation (Office of the United Nations High Commissioner for Human Rights 2025). The UN Secretary-General's 2020 Call to Action for Human Rights and Roadmap for Digital Cooperation both made "digital human rights" a priority, calling for guidance on how human rights standards apply in the digital age (UN Secretary-General 2020; Guterres 2020). Indeed, the UN system is now producing a large volume of outputs on technology and rights—a recent mapping by the High Commissioner in 2024 found "an astounding level" of UN human rights work related to digital tech (United Nations High Commissioner for Human Rights 2024; Human Rights Council 2024).

Crucially, the UN is urging governments and companies to put human rights at the center of digital innovation and regulation. The High Commissioner's 2024 report recommended that states, businesses and other stakeholders "take into account and implement" the growing body of UN human rights recommendations "that apply to the design, development, operation, use, and regulation of digital technologies" (United Nations High Commissioner for Human Rights 2024). It called for intensifying efforts to ensure human rights are "fully considered across all policy areas relevant to the governance of digital technologies," from trade and consumer protection to cybersecurity and artificial intelligence (United Nations High Commissioner for Human Rights 2024). One proposal is to create new "peer review" mechanisms (akin to the Universal Periodic Review) focused specifically on digital rights, so that states can share best practices and address gaps in protecting rights in the tech sector (Human Rights Council 2024). The UN Secretary-General has likewise stressed that both governments and tech companies must conduct human rights due diligence for new technologies. In his roadmap, he urged Member States to "place human rights at the centre of regulatory frameworks and legislation on the development and use of digital technologies," and he called on technology firms to publicly pledge to respect privacy and other rights in their products and services (UN Secretary-General 2020). The UN's message is that technology governance should always be guided by the universal human rights framework—ensuring that digital progress does not come at the cost of human dignity, equality or freedom.

In the specific context of XR and human rights, the literature is only beginning to emerge. XR brings the possibility of new types of rights issues—for instance, the concept of "bodily privacy" or mental privacy, since devices like VR headsets and AR glasses can collect intimate data about one's physiological responses and surroundings. There are concerns about eye-tracking data, emotional analysis, and other sensitive information in XR being misused, implicating the right to privacy in unprecedented ways. Likewise, if XR becomes a venue for education, work, and social life, then accessibility and non-discrimination become key: will people with disabilities have equal access? Will content moderation algorithms inadvertently silence minority groups' expression in virtual spaces as sometimes happens on social media? An EU-funded study concluded that there is a need for "improved protection from harmful online content to promote and strengthen compliance with human rights law at the national and international level" in XR and for clearer allocation and demarcation of responsibility for harmful content (Vinders 2023). It also concluded that XR can have both positive and negative impacts on human rights (Vinders 2023). This thesis attempts to strike a balance between discussing both positive and negative impacts on human rights. The study also discusses the possible necessity of new and emerging rights like the right to disconnect and right to be online that might be relevant in an XR-pervasive society (Howkins and Vinders 2022), a point also raised by Renieris (2023). These discussions reflect doubt in the current human rights paradigm's ability to account for digital harms and will be discussed further in Chapter 8.

In summary, technology platforms are now central to human rights realization, and XR is poised to continue that trend by blending physical and digital realms. The literature encourages using the UDHR and the corpus of human rights law as a normative compass for platform governance, but also urges realism about gaps in enforcement and conceptual fit. A notable gap in current research is specific, detailed analysis of XR providers' human rights responsibilities. Much of the focus to date has been on social media and internet access; only recently have XR companies been scrutinized for, say, how their content policies align with freedom of expression or how their data practices might infringe privacy. This thesis situates consumer XR platforms squarely within that BHR discourse. Using the UDHR as the rights baseline and the UNGPs as the governance paradigm, it treats device and platform affordances as sites where the "responsibility to respect" must be specified: not only avoiding infringement, but designing and governing immersive systems so that foreseeable rights impacts are identified, mitigated, and remediated. In doing so, the project extends BHR's largely content- and supply-chain-oriented literature into embodied, mediated environments where platform design choices structure expression, association, safety, privacy, and equality at the level of lived experience. It also attempts to close the BHR implementation gap by proposing an embodiment-based framework to clarify the level of human rights responsibility of digital platforms.

By translating due diligence and remedy into IXR's concrete platform practices, the thesis contributes to closing the implementation gap the BHR field continues to acknowledge—clarifying how a social-expectation standard can become operational governance for US- and EU-anchored XR platforms with global reach.

2.5. Current State of Consumer XR

Having examined theoretical and governance literatures, this section turns to the current state of consumer extended reality—the practical context in which XR is developing today. Understanding the industry and adoption landscape of XR is crucial for grounding the subsequent rights analysis in reality. Over the past few years, XR has transitioned from a niche technology to a steadily growing consumer market, albeit one that has not yet achieved the ubiquity that some tech evangelists predicted during the recent "metaverse" hype.

Beyond consumer applications, XR technologies are increasingly deployed in professional contexts. Healthcare uses include surgical training, exposure therapy for PTSD and phobias, pain management, and rehabilitation (Kouijzer et al. 2023). Educational applications range from virtual laboratories to historical recreations and language immersion (Dhimolea et al. 2022; Potkonjak et al. 2016; Desai 2018). Industrial uses include design visualization, remote collaboration, and safety training (e.g., for hazardous environments) (Scorgie et al. 2024; Berg and Vance 2017). Military and defense applications, such as training simulations, have been significant drivers of XR development (Schroeder 1993). While this thesis focuses primarily on consumer applications due to their direct fundamental rights implications for the general public, these professional uses also raise important considerations regarding fundamental rights that should be explored in further work.

The XR market primarily encompasses VR headsets, AR devices (including forthcoming glasses), and hybrid MR systems. As of 2025, VR headsets (which fully immerse users in virtual environments) form the bulk of consumer XR usage (Siegler 2025). Market research indicates that one company—Meta—continues to dominate the consumer VR space through its Quest line of headsets (Siegler 2025). In 2014, years before their rebranding, Facebook purchased VR headset start-up Oculus and began integrating it into its "wider suite of social software," developing an imaginary portraying it as "a new frontier for social media" (Egliston and Carter 2022). In 2021, Facebook's rebranding to "Meta" and its heavy investment in the "metaverse" triggered industry fervor, including increased sales of the Quest 2 headset and the release of the Quest 3 (Siegler 2025). By 2024, Meta's strategy of selling hardware at relatively affordable prices (often below cost) to drive adoption had paid off in market share: Meta captured roughly 77% of global VR headset shipments in 2024, and with the launch of the Quest 3S in late 2024, its share spiked to about 84% in Q4 2024 (Siegler 2025). Competing VR devices exist—notably Sony's PlayStation VR2 (tethered to the PS5 console and popular among gamers) and various Windows PC VR headsets—but none rival Meta's user base and ecosystem. Sony's PSVR2, for instance, achieved a boost to around 9% share in late 2024 following price promotions (Siegler 2025), appealing to the console gaming market. A major new entrant was Apple, which announced the Vision Pro MR headset in 2023 and released it in 2024. The Vision Pro, positioned as a high-end "spatial computing" device blending AR and VR, garnered enormous attention; however, its very high price and initial focus on productivity and enterprise use mean it has not (yet) reshaped the mass market. Indeed, after an early burst of sales to enthusiasts, Vision Pro shipments declined significantly by the end of 2024 (Siegler 2025). Still, Apple is continuing its XR development, including cheaper MR devices (Walker 2025), and its entry into the market may yet catalyze XR development and competition in coming years. Indeed, Samsung is expected to release a series of XR devices starting in the fall of 2025 (Cole 2025).

In the augmented reality segment, truly consumer-oriented AR glasses have struggled to come to market, although non-AR smart glasses are making inroads; sales of the Ray-Ban Meta smart glasses tripled year-over-year in 2025 (Vanian 2025). True AR products like Google Glass (a pioneer a decade ago) found more success in enterprise settings (Clark 2023). Many AR devices remain enterprise-focused or in prototyping (Carter 2024), although there is consumer momentum building as miniaturization improves. Companies like Xreal have released lightweight AR eyewear for media viewing, although they are tethered by wire to another device (Stein 2025b). Apple is expected to enter the smart glasses and eventually the AR glasses market in the coming years (Clover 2025). Industry analysts predict AR smart glasses will grow as technology improves and as integration with AI opens new use cases (Siegler 2025). Snap's developer-focused Spectacles are nearing commercialization (Stein 2025a), and Amazon is reportedly developing AR glasses for consumers and delivery drivers (Ma and Osawa 2025). In the most significant sign that AR glasses could be poised to make an industry impact, though, in September 2025, Meta announced its Ray-Bans Display glasses—the first mass-market AR glasses of the current XR development wave (Meta Developers 2025). Although their $800 price tag is still significant, it is less than half the price of Google Glass when adjusted for inflation.[24] Though their commercial viability has yet to be determined, considering the popularity of Meta's smart glasses, it is possible that this could be the inflection point for AR glasses entering the consumer domain.

The consensus is that AR could eventually surpass VR in everyday impact (by enhancing the physical world rather than replacing it), but VR has made more headway so far in engaging consumers (especially for gaming, entertainment, and social VR). It is worth noting that overall, XR device sales experienced a dip in the early 2020s after an initial boom—global VR headset shipments actually fell ~12% year-on-year in 2024, marking the third year of decline (Team Counterpoint 2025). This has been

[24] Google Glass started at $1,499 (Bohn 2014), which is over $2,000 in 2025 dollars (Bureau of Labor Statistics, n.d.).

attributed to factors like hardware limitations, lack of must-have content, and a post-pandemic cooling of enthusiasm (Siegler 2025). However, enterprise demand for XR (e.g., for training and simulation) provided a cushion and grew even as consumer demand slumped (Siegler 2025). The industry remains optimistic that technological improvements (lighter headsets, better optics, more content and services, and the integration of AI) will spur the next wave of adoption (Siegler 2025). In fact, projections before the pandemic often foresaw explosive growth by decade's end, with various groups predicting hundreds of billions of dollars to up to $5 trillion in economic impact (Garcia 2023), an estimate that now appears overly optimistic. Nonetheless, a multi-hundred-billion-dollar market in the coming decade is plausible as XR applications diversify and technologies mature.

The US has been the epicenter of consumer XR innovation since the early days of VR, home to Meta, Apple, Microsoft (which pioneered enterprise AR with the HoloLens), and many content developers.[25] US consumers have accordingly been early adopters of VR for gaming and social experiences. American tech culture's interest in the "metaverse" concept peaked around 2021 and 2022, driven by Meta's promotion and a broader cultural moment (including other platforms like *Roblox* and *Fortnite* being discussed as "proto-metaverses") (Ravenscraft 2023). While the feverish rhetoric has tempered, the US remains a leading market for XR devices and content creation. Policy-wise, the US government has had no specific regulation for XR, though agencies and the military are significant investors in XR for defense and training (Nieuwsma 2025; Vive Business, n.d.). Some lawmakers have raised concerns about safety in the metaverse and child protection, but legislative action is still in exploratory stages (TechPolicy 2025). By contrast, the European Union and European countries engage with XR largely through existing digital regulation—ensuring that emerging XR offerings comply with GDPR (privacy) and upcoming AI regulations, for example. The EU has funded research (like the aforementioned TechEthos project) to study XR's societal impacts. In 2023, the European Commission

[25] China has emerged as a significant player, with companies like Pico (now owned by ByteDance) and XReal developing competitive hardware, and the Chinese market representing substantial growth potential (Statista 2025). South Korea (through Samsung) and Japan (tbrough Sony) also contribute significantly to the global XR ecosystem. However, to limit the scope of the discussion, I focus on US XR companies.

published a strategy paper on virtual worlds (European Commission 2023b), aiming to shape an open and "human-centric" metaverse, and launched a VR/AR Industrial Coalition (European Commission 2025d). These efforts indicate an intention to influence the development of XR in line with European values (interoperability, privacy, safety) and not leave it purely to foreign big tech.

The current primary uses of consumer XR include gaming and entertainment (including VR games, immersive films, virtual tourism), social interaction (social VR platforms like *VRChat* and Meta's *Horizon Worlds* where users hang out as avatars and attend virtual events or concerts), creative and educational applications (such as virtual art programs, language learning in VR, etc.), and some fitness and health uses (including VR fitness apps, meditation experiences, and exposure therapy in controlled VR environments). The "metaverse" concept envisions many of these use cases converging into persistent virtual worlds where people might also work and conduct commerce. However, this has not come to fruition, illustrated by the decline in VR uses. Mobile AR (via smartphone apps like Pokémon Go, Snapchat's AR lenses, or IKEA's furniture placement app) arguably touches far more users, introducing AR concepts on familiar devices and laying the groundwork for potential future immersive AR uses.

The literature and reports on XR's trajectory often emphasize that we are at an early stage akin to the internet in the early 1990s or smartphones in the early 2000s. Immersive technology is expected to integrate with other emerging tech like artificial intelligence and 5G connectivity, potentially leading to transformative new applications. Experts are split on if and when a truly immersive "metaverse" will materialize for the average person, but most agree that aspects of XR will gradually seep into everyday life (for example, AR elements in routine smartphone use, VR for specific professional training, etc.) (Anderson and Rainie 2022). This situational analysis reveals a gap in the literature as well: while there is abundant coverage of XR's technical development and market trends, there is comparatively less research on the human rights implications of these current trends. Most policy discussions are just beginning to catch up to XR, often extrapolating known issues from social media rather than examining XR-specific dynamics in depth. Consequently, one of the contributions of this thesis is to contextualize the state of consumer XR within a rights framework. Essentially, I ask: as XR stands today, what rights are already engaged or at stake, and what can we learn from current conditions to shape a better, more rights-respecting future considering the likely trajectory of the technologies? By doing so, this work addresses a gap between technical XR literature and normative human rights scholarship. In providing this review of XR's current state, we are better positioned to identify where governance, design, and enforcement interventions might be most needed to ensure XR evolves in a rights-respecting manner.

In this chapter, I have surveyed the historical XR ethics literature; the philosophical underpinnings of XR as a mediated, technologically constructed reality; the emerging norms and challenges of governing platforms; the frameworks of business accountability to human rights; and the landscape of the contemporary XR consumer industry. The literature illustrates that XR sits at the confluence of these domains. Yet it also reveals fragmentation—few works have bridged platform governance, human rights, and modern XR. This thesis aims to bridge those gaps. The theoretical insights on mediation (Section 2.2) will inform my argument that XR's design choices carry moral weight for user experiences. The platform governance review (Section 2.3) grounds my inquiry into what regulatory and self-governance models might be apt for XR. The business and human rights discussion (Section 2.4) provides a normative foundation—the UDHR and UNGPs—to assert that fundamental rights must be protected even when reality is mediated by private platforms. Finally, the industry overview (Section 2.5) ensures my analysis stays tethered to how XR is unfolding in practice. Together, these literatures set the stage for the next chapters, where I investigate the philosophical underpinnings into XR as infrastructure and relationship to embodiment (Part II), then its specific rights implications for safety, privacy, freedom of assembly, and freedom of expression (Part III). By drawing on and connecting these diverse scholarly conversations, the thesis contributes to an urgently needed understanding of the impact of extended reality on fundamental rights in a way that is philosophically grounded, governance-aware, and attuned to real-world developments.

Part II: Theory

Overview

Part II, comprising Chapters 3 and 4, develops the theoretical core of the dissertation. It asks what it means to treat extended reality (XR) not as a set of apps or devices, but as a reality that is constituted—and thus normatively shaped—by its mediating infrastructures and by the ways bodies are rendered and regulated within them. The chapters that follow argue that XR's "onlife" character binds sensory and social experience to technical and institutional design choices, with implications that reach well beyond usability into questions of power, equality, and rights. In doing so, they address my first research question:

RQ1: What does the structure of IXR services mean for individual user experiences?

Chapter 3 advances the central claim that XR is best understood as infrastructure: the constitutive substrate through which experiences become possible at all. Operating at this level of abstraction, platform organizations, hardware makers, devices, and users are arranged in stratified layers of mediation, with decisional power cascading downward and autonomy correspondingly constrained. This stratification means that both sensory and social experience are conditioned by corporate choices and by one's purchasing power, risking a tiered reality in which access and quality of experience are unequally distributed. The chapter thus reframes XR as a *fundamentally mediated reality* whose architectures of affordance organize power.

Chapter 4 complements this infrastructural analysis with a historical and philosophical account of embodiment in virtual environments. It traces the movement from early, text-based narratives of disembodiment toward today's more explicitly embodied avatars, showing that *who appears* and *how* online have long reproduced offline hierarchies of gender, race, and disability, despite promotional narratives to the contrary. Drawing on phenomenology, the chapter argues that virtual embodiment is never merely optional self-presentation; it shapes and is shaped by lived experience, with consequences for whose participation is legible and safe in XR spaces.

Together, these chapters supply the conceptual frame for the dissertation's later rights analysis: if XR infrastructures constitute experience and if embodiment in XR is both consequential and contested, then governance questions must be asked at the level of reality construction itself. Part III takes up this task by examining how these theoretical commitments bear on safety and privacy (Chapter 5) and on freedoms of assembly and expression (Chapter 6).

In short, Part II argues that XR is a reality built through layered mediation and lived through bodies that are differentially vulnerable and empowered. Naming XR as infrastructure and embodiment as constitutive experience is not a semantic choice; it is a normative one. It clarifies why design and governance decisions distribute experiential quality—and why a rights-attentive approach is required in the parts that follow.

Chapter 3: Extended Reality as a Fundamentally Mediated Reality: XR Infrastructure and the Ethics of Experience

3.1. Introduction

Extended reality (XR) technologies are increasingly entering the consumer domain, and with them questions about what they mean for our lives on- and offline. XR encompasses virtual reality (VR), augmented reality (AR), and mixed reality (MR) (Milgram and Kishino 1994), and as intermediaries between us and the physical and virtual spheres, these technologies impact our experiences, wellbeing, and even fundamental rights. The rise of XR underscores the blurring between the physical and the virtual characteristic of the "onlife" environment the rise of information and communication technologies has created (Floridi 2015). The muddled boundaries of the onlife raise fundamental questions about how we experience our reality, and because XR technology promises to create a new extended reality where the physical and virtual interact to different degrees, it is a particularly salient area of philosophical inquiry. Historically, not all groups have had equal experiences in cyberspace, which carries into XR (Hine 2024b). Racist and sexist harassment are rife on social VR platforms, and many platforms and devices are not accessible to disabled users, impacting how users experience XR. This is of significant concern because XR's immersive, embodied realism creates experiences—both sensory and social—similar to those in the physical world (Hine 2024b; Fauveau et al. 2024) and thus nondiscrimination, safety, privacy, and other fundamental rights are of heightened concern (Hine, Cowls, et al. 2024). In this chapter, I discuss a conceptualization of extended reality as a *fundamentally mediated reality* and emphasize the implications of that mediation for our sensory and social experiences in the physical and virtual spheres. I do so using the level of abstraction of infrastructure (Floridi 2008), using it to argue that XR technology is the infrastructure of a fundamentally mediated, "onlife" reality.

This chapter is indebted to several areas of study, the first being mediation theory. I adopt the "empirical-philosophical" approach described in (Verbeek 2012), drawing on both theory and actual examples of technology. Affordance theory also makes an appearance. Affordances, as defined by Gibson (1979), are possibilities for action that an environment or object "offers" a subject. They are relational properties that affect a being's abilities in a given environment (Chemero 2003). When a specific organization—such as a technology company—is defining affordances, that creates a power hierarchy because they are defining what actions are available to the user. I also utilize infrastructure theory as a key framing. At a basic level, infrastructure is what other things "run on" (Star 2002). At a higher level, infrastructure is "part of human organization" and must be studied as such (Star 2002), especially when it does not serve specific groups (Star 1999). For instance, a smartphone that is too large for the average woman's hand means that the keyboard becomes a piece of infrastructure that does not serve all groups equally well (Petter 2018). While much has been written about specific incidents in XR and how different groups have different experiences with the technologies and experiences they facilitate (with some of these incidents referenced throughout this thesis), no work has yet examined the power structures that enable them. As the infrastructure of a fundamentally mediated reality, XR technology plays a primary role in how people experience XR. The infrastructure level of abstraction allows us to look at the ecological structure of XR (Star 1999), at layers of power, and thus investigate *why* people have differential experiences and what can be done to make XR as accessible and positive as possible.

Infrastructure is inherently linked to questions of power and hierarchy, as whoever makes decisions about infrastructure is making decisions about human organization (Star 1999). In the case of XR, this decision-making power is particularly pronounced because XR's existence is dependent on its infrastructure. To borrow from Searle (2018), XR infrastructure is *constitutive* of the reality. Many things in our physical world depend on physical infrastructure: cycling takes place on paved roads and paths, taking a shower indoors is possible because of pipes, and so on. However, this infrastructure is merely *regulative*; it guides and constrains existing behaviors rather than enables their existence. Without that infrastructure, the world and those behaviors are still there; you can ride a bicycle without a paved road, and the bicycle still exists in the absence of a road. This is not the case with XR, which does not exist without its enabling infrastructure. In other words, a bicycle (and road) in an XR environment cannot exist without the XR platform and cannot be used without an XR device, and without those enabling pieces of infrastructure, the bicycle and road cannot exist (regardless of their persistence when any individual user logs on or off). Because XR infrastructure is constitutive of the reality, it is fundamentally mediated by that infrastructure: a fundamentally mediated reality. This chapter thus contends that extended reality (XR) constitutes a new kind of infrastructural mediation—one that not only delivers experience but helps define what kinds of experiences are possible and accessible. This has profound ethical implications; when XR infrastructures are proprietary, opaque, or inaccessible, they risk entrenching existing inequalities, excluding marginalized users, and fragmenting shared reality itself. Thus, the normative urgency of this paper lies in asking: Who gets to inhabit the future of reality?

Sittig and Singh (2010) present a sociotechnical model for studying health information technology, a critical part of health infrastructure. Their model involves eight dimensions: hardware and software computing infrastructure, clinical content, human-computer interface (HCI), people, workflow and communication, internal organizational features, external rules and regulations, and measurement and monitoring. I adopt this model in this chapter (with the substitution of more general "content and experiences" for "clinical content") because it is a compelling way to break down a complex technological infrastructure and observe its constituent parts. I will examine these at four levels: the platform organization, the hardware company, the device, and the user. At each level, I will explore how the entity mediates the infrastructure of XR and how, each level down, some decision-making power and thus autonomy is lost.

In this chapter, I focus on immersive extended reality (IXR) devices and applications, which encompasses XR that mediates one's entire sensory field (Hine, Rezende, et al. 2024). With current XR technology, this applies mainly to the visual field, and so IXR right now primarily refers to modern headset VR and "immersive" AR, which includes AR glasses but not, for example, smartphone AR, heads-up car displays, or advertising or sports information overlays on television broadcasts. These devices are the most mediating of one's sensory and social experiences and thus the most impactful on one's fundamental rights.

The chapter proceeds as follows: Section 3.2 examines the entities that have the most control over users' social experiences: platform operators. Section 3.3 looks at hardware companies, which control the mediation of users' sensory experiences. Section 3.4 discusses the devices themselves, and Section 3.5 the users. Section 3.6 synthesizes the previous sections to discuss how layers of decision-making and mediating power impact how users experience IXR. Section 3.7 concludes.

3.2. Platform Operators

Unlike physical reality, IXR requires a platform, meaning that whoever creates that platform acts as a fundamental mediator of XR, with correspondingly significant decision-making power. Platform organizations—often, but not always, companies—that run IXR platforms influence the content, human-computer interface, internal policies, people, and hardware and software that mediate user social experiences.

3.2.1. Content

The most apparent level of mediation is of content. Platforms consist of content, which in IXR can also involve embodied user *conduct*. Rather than text, photos, and videos, IXR content spans AR filters, VR worlds, live behavior and interactions, and other modalities. Thus, there are new forms of static *content*, as well as a plethora of dynamic *conduct*. These form the basis of a user's experience, and the quality of the content is directly related to the quality of the user's experience, much like the quality of the water going through pipes impacts the person drinking that water. The larger question of whether a particular platform is "good" and what makes it so is beyond the scope of this chapter, but I will focus on three specific aspects crucial to experience quality: content moderation, governance and culture, and platform accessibility. All three are part of the infrastructure of IXR and all three are heavily influenced by the platform organization itself, which in turn impact users' social experiences.

3.2.2. Content & Conduct Moderation

As with other online platforms, content moderation is crucial to having a quality experience in IXR. However, IXR creates additional challenges because content moderation also involves the moderation of dynamic *conduct*, which is inherently more challenging than moderating content. If a platform is full of abusive or toxic content, or people constantly behaving poorly, people will be less inclined to use it. Most of the time, content moderation blends into the background as part of the invisible platform infrastructure; when it breaks down and toxic content seeps into people's platform experience—or when one's own content is moderated—is when it becomes apparent. While often framed as a neutral or protective process, moderation in IXR operates as a form of infrastructural regulation: it shapes what forms of conduct and identity are permitted to appear, which harms are acknowledged, and who is burdened with maintaining safety.

Content moderation can be done by human or automated means, or some combination of the two. Moderation enforcement has a direct bearing on the quality of one's social experiences in IXR. Not only are already-marginalized communities the most likely to be the targets of abuse based on their gender, race, or sexuality (Center for Countering Digital Hate 2023), but their content is also more likely to be targeted for takedown, both by human and automated mechanisms (Oliva et al. 2021). This means that the infrastructure of moderation is much more present to them than to someone from not from a marginalized community, who can exist in an IXR space without fear of over-moderation.

On a logistical level, IXR content moderation presents challenges because of new content and conduct modalities. Both challenge the concept of automated moderation, which relies on machine learning (ML) models trained to identify abusive content (Gongane et al. 2022). However, this means that content must be in a standardized and analyzable format. It is likely that the lack of universal standards for XR is hindering automated content moderation (XR Association 2024), but efforts are ongoing and platform companies are heavily involved; all of the "Magnificent Seven" Big Tech companies save Tesla are involved in the Metaverse Standards Forum (MSF), as are other IXR companies like Pico and Sony (Mallika 2024; Metaverse Standards Forum 2024).[26]

At present, major social VR platforms primarily use human moderation (Schulenberg, Li, et al. 2023; Gray et al. 2024c). While this theoretically allows for them to take more context into account, it causes its own issues. On a practical level, in-world moderators do not scale; in one study, just 24% of potentially harmful incidents were addressed by moderators (Sabri et al. 2023). As a result, human moderation is not an adequate proactive solution. Instead, platforms are primarily reactive and rely on player reports of abusive behavior. However, these reactive measures "do not prevent harm and they tend to place the burden of managing safety on victims, who are most commonly women and other marginalised users" (Gray et al. 2024c). This has proved problematic for "borderline incidents" that may or may not be acknowledged as abuse (Gray et al. 2024c). Furthermore, whether or not platforms provide information on reporting processes and outcomes may influence people's willingness to report, as not informing people creates the impression that their reports are being ignored and discourages them from further reporting (Gray et al. 2024c). Thus, the way that platforms delegate responsibility to moderators and act on user reports—in other words, the moderation infrastructure they create—has a large and potentially inequitable impact on individual social experiences.

Automated moderation, based on systems trained on biased human decisions, is also vulnerable to bias. Algorithmic content moderation systems contain inherent biases that results in content from already-marginalized communities being taken down more often than content from other communities (De Gregorio and Stremlau 2023; Haimson et al. 2021). These stem from the decisions of platform organizations make about what training data they use, as automated systems replicate biases within training data. When human moderation decisions are biased, so too are the systems trained on that data. And human moderation is frequently biased—for instance, reports on live stream platform Twitch disproportionately target women (Zolides 2021). However, it must be noted that these inequities are in part because of how Twitch crafts its Community Guidelines (Zolides 2021), showing the mediating

[26] Alphabet is involved as Google (Metaverse Standards Forum 2024).

power platform organizations possess. Like live streaming, IXR contexts that involve avatars bring in elements of physical appearance and the biases that accompany that, such as racism, sexism, ablism, and other identity-based judgements (Hine 2024b), again meaning that the infrastructure of moderation is more apparent to them. Content moderation—both human and automated—thus mediates not just behavior but also presence, implicitly defining who is able to safely engage with IXR.

A problem for both human and automated content moderation is the issue of parody and satire in content. Even if IXR content and conduct were easily characterizable, their multiple layers of meaning creates a contextual opacity that complicates moderation. In 2022, *Buzzfeed* journalists created a world in *Horizon Worlds* called "The Qniverse" and filled it with content banned from Facebook and Instagram. It remained up after 36 hours, showing an apparent lack of automated screening mechanisms. After three separate reports to Meta, they received a message that "Our trained safety specialist reviewed your report and determined that the content in the Qniverse doesn't violate our Content in VR Policy." The journalists theorized that "maybe content moderators took it to be a parody" (Baker-White 2022). The fine line between parody and not is difficult for even humans to assess, to say nothing of algorithms.

Conduct shares these problems. Behavior that would be unacceptable against strangers may be accepted or even welcomed between friends—think about the difference between a "buddy punch" and walking up to a stranger and punching them. To an outsider—or a motion detection algorithm—they may be indistinguishable, even though only one causes harm. Such examples reveal that mediation here is not simply a matter of detecting deviance, but of interpreting meaning within socially contextualized embodiment—a task that is both politically charged and epistemically uncertain.

There are indications that IXR platforms are beginning to explore more automated means of content moderation. For instance, VR platform *Rec Room* uses voice filtering software to proactively mute abusive users (Gray et al. 2024c; Hughes 2021). Proactive automated moderation would reduce the burden on individuals to report abusive behavior. However, as mentioned above, it brings with it a new set of concerns. Algorithmic content and conduct moderation could more actively prevent harm, but must be responsibly developed and implemented to avoid exacerbating biases. In one study, approximately 30% of algorithmic content moderation decisions could be classified as "arbitrary" (i.e., dependent on model development choices like the parameter initialization seed) (Gomez et al. 2024). This is a part of content and conduct moderation infrastructure that is wholly controlled by the governing platform organization.

In sum, platform content moderation in IXR environments exemplifies a form of regulative mediation—a layered process by which platforms do not simply filter harmful content, but actively shape the conditions of social legibility, harm recognition, and experiential participation. This mediation is not neutral: it encodes institutional values into the infrastructure of perception and social interaction. The invisibility of this infrastructure to some users and its hyper-visibility to others—especially women, racialized users, and gender-nonconforming individuals—renders the experience of "reality" unequally accessible. Moreover, by delegating safety to reactive, user-triggered mechanisms, platforms privatize responsibility while maintaining control over enforcement and epistemic standards. In doing so, they construct a tiered mediated reality: one in which experiential legitimacy depends on one's social location, perceived deviance, and conformity to platform norms.

3.2.3. Governance and Culture

Depending on the platform structure, platform governance is not always top-down. IXR platforms can be either centralized or decentralized, two forms of governance mediation that have unique risks. Centralized platforms are owned and operated by a single entity, often a corporation. For example, *Horizon Worlds* is owned and operated by Meta, while *Rec Room* is published by Rec Room Inc. Decentralized platforms use a distributed governance model, sometimes leveraging a blockchain (Verizon, n.d.). *Decentraland*, the most prominent decentralized IXR platform, uses a decentralized autonomous organization (DAO) for community governance; every member of the community can vote on proposals that are recorded on the blockchain.[27] This affects how rules and community standards are

[27] Due to the high "gas" fees associated with using the Ethereum blockchain, Decentraland records votes "off-chain." A three-person DAO Committee "selected by the community" is then responsible for recording decisions on the blockchain.

established and enforced. On a decentralized platform, platform rules—the platform's governing infrastructure—are theoretically democratically created, while on a centralized platform, the single governing entity establishes the rules.

These have different repercussions for rulemaking. In the centralized case, the rules may be affected by the platform organization's commercial interests, such as their desire to not be banned in certain countries (Hine 2023). However, decentralized governance is no panacea—it reflects the opinions and biases of the community, which could result in actions or rules that are offensive to or oppressive of portions of the community. For instance, a journalist who witnessed racist harassment in a *Horizon Worlds* comedy club reported that the individual being abused was ejected from the club using a "poll-to-remove" feature, and when the journalist questioned the decision, he was also ejected (Gray et al. 2024a). This case illustrates how governance infrastructure mediates power relations: by embedding social norms into technical affordances, platforms can empower majorities to silence or eject dissenting or marginalized voices, reinforcing structural asymmetries under the veneer of collective control. The structure and rules of an IXR platform undergird and constrain its content moderation infrastructure, so whatever entity controls that process has significant power to construct experiential hierarchies in IXR.

Platform governance in IXR constitutes a second-order form of normative mediation—it structures not just what can be said or done, but how norms themselves are generated, contested, and enforced. Whether governance is centralized or decentralized, the key mediating function is the production of authority: who gets to define acceptable behavior, whose experiences are legible as harm, and whose voices shape the evolving norms of digital space. Whether centralized or decentralized, governance in XR platforms does not merely moderate behavior—it prefigures the structure of reality itself, determining whose norms become infrastructural defaults and whose dissent becomes invisible, disruptive, or removable.

They are in turn overseen by the Security Advisory Board, a group of five chosen by the Decentraland development team ("How the DAO Works" 2024). Thus, there is some amount of centralized authority even in decentralized platforms.

3.2.4. *Accessibility*

Accessibility is how platform organizations ensure their platform is usable for people with disabilities and is part of the platform infrastructure. Thus, platform organizations must make technical decisions that affect accessibility. IXR apps and platforms present accessibility barriers for users with physical, visual, hearing, and/or cognitive disabilities (Creed et al. 2024b), partially because XR accessibility standards are still being developed (W3C Working Group 2021). As a result, through their design decisions, platform organizations mediate who can use their platforms and how. For instance, blind and low-vision users often struggle to use IXR platforms because of a lack of standard accessibility technology (like screen readers on the traditional web) (Zhao et al. 2019; Collins et al. 2023). Thus, platform access is majorly limited by the accessibility infrastructure—or lack thereof—that platforms invest in, which in turn means that IXR infrastructure functions less well for specific people and thus that their ability to experience IXR is impaired. These technical decisions function as mediating acts: they preconfigure which bodies and senses are treated as normatively compatible with XR, and which are excluded by default.

A form of content that is not unique to IXR but of unique importance in IXR is user representation, which also impacts accessibility. As the web has evolved, so too has user representation, from textual descriptions to pictorial icons to three-dimensional, full-body avatars (Hine 2024b). Avatars are the representation of a user and, especially in VR, users identify strongly with them (Freeman et al. 2020). Thus, representation is important so that as many users as possible can portray themselves as they like; Meta emphasizes that it has over a quintillion possible avatars to enable people to be "authentically" themselves in VR (Meta Quest Blog 2021). However, early VR platforms were not so inclusive, often lacking darker skin tone options, and modern platforms still lack many disability representation options (Hine 2024b). Thus, avatar creation infrastructure is not always equitable, and without adequate representation options, people (especially of marginalized identities) may not feel comfortable in those virtual spaces, creating barriers to access. Avatar self-presentation also opens new avenues for targeted harassment (Hine 2024b). The avatar infrastructure is thus not merely aesthetic—it is a moral and epistemic infrastructure that enables some users to be perceived as real, recognizable subjects, while others are left unrepresented or misrepresented in ways that diminish their social standing and comfort.

Representation options also mediate how people behave. The "Proteus Effect" describes the phenomenon where people's behavior changes depending on their digital self-representation. For example, participants who used more attractive avatars were more prone to self-disclosure, and people in taller avatars were more confident in negotiation tasks (Yee and Bailenson 2007). Thus, via their representation options, platforms can influence individual behavior, acting as a mediator between them and others. This is related to the online disinhibition effect, which can see people behave worse when online than they do in the physical world (Suler 2004). Whether platforms allow users to be anonymous or not will likely affect this. If they do so, it may result in more harassment, even coupled with moderation. This is an accessibility issue because how users behave towards others affects their experiences of IXR, potentially in a negative way. Here, accessibility becomes intertwined with behavioral engineering: platforms' design choices not only influence how users are seen, but also how they act and are treated—exposing marginalized users to disproportionate risks of harassment or misinterpretation.

3.2.5. HCI

The human-computer interface is a crucial element of any technology, including IXR. As with other technologies, how the HCI is designed has usability and accessibility implications. One that is particular to IXR, though, is the usability of physical anti-harassment measures. Because harassment in IXR, especially embodied VR environments, feels more visceral and akin to physical-world harassment than harassment on the non-immersive Internet, it is of particular moral concern and prevention measures should be as easily accessible and effective as possible (Hine, Rezende, et al. 2024). Some extant mechanisms include reporting buttons in menus ("Updates to User Reporting Requirements and Developer Tools in VR" 2023), muting functions, and "power gestures" that creates a bubble of personal space (Stanton 2016). However, users often report being unable to figure out how to use safety mechanisms in the heat of the moment (Blackwell et al. 2019), meaning that effective design and user education to ensure that reporting mechanisms are intuitive to access when one is being harassed are crucial. In other words, how platform organizations design reporting infrastructure impacts how it is able to be used and by whom.

3.2.6. Internal Policies and People

Every IXR platform body has its own internal people, policies, and politics. Internal dynamics and procedures determine who at a company is empowered to make decisions. For instance, if engineers have concerns about business practices, they may not be empowered to speak up if part of an organizational hierarchy that does not allow their concerns to be transmitted up to decisionmakers. A decentralized organization may not have suitable procedures in place to escalate concerns and make decisions; while decentralized decision-making can be good for responsiveness by circumventing bureaucracy, it suffers in terms of reliability and compliance, efficiency, and consistency (Vantrappen and Wirtz 2017). Organizational values also inform internal policies; the people who establish those values and the ones that translate them into internal policies establish who has decision-making power and thus who has power over the structure of IXR platform infrastructure. IXR platform executives report being influenced by science fiction classics, including *Snow Crash* and *Ready Player One* (Tassi 2021; Newton 2021; D'Onfro 2016). However, science fiction does not translate seamlessly to reality, meaning that the decisions about IXR infrastructure made in pursuit of these imaginaries—originating largely from white, male, Western cultural contexts—may not take into account how real users want to use this technology in the real world. As a result, the mediation of XR environments can reflect aspirational narratives and internal politics rather than lived experience—producing systems optimized for speculative futures rather than equitable presents.

3.2.7. External Regulations and Hardware

Sittig and Singh (2010) define "external rules, regulations, and pressures" as "external forces that facilitate or place constraints on the design, development, implementation, use and evaluation" of the technology. IXR platform organizations are governed by these, particularly laws and rules created by governments and the technological standards that guide technology development. While platform organizations themselves can be influenced by outside factors, here I will mention that IXR platform organizations, particularly so-called Big Tech companies, are active in lobbying government bodies for favorable laws; Amazon, Google, Meta, and Microsoft together spent $64.2 million on lobbying in 2023 (Henshall 2024).

Big Tech companies are also active in lobbying for technical standards, including for IXR. Technical standards are political because getting one's standard adopted is lucrative for patent-holders, avoids costly redesigns, and functions as a mechanism for values exportation (Roberts et al. 2023). The aforementioned Metaverse Standards Forum was founded by companies including Adobe, Epic, Meta, Qualcomm, and Unity. While files like JPEGs all conform to a standard specification (for JPEGs, ISO/IEC 10918-7:2023 (ISO/IEC 2023)), as do pieces of physical infrastructure like PVC water pipes (ISO 1452-1:2009 (ISO 2009)), XR lacks such standards, so, for example, items from different IXR platforms cannot be transferred and displayed on other platforms. While outsiders are not privy to the inner workings of the MSF and any internal political processes, it is notable how involved private companies are in these standards, creating a situation where the providers of IXR infrastructure are deciding how it will be implemented. This entanglement of lobbying, standards-setting, and hardware influence reflects a form of meta-infrastructural mediation, wherein platform organizations shape not only the experiential layers of XR but the technical and legal architectures that define its future. By embedding corporate priorities into both policy and hardware, they extend their power beyond platforms—structuring what realities become possible, compatible, or profitable in the first place.

Platform organizations are the highest-level mediator of IXR. IXR is fundamentally a platform-driven experience, meaning that the organizations that control them are fundamental mediators of extended reality. If XR defines the edges of perceptual and social reality, then the decisions embedded in its infrastructure are not ethically neutral. They determine who is visible and who is included. Beyond the platforms and experiences themselves, it is also likely that platform organizations also influence the next level down—hardware—especially since some companies, including Meta, create both platforms and hardware. While platform organizations are constrained by technological capabilities, they also guide hardware development by deciding what sort of experiences they want to provide, including whether they want to focus on AR or VR experiences. Meta in particular has begun prioritizing AR devices and experiences after seemingly deciding that AR is a more promising consumer experience (Rodriguez 2024), thus shaping the infrastructural hardware and consumer experiences. Although this influence goes both ways, platform organizations indisputably have a role in hardware priorities and development. In the next section, we will discuss the role of hardware companies in the mediation of IXR.

3.3. Hardware Companies

Because devices are the only gateways into IXR, they have to be designed and manufactured by a hardware company. From sensor architecture to operating systems, their design choices precondition the user's perceptual, physical, and social engagements with IXR. These decisions affect not only usability and privacy but also who can participate—and how—within mediated environments. IXR technology is egocentric (Grauman et al. 2022), meaning that it collects data about the world from the perspective of the user, which is novel because in the physical world, only individuals egocentrically experience the world.[28] IXR technology can not only observe the world from an egocentric perspective, but also datafy it, creating novel datasets and accompanying privacy concerns. Furthermore, because IXR technology is often worn on the body, it impacts individual self-presentation in the physical world. We will discuss more specifics about the impacts of IXR devices in the next section; this will focus on the decisions the hardware companies make about those devices.

[28] It could be argued that some other wearables, such as the Humane AI Pin, are also egocentric technologies, but they have a limited field of vision and face major questions about their commercial viability (Mickle and Griffith 2024).

3.3.1. Hardware

By deciding what sensors are included on a device, hardware companies have direct control over what kinds of data can be collected in the physical environment. These sensors are generally unobservable by the user, fading into the invisible infrastructure of the device, but they are continuously collecting data. However, users are often not aware of the magnitude of data collection (Abraham et al. 2022), and parents lack awareness of the privacy implications for their children (Cao et al. 2024), showing the embeddedness of infrastructure.

IXR also brings in novel privacy concerns. Because IXR is an egocentric technology and IXR devices collect data about one's physical local environment, local privacy is of significant concern (Hine, Rezende, et al. 2024). This includes information about the physical surroundings but also about bystanders who may be unaware that their data is being collected. Data collection is of course necessary to make IXR function—for instance, hand trackers need to observe the user's hands—but platforms can also collect auxiliary data not strictly necessary for provisioning their services. They can then use this data for commercial purposes, theoretically including targeting advertisements. This may affect how users feel comfortable using the technology because their egocentric perspective, including their biometric data but also data about their local environment, is being observed and datafied. Research shows that even the perception that one's online activity might be monitored can create a chilling effect (Penney 2016), and so an extended reality with fundamentally less privacy than physical reality—or other digital environments—might also change how individuals are comfortable interacting with it, with marginalized individuals potentially more reluctant to sacrifice their privacy. In other words, how hardware companies bake in privacy (or do not) to the device infrastructure influences its use, mediating XR not merely through functionality but also through epistemic filtering.

3.3.2. Software & HCI

The decisions hardware companies make about their products—the infrastructure of IXR—are guided by larger corporate strategies. These strategies thus inform how their products mediate user experiences. For example, Apple and Meta have products occupying different ends of the price spectrum. The Apple Vision Pro costs $3499 (plus tax), while the Meta Quest 3s starts at $299 (Meta, n.d.; Apple, n.d.-a).[29] When optimizing for the high-end or mass market, companies are forced to make decisions about their hardware that will affect the device's functionality and thus the consumer experience. For example, the Apple Vision Pro has a resolution of 11.7MP per eye, one of the highest on the market, which reviewers acknowledge contributes to a superior user experience (Patel 2024), but at over ten times the cost of other devices.[30]

This also may affect what accessibility measures companies invest in. Hardware companies ship their devices with an operating system (OS). While platform organizations control the level of accessibility in their products, hardware companies implement accessibility functions for their devices to compensate for the affordances imbued on devices that may not be universally usable. Because IXR devices vary in form and function more than smartphones, tablets, and laptop or desktop computers, there are no standard accessibility technologies and limited guidance (Creed et al. 2024a), so devices and OSs vary widely in their level of accessibility, which in turn limits who can use these devices. The Meta Quest Accessibility page lists 12 features that users can adjust (Meta 2025),[31] while the Apple Vision Pro offers 26 accessibility settings across vision, physical and motor, hearing, and speech areas (Apple 2025a). Beyond IXR, Apple has made accessibility part of its larger corporate strategy, and its devices are considered some of the best amongst disabled communities, especially people with vision impairments (Wisconsin Council of the Blind & Visually Impaired 2021; Raz Mobility 2024; Aquino 2016). The Vision

---

[29] Prices as of July 2025. Meta does have more advanced headsets; the Quest 3s was chosen as a low-priced example to contrast with the Vision Pro.

[30] Hardware pricing interacts with a company's broader business model when those companies are also software or platform companies. For example, a company that generates more profit from hardware—which may be at a higher or lower price point depending on manufacturing costs—will have to generate less revenue from software, advertising, and other sources. This impacts how companies will collect and leverage user data.

[31] As of July 2025; this is an increase from nine features in September 2024.

Pro has also been acknowledged as a highly accessible general-purpose computing device (Leland 2024). In setting their business models and priorities, hardware companies seem to make trade-offs between disability and price accessibility, which control not only how their devices are used, but whether they can be used at all by specific people. Thus, access to IXR devices and accessibility infrastructure is mediated by business strategies (and capitalism), impacting who can access it and how. In setting these priorities, hardware companies thus control not only how their devices are used, but whether they can be used at all by specific people. This constitutes a form of accessibility mediation, where business models embed exclusion into the infrastructure—not as a technical limitation, but as a byproduct of market-driven design.

Hardware companies also decide what level of access to sensors and hardware they will grant developers and platform organizations. Both Apple and Meta initially restricted developer access to camera feeds for privacy reasons, before later opening them to various degrees (Heaney 2024b; 2024a). Meta has also opened its operating system to third-party devices, meaning that other hardware companies can use Meta Horizon OS instead of developing their own OSs (Malik and Paul 2024). By opening this piece of IXR infrastructure to more device manufacturers, Meta could be establishing itself as an XR infrastructure provider, which could open the door to more consumer devices and IXR experiences. However, it also creates the possibility of lock-in for both OSs and accessibility measures.

In setting their business models and priorities, hardware companies control not only how their devices are used, but whether they can be used at all by specific people. Thus, access to IXR devices and accessibility infrastructure is mediated by business strategies (and capitalism), impacting who can access it and how. In setting their business models and priorities, hardware companies control not only how their devices are used, but whether they can be used at all by specific people. This constitutes a form of accessibility mediation, where business models embed exclusion into the infrastructure—not as a technical limitation, but as a byproduct of market-driven design.

Hardware companies also make decisions about system input mechanisms and feedback systems. However, because these relate to the direct physical and sensory experiences of the user, I will discuss them in the next section, which focuses on devices.

3.3.3. Internal Organizational Features & People

Internal organizational hierarchies shape the mediating power of hardware companies, structuring whose concerns reach decision-making levels and whose do not. Experience-mediating decisions are guided by larger corporate strategies, including, as discussed, price points and what type of XR to prioritize. Like platform companies, internal structures impact how decision-making power is distributed and whose concerns and priorities are heard. Hardware companies are generally centralized, meaning that the company itself and its internal leadership are the primary decisionmakers; the decentralized governance structures adopted by some platforms do not function as well when a product has to be built, marketed, and sold. This concentration of design authority means that the experiential norms of XR are shaped not through deliberation, but through internal corporate imaginaries—rendering mediated reality contingent on the strategic visions of a few firms.

3.4. Devices

The IXR devices created by hardware companies are a key part of XR infrastructure. Without devices, there is no IXR, meaning that those devices are fundamental mediators of that reality. The decisions made by hardware companies influence how they mediate the user's sensory experiences, which impacts how users interact with both extended and physical reality. In other words, devices do not merely display reality—they construct and constrain it, hardware company priorities into the users' embodied sensory experiences. These sensory impacts will be the focus of this section.

3.4.1. Hardware and software

IXR devices have multiple constituent parts, all of which mediate the user's sensory experiences in different ways. The most readily apparent is the display. For VR devices, this is typically a screen; for AR devices, this is a transparent lens. AR devices are thus considered "see-through." VR devices can simulate the transparency of AR devices when used in "passthrough" mode, but are displaying a video projection of the surrounding world. These mediate how and where the devices can be used. For instance, a pair of AR glasses are easier to use out in the world because they are see-through devices that blend into the user's self-presentation more than a VR headset.

In terms of one's sensory experiences, on a baseline level, AR devices mediate like glasses do; they are a transparent lens, perhaps vision-correcting, between one's eyes and their surrounding environment. While this is a form of technological mediation, I will focus on the novel aspects of mediation, i.e., the digital elements. These are what create unique affordances compared to non-XR technologies, and as an egocentric technology, these affordances impact user experiences (Grauman et al. 2022). The primary significance of this is that AR devices add information to the user's visual field. The quality of the actual overlays depends partially on the display. For instance, the Microsoft HoloLens display is fixed at a focal distance of 2.0 meters (Microsoft 2021). Thus, when objects are represented at a distance closer or farther from the user, it can cause eye strain and discomfort through the vergence-accommodation conflict, a conflict between how the eyes focus and how they rotate to view an object clearly (Microsoft 2021). More research is recommended on possible permanent effects, especially in children (ANSES 2014).

The mediating effect of devices is even more apparent with VR, where everything the user perceives is shown as, essentially, a video on a screen. This creates pernicious visual impacts; field of vision and color range are restricted (Patel 2024), changing how the physical world is perceived on a fundamental level and reducing the quantity of information that can be perceived—or contained in—an extended reality compared to physical reality. While the user may not be aware of the comparatively limited range of vision or that they are seeing fewer colors than normal, at least until they remove the headset, it still impacts what they are able to perceive. These perceptual constraints illustrate a form of sensory filtration, where the device determines which aspects of the physical world are visible or rendered and which are distorted or omitted. Furthermore, in divorcing vision from other senses, IXR may create more subtle sensory impairments. A study of rats found that spatial navigation in VR was impaired due to the "elimination of spatially informative multisensory, nonspecific cues and minimization of vestibular cues" (Aghajan et al. 2015), indicating that IXR does not just affect vision or even just the five "primary" senses—it also implicates proprioception and other sensory systems in a different way than physical reality does.

The final kind of technological mediation IXR devices do is via algorithms, which convey the *reality* of XR to the user. These range from the algorithms that stitch together video feeds into a coherent visual to the AI assistants that some devices integrate and thus can be either highly transparent or more clearly present as a mediator. AI assistants, often voice-activated, affect a user's experience based on how good they are, but also based on how well they are able to respond to a user's queries. For instance, voice assistants have been shown to understand some accents less well than others (Harwell 2018). Functionality varies across languages, and the majority of the world's 7,000 languages are not served by the most popular voice assistants (Kann 2022). Furthermore, not all models are available in all countries due to strategic decisions or regulatory factors (Fried 2024). These algorithmic mediations affect more than functionality; they determine whose queries are intelligible and whose languages are systemically excluded—extending platform asymmetries into everyday interaction.

IXR devices also mediate one's self-presentation in the physical world, where an IXR device becomes part of an individual's self-presentation. Some devices are more contextually transparent than others, meaning that they are less conspicuous in use (Verbeek 2012; Van Den Eede 2011). AR glasses such as the Meta Ray-Ban blend in like normal glasses, while the Apple Vision Pro's "EyeSight" feature, which projects the user's eyes onto the front of the device when another person tries to interact with them, has been criticized as overtly uncanny (Patel 2024). However, mediating devices can become more contextually transparent over time; Apple's AirPods were initially mocked for looking strange, but eventually became a status symbol (Tinari 2023). IXR devices may cause an off-putting self-presentation at first, but could change social perceptions as they become prevalent.

Overall, IXR devices are a key piece of infrastructure that are fundamental to accessing IXR, but they also mediate the user's sensory experiences. However, depending on the decisions made by the hardware company, they may not function the same for everyone, meaning that the infrastructure is not experienced the same way by all. Through their displays, sensors, and integrated systems, IXR devices act as gatekeepers of perceptual fidelity and social legibility, reinforcing biases in who can access, express, or be recognized in mediated environments.

3.4.2. HCI

Human-computer interfaces on devices include input mechanisms (which bridge user actions to affect IXR) and feedback systems (which provide output from XR to the user). IXR device input mechanisms include physical buttons on the device itself (like the Viture Pro's buttons or Apple Vision Pro's Digital Crown (Apple, n.d.-b; Viture, n.d.)), touchpads on the device (like the now-defunct Google Glass (Google, n.d.)), handheld controllers (like the Meta Quest and Pico ranges (Meta, n.d.; Pico, n.d.)), hand tracking, and eye tracking (of which the Apple Vision Pro uses both (Apple 2025b; 2024)). Some also support voice commands.[32] These create different affordances that shape how users interact with extended reality and mediate their experience in a variety of ways. For one, they affect the level of realism. We do not control physical reality with handheld controllers, which makes hand tracking more intuitive (Kapsoritakis 2022). They also affect the level of accessibility, as handheld controllers require a level of dexterity, while hand tracking requires the user to be able to perform specific motions and the sensors to be able to recognize their appendage as a hand, which means that someone missing fingers or a hand, or with a differently shaped hand, may be unable to use it. Eye tracking also requires vision to navigate with, and often the ability to move both eyes together, which not everyone possesses. Thus, the affordances

[32] See, for example, the Apple Vision Pro (Apple, n.d.-c).

of the devices (established by the hardware companies) affect how well the devices function for people, creating situations where the infrastructure of IXR functions less well for some people when accessibility measures are inadequate. Following Hutchby's sociotechnical interpretation of affordances (Hutchby 2001), XR devices do not simply enable interaction—they frame and constrain possible interactions, thus becoming integral to the power asymmetries encoded at the design layer by hardware companies. When hardware affordances presume normative bodies—e.g., full manual dexterity, stereoscopic vision, normative speech patterns—they render others less visible, less capable, or altogether excluded from meaningful interaction.

Feedback systems are a crucial component of how IXR devices mediate user experiences, creating a bridge between user actions and virtual responses. Unlike traditional computing interfaces where feedback is primarily visual, IXR devices employ multiple sensory channels to create a more embodied interaction model. Haptic feedback through controllers or wearables provides tactile sensations that simulate physical interactions, while spatial audio cues help users locate virtual objects and events within their extended reality environment. This multi-modal feedback infrastructure is essential for creating what Steuer (1992) calls "telepresence"—the sense of being present in a simulated, or mediated, environment—through increased sensory information.

With the exception of handheld controllers, which provide haptic feedback, IXR haptic devices have yet to reach the consumer mainstream (Wang et al. 2019). Wearable haptic gloves and suits exist, although have yet to be widely commercialized (Fleck et al. 2025), and can create greater sensory fidelity. These feedback systems highlight how IXR devices must compensate for the sensory experiences they mediate away. When a user reaches for a virtual object, they lose the natural tactile feedback they would experience in physical reality. The device must artificially reconstruct these sensory cues through haptic feedback.[33] However, haptic devices, like higher-end headsets, can be out of the price range of most consumers. The infrastructure of feedback thus becomes another point where hardware decisions

[33] Other sensory enhancement devices, like smell generators, exist (see the Olorama), but have yet to reach consumer viability; many of the same arguments about accessibility and mediation apply to these as well.

materially affect the quality of user experience, contributing to the tiered nature of XR. This demonstrates how IXR devices are not merely adding to reality but fundamentally mediating users' sensory experiences through their infrastructure. Human-computer interfaces are thus a site of embodied mediation, where physical access is differentially distributed—reflecting the priorities of designers over the needs of diverse users.

3.4.3. Content

IXR devices also affect how users experience IXR content. One key factor in sensory perception is screen resolution. With 20/20 vision, the human eye has a resolution of approximately 1 arcmin—hence Apple's boasts that its "Retina Display" pixels are imperceptible to the human eye (Plait 2010). When the screen is not just a phone screen or computer monitor, but your entire surroundings, lower resolution becomes apparent and impacts not just one's sensory perception of the world, but also their perception of its realism. However, as mentioned above, this tends to be price-correlated: the $3,499 Apple Vision Pro has a screen resolution of 3,386 pixels per inch (PPI), nearly three times as many as the $499 Meta Quest 3 (Sorrel 2024).[34]

A factor related to resolution but mostly dependent on the speed of one's data connection is latency. More latency means that the user is more aware that their experience is being mediated, and thus the device is less metaphorically transparent. Latency is less likely with high-speed broadband, but such plans can be costly and not available in areas without adequate Internet infrastructure.[35] The same applies with the quality of cameras and sensors (Adhanom et al. 2023), which feed into not only VR device displays but also frequently its input mechanisms. If, for example, an IXR device is controlled via hand gestures, like the Apple Vision Pro, then lag in sensing a user's gestures interferes with their ability to

[34] However, other factors such as resolving power (a result of lens and display interaction) can compensate for a lower resolution screen in some cases (Lang 2024).
[35] In at least 15 countries, the cheapest Internet plan exceeds 10% of the gross national income per capita, and 400 million people worldwide are not covered by the infrastructure required for Internet access (Kemp 2024). XR requires high-speed broadband or mobile data (Alriksson et al. 2021), which further limits the population that can access it.

interact with their virtual environment, again creating a metric for experiential quality linked to device price. Because the device mediates not just content but the realism and fluidity of experience, disparities in resolution and responsiveness effectively stratify XR participation by device quality and broadband access, enacting a form of experiential hierarchy where the richness and believability of XR is contingent on hardware power and connectivity privilege.

3.5. Users

Within the confines of the decisions that platform organizations and hardware companies have made, and the characteristics of their devices, users can then make decisions about their experiences and how they access and use IXR. Users appear to have autonomy in navigating IXR, but their actions are deeply contingent on infrastructural decisions made upstream by platform and hardware providers. These infrastructures shape what is accessible and possible within the IXR environment. In this sense, user "choice" in IXR is often better understood as constrained agency, exercised within the affordances, exclusions, and power relations embedded in technical design and institutional priorities.

3.5.1. Hardware & Software

The primary decision users can make center around what hardware and software they elect to use. However, these choices are still fundamentally constrained. Users can theoretically choose from any headset on the market, but as discussed above, can practically only choose those that are financially accessible to them. Even if a specific headset would suit them better due to its features or accessibility measures, if that headset is outside of their budget, they cannot access it and their preferred version of extended reality, showing its mediated nature. Their extended reality becomes one of necessity, not preference, bounded by market pricing and infrastructural lock-in. Additionally, while users can choose what experiences they access on IXR devices—within the same boundaries of cost—they often cannot choose what headset software they use. Devices are generally locked to specific operating systems (one cannot run Android on an iPhone, for example[36]) and while some devices allow "side-loading" of apps that are not from official app stores, most users are limited to apps that are available through conventional downloads.[37] These limitations reveal a core tension: although users are the experiential endpoints of XR systems, they rarely control the technical or policy layers that mediate those experiences.

3.5.2. Content

Content is another area users have some amount of control over, specifically around user-generated content. Using the tools provided by platform organizations, they can create content ranging from AR filters to immersive VR worlds. However, this content is created and filtered within the confines of the content guidelines and toolkits provided by the platform and affected by the affordances of the device used to create it. Similarly, while IXR offers users a wide variety of experiences, if an experience has not been programmed in, if it exceeds the computational ability of a device, or if there are inadequate accessibility measures, the technological nature of IXR infrastructure makes itself apparent through obstacles not present in the physical world. Additionally, the way users access experiences and the quality of those experiences depend on measures like content moderation and user education that help users know what to expect from a given experience and then have a safe experience. While users may be framed as empowered creators, the rules, tools, and invisible protocols embedded in IXR infrastructure shape not only what can be built—but whose content is seen, valued, and preserved.

3.5.3. Workflow & Communication

As IXR devices are increasingly marketed for work, users can integrate them into their workflows in various ways, leveraging the different affordances of the devices (defined by the platform and hardware

---

[36] "Project Sandcastle" could install a version of Android on jailbroken iPhone 7s and earlier, but it is no longer actively maintained (SimplyMac 2024). Emulators exist (Sandu 2024), but they run in virtual machines, not on the iPhone directly. These solutions require considerable technical expertise and can compromise the security of the device.

[37] There is an alternative app store for Meta Quest devices, Sidequest VR ("SideQuest," n.d.), but using it also voids the device's warranty.

companies). IXR was adopted early in enterprise applications, especially warehouse environments and training (Howell 2024; Metz 2017). Now, devices are also aiming at white-collar productivity applications, with marketing for the Meta Quest Pro and Apple Vision Pro emphasizing their productivity potential for things like word processing and video editing (Meta Quest 2024; Apple 2023). With the launch of the Apple Vision Pro, Apple is emphasizing "spatial computing" as the next form of general-purpose computing (DeVon 2024). However, these devices are aimed at a different audience than enterprise IXR devices. White-collar workers have more choice in whether and how they integrate IXR devices into their workflow; blue-collar workers may face usage mandates for things like workplace training and other job functions. Thus, while some workers will have choice in how they incorporate IXR infrastructure into their jobs, for others, it will become a new default. Workers with employee-mandated device usage will likely be subject to increased employer monitoring, just as many employees with employer-issued laptops are (Tong 2023). This divide reflects how IXR infrastructure can become a vector for digital labor stratification, deepening existing inequalities in autonomy, privacy, and surveillance.

Because of the sensitive nature of IXR data, this surveillance could be particularly impactful; theoretically, eye-tracking data could be used to make judgements about employee attentiveness despite the flaws of using eye motion as a proxy for attention (Liddicoat 2022); eye tracking data can also be used to infer information about a user's physical characteristics, personality traits, sexual identity, and health conditions, among other things (Kröger et al. 2020). Indeed, the EU AI Act[38] bans the use of AI systems to infer emotions in places of work and education (Art. 5). While workers may have some latitude to use IXR in different ways, it is likely to become part of employer surveillance infrastructure in different ways depending on the nature of an individual's job, likely stratified by income and geographic bounds.

[38] (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) 2024)

3.6. Discussion

This chapter has demonstrated that XR is not only a mediated reality, but one whose forms of mediation are infrastructurally layered and power-laden. To understand how power operates in this reality, we can apply Floridi's (2023) typology of poietic (world-making), metamorphic (world-transforming), and cybernetic (world-steering) power. Poietic power resides primarily with platform and hardware companies who decide what is technically possible and economically viable—what kinds of extended realities can even be instantiated. Users may exercise creative agency within these boundaries, but always through tools and systems not of their making. Metamorphic power is likewise asymmetrically distributed: while users can adapt to XR, platforms can reshape it at will—altering design, moderation, access, and APIs through opaque, often commercially driven decisions. Cybernetic power, in turn, is expressed through steering behaviors like market prioritization (e.g., Meta's AR turn), standard-setting, and interface redesigns that guide both industry direction and user behavior. In short, power over XR is infrastructural, expressed not in overt commands but in the invisible defaults, inclusions, and exclusions encoded into the medium itself.

Due to their limited poietic and cybernetic control, users are at the bottom of a cascading pyramid of power. While XR platforms offer the promise of new realities, in practice, access to those realities is tiered by infrastructure. Wealth, geography, physical ability, and corporate priorities all condition one's perceptual and participatory position. Whether a given user can access IXR may be predicated on a business decision about device price or accessibility measures. In physical reality, one cannot pay to have more or better senses than others,[39] nor is their ability to experience physical reality predicated on the purchase of a physical item. The same is not the case with XR. Many of the factors that mediate one's ability to interact with and experience the virtual world echo—but should not, of course, be construed as exactly equivalent to—the concept of disability in the physical world. Under the social model of disability, a disability is the result of an individual impairment interacting with a social environment

[39] A possible exception is paying for corrective medical procedures such as cataract surgery or cochlear implants. However, while these elevate one's experience of a specific sense above their pre-procedure baseline—and that of those who cannot access those procedures—it does not augment them compared to the general population like IXR devices can.

unaccommodating to differences in physical and mental traits (Shakespeare 2016). For example, someone who uses a wheelchair due to a physical *impairment* is able to enter a building if the building has a ramp, but if it only has stairs, their ability to enter that building is quite literally *disabled;* note that this is an issue with the infrastructure of the physical world. When it comes to IXR, barriers to usability through hardware quality create a form of disability baked into IXR infrastructure from the start; the reality itself is driven by affordances, not just specific experiences in it. Individuals who can pay more will have a better experience—a better reality—because of their superior hardware.[40] Device mediation thus creates a fundamental level of inequality: those with the money to purchase higher-quality devices and higher-speed broadband will have superior experiences; those who cannot will have worse experiences. Furthermore, while in physical reality lack of accessibility can be overcome via a variety of actors and through a variety of mechanisms (such as through accessibility laws, petitioning, and public advocacy) in extended reality, lack of accessibility can be locked in if the hardware or software provider does not prioritize it. As a result, it is highly likely that an extended reality will be a fundamentally unequal one, with tiered experience quality that embeds a discriminatory digital divide in the infrastructure of reality itself. The XR infrastructure thus encodes a form of digital stratification: reality itself becomes a premium product, mediated differently for different people.

If poietic and cybernetic power remain concentrated in corporate hands, the external rules and regulation aspect of infrastructure represents one of the few levers for redistributing control. In physical reality, infrastructure is governed by public standards—safety codes, accessibility laws, building permits. In XR, the lack of enforceable standards and the dominance of proprietary control allow platform governance to substitute for public governance. This blurs the boundary between infrastructure provider and rights adjudicator, giving companies significant power over fundamental rights, embodiment, and access with limited oversight. To mitigate these imbalances and grant more powers to users in the

---

[40] This was foreseen in Neal Stephenson's 1992 novel *Snow Crash*, often (but erroneously) credited with coining the term "metaverse" (Hine 2024b), where public terminals allow for anyone to access a virtual world for free, but users accessing the metaverse through public terminals appear as grainy, black-and-white avatars and are stigmatized as a result (Stephenson 2003).

hierarchy, it is vital to develop public, rights-based standards for XR infrastructure—standards that treat XR not merely as entertainment, but as a constitutive environment where rights and identities are explored and shaped.

XR is not just a new interface or product class—it is a reality-rendering infrastructure, one whose architectures of mediation shape cognition, agency, and community. As this paper has shown, how mediation is built determines whose experiences are enriched, whose identities are supported, and whose participation is foreclosed. To govern extended reality justly, we must move beyond whether it is mediated and toward shaping the terms and consequences of that mediation.

3.7. Conclusion

The infrastructure of physical reality—roads, buildings, utilities, public spaces—has historically been regulated and maintained, however imperfectly, by the state in service of the public good. XR represents a profound departure from this model: its foundational infrastructure is developed, deployed, and governed almost entirely by private corporations. This shift is not just a matter of who owns the tools of access, but of who shapes the contours of reality itself, and is particularly consequential because IXR infrastructure is not merely regulative of existing behaviors and experiences, but constitutive of the reality itself. In a way, IXR platform companies possess more power over their platforms than governments do over their countries; platform companies can shape the structure and physics of reality itself.

The corporate control of IXR's mediating infrastructure creates a fundamentally different power dynamic than that of physical reality. While companies have long influenced many aspects of human experience under capitalism, they have never before had such direct control over the infrastructure of reality itself. The mediating capacities of IXR—what can be sensed, expressed, or navigated—are no longer open environments but privatized pipelines, governed by commercial priorities, engineering choices, and proprietary standards.

This corporatization of reality infrastructure raises profound concerns about equality and access. The quality of one's extended reality experience—from visual fidelity to interaction capabilities to accessibility features—becomes directly tied to purchasing power in ways that transcend typical digital divides. Unlike physical reality, where sensory experiences are fundamentally equal and accessibility challenges can be addressed through various social and legal mechanisms, XR risks embedding inequality into the fabric of reality itself through tiered hardware capabilities and corporate priorities. When these infrastructures are designed without transparency, accessibility, or public accountability, they risk producing a tiered reality—one in which a user's capacity to participate meaningfully is determined by purchasing power or bodily conformity to normative standards. Some users may encounter immersive environments that feel seamless, safe, and expressive; others may confront glitchy rendering, unrepresentative avatars, or wholesale exclusion from social spaces. These are not superficial differences. In a mediated world, unequal access is inequitable experience.

Such stratification poses a challenge not only to usability, but to justice. As IXR becomes increasingly embedded in education, employment, and social life, the distribution of experiential access will help define who is visible and who is allowed to benefit. In this light, IXR must be understood not as a neutral technological frontier, but as a contested political space.

This is not intended to be an anti-corporate screed. Indeed, while governments have and continue to invest in IXR research and development, much of modern IXR would not be possible without the private sector. Rather, this chapter is a philosophical inquiry into what it means to construct a mediated reality and a call to interrogate its consequences. If XR becomes a central arena of human life, then the question is not just what we can build, but for whom it is built—and who is left out. Society must consider whether this privatized model of reality infrastructure serves the public interest as IXR technology continues to integrate into everyday life. The unique affordances and opportunities of extended reality are remarkable, but in creating a fundamentally mediated reality controlled by corporate interests, we may be inadvertently constructing a fundamentally unequal reality.

Governance efforts must move beyond technical risk mitigation and embrace infrastructural ethics, making commitments to designing and regulating IXR systems that safeguard dignity, inclusion, and epistemic fairness. If mediation is now the mechanism by which reality is constituted, then the governance of mediation is the governance of the real. A just mediated future will require not only innovation, but interrogation—of whose realities are being built, and at what cost, to ensure that extended reality develops in ways that promote rather than undermine equality, accessibility, and human flourishing.

Chapter 4: Virtual Reality, Cyberspace, and Embodiment: A Historical Debate with Contemporary Resonance

4.1. Introduction

Even before the Internet, cyberspace existed. It was formed of text-based networks that laid the groundwork for modern Internet communication, which is becoming more embodied through graphical representations of the self online and, increasingly, in virtual reality (VR). This chapter discusses the evolution of digital embodiment—from the early days of cyberspace and VR, as they developed contemporaneously but separately, to today—and the narratives being promoted about it, which often differed. In the physical world, our bodies impact our experiences as we are judged along lines of gender, race, disability, and other facets of our identities. While the form and extent of embodiment in cyberspace and VR have changed, what has not changed is that virtual embodiment also creates different experiences for different people, often along the same lines as in the physical world.

VR is thought of as a very recent technology, partly because of its associations with more recent AR and MR technologies, but its origins lay in the 1960s with Morton Heilig's multi-sensory simulator called the "Sensorama" and Ivan Sutherland's head-mounted display, the "Sword of Damocles" (Mazuryk and Gervautz 1999). The first commercially available VR devices were launched by VPL Research in the 1980s, when home computers were still relatively rare and before the Internet was widely available to the public (Lanier 2017). Thus, theories about the two were evolving in tandem but separately as people reckoned with how their identities offline translated online. In the 2010s, when the Internet had evolved to include social media, technological advances made "social VR" more widely accessible, merging the debates. As we live more and more of our lives online, our on- and offline lives merge into an "onlife" (Floridi 2015), and our experiences in virtual spaces significantly influence our well-being.

This chapter analyzes historical perceptions of virtual embodiment,[41] examining its implications for our experiences online and in extended reality (XR).[42] Ideas of virtual embodiment have evolved from a Cartesian dualist perspective where a user's cyberspace embodiment was seen as independent from physical characteristics, to acknowledging that physical characteristics could be embodied in cyberspace, to insisting that they should be celebrated. Throughout this development, this chapter will argue that narratives promoted by the proponents of emerging technology—mainly able-bodied white men—have overlooked the experiences of marginalized communities, who are often embodied in cyberspace in ways that create disparate experiences. By analyzing the origins of cyberspace, consumer VR, and the embodiment debate, this chapter underscores the importance of recognizing how our bodies impact our experiences in virtual environments and the need for vigilance so that harms to marginalized communities are not overlooked by those controlling the narratives of emerging technologies.

"Cyberspace" has adopted different definitions over the years, including one that is synonymous with VR. I use the term "cyberspace" to refer to virtual connected spaces where people can communicate, and explain other definitions when necessary. Cyberspace emerged prior to the creation of the World Wide Web in the United States (US), where text-based bulletin board systems (BBSs) that people used to post messages and engage in discussion were invented. While BBSs eventually spread to other countries, including England, Indonesia, Sweden (Driscoll 2022, 65), China (Woon 2011), Finland (Saarikoski 2020), and Turkey (Furman 2015)—and in some cases persisted beyond the decline of BBSs in the US—the use of dial-up systems to undergird BBSs created financial and logistical difficulties to connect international BBSs to the vibrant US BBS ecosystem (Driscoll 2022, 72), where there were over 100,000 active BBSs (Driscoll 2020); there were comparatively fewer internationally (Driscoll 2022, 72). Similarly, while VR development did eventually emerge outside the US, early VR companies were primarily based in the US. The Internet also originated in the US, and Americans made up more than half of Internet users through

[41] I use "embodiment" not just to refer to a visual representation of the body, but in the Oxford English Dictionary sense of "giv[ing] a concrete form to" something (*OED Online*, "embody | imbody, v.").

[42] In the 1980s, VR—as the use of mediating wearable technology to interface with virtual worlds—was the primary focus of consumer development, and the terminology in this chapter used reflects that (i.e., I do not use "IXR" because it was not a relevant term then). While there were professional and industrial applications of VR, this chapter focuses on consumer applications of VR because those were the ones that primarily impacted individuals and shaped cultural narratives.

the 1990s (Elon University 2020). Thus, this article is inevitably US-centric in its reconstruction of the origin of cyberspace, VR, and the embodiment debate, but its insights can be extrapolated to the more international Internet of today.[43]

Before beginning my analysis, two philosophical concepts must be clarified: those of Cartesian dualism and experience. "Cartesian dualism" is often used as a shorthand for the idea attributed to René Descartes that the mind and body are part of two separate worlds, with the body seen as a "mere unconscious or insentient machine, effectively a complicated bit of clockwork," while the mind is the site of consciousness (Baker et al. 1995, 7). The mind is made of an immaterial substance and is yoked to a material body, but can exist separately as a soul (Blum 2019); the two interact when sense-perceptions cause mental effects or mental states lead to physical effects (Baker et al. 1995, 7). However, whether Descartes was a Cartesian dualist as popularly conceptualized is questionable (Baker et al. 1995). Because the literature has adopted "Cartesian dualism" as a label for the kind of mind-body separation discussed in relation to cyberspace, I will as well, while acknowledging the complexity of the discussion. Though I distance myself from this debate, by acknowledging it I hopefully can be absolved of any philosophical crimes committed by perpetuating the "Cartesian Legend" (Baker et al. 1995, 1).

This chapter's embodied concept of experience is drawn from phenomenology, following a long line of phenomenologists including Husserl, Heidegger, and Merleau-Ponty who argued that experiences are formed by interactions of the body, mind, and surrounding environment. Husserl saw sensory perception through the "lived body" as crucial to forming experiences (Landgrebe 1973; Carman 1999). Heidegger's idea of the body as the Dasein, or "being-in-the-world," connects the body and mind to sensory experiences; we first hear not a "pure noise," but "the creaking wagon, the motor-cycle" (Heidegger 1996, 153). That is, our sensory perceptions and how our body interfaces with the environment are shaped and interpreted by the mind to form our experience of the world. Both Husserl

[43] Although English is still disproportionately represented in Internet content, the diversity of languages used online has increased since the origins of the Internet (Richter 2024).

and Heidegger emphasize the relational nature of the body, which is embedded in the surrounding world—its interfacing with the environment is what forms our experiences.

Merleau-Ponty further developed this, elaborating on the idea of the "body schema," a proprioceptive and pre-reflective model of our body's abilities, limitations, and position. It is often confused with the "body image," which includes the conscious perception of the body, the conceptual construct of the body, and emotional attitudes and feelings towards the body (Gallagher 1986). Thus, while the body schema is "a non-conscious performance of the body," the body image incorporates "perceptual, cognitive, and emotional" aspects (Gallagher 1986). These concepts are co-constitutive with experiences; the body schema impacts how one interacts physically with the world, and the feedback from the surrounding environment changes the body schema. The body image can also be impacted by experiences that change someone's idea of what their body can do, which may include an emotional component. Self-presentation is a third important concept, covering the way someone shapes aspects of themselves that others can perceive—including "appearance, mannerisms, and opinions"—to convey a desired self-presentation (Schlenker 2003; Goffman 1956). Online, self-presentation becomes more malleable as individuals can construct multiple identities within the confines of the digital media they use (Jensen Schau and Gilly 2003). "Impression management" of one's self-presentation (Goffman 1956) traditionally relies on "corporeal display" (Jensen Schau and Gilly 2003), but in the digital setting, there are different forms of display for different aims. Any theory of embodied experience online must account for these three aspects, which all combine to impact our experiences.

This chapter's analysis will proceed chronologically, covering cyberspace and embodiment through three distinct eras. Sections 4.2 through 4.4 each address one of these eras; Section 4.5 concludes.

4.2. Early Years: Text, Disembodiment, and Textual Disembodiment

Cyberspace and virtual reality (VR) were developed in parallel and before widespread accessibility to the Internet, and certainly before the creation of social media. Early discourse around cyberspace portrayed it as a place where people were fully disembodied and liberated from the bonds of their physical bodies, but this vision was not supported in reality. This Cartesian discourse was promoted by early adopters who, in many cases, were also building this new technology, and it accorded with technological constraints that limited interactions to text. In contrast to early proponents, many users showed that they wanted aspects of their physical identities to be relevant online, foreshadowing future evolution in this direction. VR discourse also included a thread of disembodied escapism, but its earliest advocates saw it as a way to connect people where the transcendence of the body was a necessary step rather than the primary purpose, and then appreciate the physical world more on return. I will first discuss cyberspace, followed by VR.

4.2.1. Cyberspace

The first iteration of cyberspace, emerging in the 1980s,[44] was text-based and characterized by bulletin board systems (BBSs), multi-user domains (MUDs), and, later, MOOs ("MUD, object-oriented") where people exchanged information, chatted, and role-played. Both BBSs and MUDs originated in the US in the late 1970s but were popularized in the 1980s (Edwards 2016; Turkle 1994). LambdaMOO, the first MOO, was launched in 1991 (Rheingold 1994). Although they were most popular before the Web was invented and the Internet made public, their use continued even as the Internet spread.

At the time, the term "cyberspace" was still developing. William Gibson is often credited with coining the word, using it to refer to a 3D immersive dataspace in his 1982 short story *Burning Chrome* and its 1984 sequel *Neuromancer* (Gibson 1986; 2000), but it was in fact first used by Danish artist Susanne Ussing and architect Carsten Hoff in the 1960s as they produced cybernetic-inspired works under the name "Atelier Cyberspace" (Lillemose and Kryger 2015). Under my definition, though, cyberspace was a text-based medium at the time. It was heralded by early adopters as a place where the mind and body could be totally separate in a version of Cartesian dualism and was portrayed as a world of "total

[44] BBSs and MUDs originated in the US in the late 1970s but were popularized in the 1980s (Edwards 2016; Turkle 1994). LambdaMOO, the first MOO, was launched in 1991 (Rheingold 1994).

representation" (Heim 1993, 100) where "minds are connected to minds, existing in perfect concord without the limitations or necessities of the physical body" (Gunkel and Gunkel 1997).[45] This Cartesian split was promoted by culture-shapers like Stewart Brand and Larry Brilliant, founders of the Whole Earth 'Lectronic Link (WELL) BBS that was, while small in terms of userbase, enormously influential on early cyberculture (Turner 2010, 142). Early members included noted cyber-libertarian John Perry Barlow and many other prominent cyber-utopian writers who "conjured up visions of a disembodied, peer-to-peer utopia" (Turner 2010, 272). Many of its founders had links to counterculture and communal movements; an associate of Brand recalled that the WELL took the "tribal need" inspiring communes and put it in the form of a "disembodied tribe" (Turner 2010, 157); it was hoped this was "the route to new forms of equality and communion" (Turner 2010, 27).

These views were reflected not only by culture leaders but also by early adopters of cyberspace. Cyberspace was initially occupied primarily by tech-savvy, young, single white men (Driscoll 2022, 21–23). This gave them significant influence on the culture that lasted for years.[46] Many of these early adopters were self-styled "hackers"[47] who developed their own culture, laid out in the "Jargon File." An appendix entry on "Gender and Ethnicity" acknowledged the gender and racial composition of "hackerdom" and its general belief in textual disembodiment:

> Hackerdom is still predominantly male… In the U.S., hackerdom is predominantly Caucasian… Racial and ethnic prejudice is notably uncommon and tends to be met with freezing contempt. When asked, hackers often ascribe their culture's gender- and color-blindness to a positive effect of text-only network channels, and this is doubtless a powerful influence (The Jargon File, n.d.-b).

---

[45] This quote is often misattributed to Heim (1993, 34).

[46] By the early 1990s, about 1/5 of American households had a computer, but Black American households were half as likely as white households to have one (Driscoll 2022, 21–23)

[47] "Hackers" were those who explored systems and "how to stretch their limits"; the term did not carry the connotations of illicit data access. Individuals who did that were "crackers" (The Jargon File, n.d.-c; The Jargon File, n.d.-a).

The "hackers" were the pioneers of cyberspace and had a significant role in shaping its culture and surrounding narrative. Their views were shared by some contemporaneous observers, including critical race, disability, and feminist scholars who saw cyberspace as a revolutionary way to break down societal inequalities (Rudnicki 2017), for if people were judged only on their minds, discrimination based on bodies would have to cease.

To some extent, some early cyberspace participants did feel disembodied, or at least anonymous. For instance, a MUD participant stated to a researcher that "In RL [real life], if I'm black, or handicapped, or don't have a college degree (or even a highschool [sic] degree), that will affect how I'm treated. That matters for nothing here, really" (Kendall 1998). However, other accounts and studies showed that racist, classist, and ablest harassment (and thus embodiment) did exist in cyberspace—even if we take at face value that "hackerdom" was egalitarian, cyberspace as a whole was not. One could try to maintain anonymity and have these factors not matter, but anonymity also emboldened those who were inclined to harass other people online (Lea and Spears 1991). Harassment, especially sexual harassment, became so prevalent that women joining BBSs and MUDs were warned about "netrape" where female personae were textually violated (Cherny 1994), showing that the narrative of academics and early adopters did not apply to those who did not share the dominant and "default" identities of whiteness and maleness of the majority of early cyberspace adopters (Driscoll 2022, 22–23) and did not, or could not, maintain anonymity. Those who were not members of the "default" group had to be vigilant to avoid harassment and thus were not leaving their physical bodies behind.

Identity could be communicated directly when users chose to disclose it, or indirectly. Physical identity could be inferred through typed speech, whether through words and vernacular or the way one interprets experiences, with men's and women's online communication styles differing enough to be considered "different cultures" (Herring 1996). This is more reminiscent of phenomenology than Cartesian dualism; it shows that one's body impacts experiences in the physical world, which impacts how the mind thinks and thus communicates in cyberspace, and so even if someone knew nothing about the body of the person they were communicating with, their mind was still shaped by their bodily experiences. So, even if bodily anonymity was maintained by not disclosing their physical identity, a mind-body split was not achieved.

Furthermore, people in cyberspace were not afforded *no* identity—that is, they were not a brain floating in the ether—but were instead granted an *assumed* identity of whiteness and maleness (Nakamura 2002, 47–48; Moser and MacLeod 1996) because this was the identity of the majority of cyberspace users at the time, and people wanted to tie the text on their screen to a physical body. Boler (2007) noted that "A/S/L?" ("age/sex/location?") became one of the most common greetings in cyberspace and was a way to seek an essentialist grounding for the other person. MUD users gave "greater weight to offline identity than online identity," prioritizing information about the physical body over a virtual embodiment, and reported having more trust in those they had met face-to-face (Kendall 1998). Indeed, early cyberspace was tightly coupled to the physical world. Many BBSs catered to mostly local communities, partly because of the high cost of long-distance phone calls (Driscoll 2022, 16), and often facilitated face-to-face meetings, community gatherings, and even dates (Driscoll 2022, 153–56; Kendall 1998). Attending a physical meetup would then tie the physical body even more closely to one's online presence. Even absent physical meetings, anonymity was not disembodiment—users were still bound to a body, but not necessarily their own. If they disclosed aspects of their physical identity, or if it was inferred based on their typed speech, they could embody a digital persona more like their physical identity, but no longer enjoyed the "neutrality" they previously had.

Although even at the time there was evidence that the narrative of disembodied equality was not true for everyone (or anyone), those who promoted it were reluctant to engage with contradictory viewpoints. For the majority, "default" identity, it was convenient to believe that the same applied to everyone. This was evident at a 1991 BBS conference, where many speakers "hailed the coming of an egalitarian virtual community, free of bias" (Driscoll 2022, 174). However, the only Black woman at the conference, Lisa Downing, afterward published an open letter in *Boardwatch* magazine where she described how she was "snubbed and ignored" all weekend, cautioning that "[technology] will not erase the prejudices of the user" (Downing 1991, as cited in Driscoll 2022, 173–74). The editor of *Boardwatch* responded, insisting that she was the cause of any conflict and saying, “I doubt you were as unique and out of place as you apparently delight in thinking you were” (Rickard 1991, as cited in Driscoll 2022, 174). No one else in the community engaged after this. Regardless of exactly what happened at the conference, the way that the mostly white, mostly male community refused to engage with a critique of the culture they promoted was telling, reflecting a reluctance to engage on issues of race and gender when they contradicted their narrative of egalitarianism. White men were the majority of those online and thus the assumed identity who did not have to consider how their identity impacted their experiences (Driscoll 2022, 22–23), but believing that it was the same for everyone was erroneous.

Early cyberspace reflected the reality of the American society where it was born, which was awash with narratives of colorblindness and loath to discuss race (Kendall 1998). While the founders of early cyberspace likely genuinely believed in its potential as an equalizing force, the affordances of the technology at the time meant that only text-based communication was possible. It is logical that they would be trying to identify the supposed benefits of the technologies that they were pioneering. In general, they could be confident that, as a majority, they would not be harassed based on their gender or race, but they were often willfully blind to the fact that it did not carry over to all identity groups.

What was perceived as disembodiment by the primarily white, primarily male pioneers of cyberspace was instead a form of semi-anonymous embodiment, just in a default, “invisible” identity that one could exist in unchallenged because it was the dominant identity. Not everyone could access this form of uncomplicated embodiment, but many users desired it. One way this manifested was in affinity spaces. Identity-oriented BBSs, including for women, people of color, and disabled users, and specific sections of general-purpose BBSs sprung up to provide users with safe cyberspaces (Driscoll 2022, 151–54). By making specific non-dominant identities the majority, these shared spaces allowed them to think about physical identity less and experience the same bodily anonymity that white men did in most of cyberspace, escaping what could otherwise feel like a “nightmare” (Driscoll 2022, 151). Since inclusion in these spaces was predicated on one’s physical identity, virtual identities were still grounded in physical ones.

Even outside of affinity spaces, people showed a desire to bring a physical body into cyberspace. MOOs and MUDs often involved role-playing that required users to create a character description. Notably, following the color-blind discourse of the day, many of these eschewed formal categories for race, even though some included them for gender (Nakamura 2002, 37–38). These self-descriptions allowed people to try on new identities. Rather than exist as floating minds in the ether of cyberspace, they actively portrayed themselves not only as their physical identities truly were, but as other identities. Some claimed they did so for practical reasons; one man who played in MUDs as a woman said, "I do it to improve the ratio of women to men. It's just a game" (Turkle 1997, 212). Sometimes this was to explore aspects of their own identity; individuals questioning their gender identity could virtually embody different genders online in a way they could not necessarily do in the physical world. Regardless of motive, identity switching was a common practice; a study of MOOs found that 40% of participants in social MOOs had engaged in gender-switching, and more than half of participants in role-playing MOOs had (Roberts and Parks 1999).

Sometimes this led to problematic forms of embodiment. Many female personae, especially those played by men, were extremely sexualized (Nakamura 2002, 43–47). Furthermore, users often adopted highly stereotyped racial identities in cyberspace, a kind of "identity tourism" that entrenched racial stereotypes (Nakamura 2002, 43–44).[48] Ironically, these stereotyped embodiments were encouraged by the text-based medium; Nakamura noted that cyberspace being "disembodied" meant that "the need to create very clear, recognizable personae is thus a practical one" (Nakamura 2002, 39). In creating these "clear, recognizable" characters, people often fell back on stereotypes. This reality differs significantly from the Cartesian belief of early adopters that minds could exist merely as minds, with no ties to the physical body. Users wanted to bring some kind of body with them—whether their own, someone else's, or an invented one—and so "in constructing this necessary difference, the subject has recourse only to those markers of difference that already exist within the symbolic order… racial stereotypes provide

[48] These often cut along intersectional bounds; Asian female personae were especially subject to sexualization (Nakamura 2002, 43–47).

familiar, solid, and reassuring versions of race" because of their presence in media (Nakamura 2002, 40). By bringing a body that was not theirs in the physical world into cyberspace, people also brought racial stereotypes of the physical world into cyberspace.

Those who tried on different identities found that inhabiting them convincingly was difficult for the abovementioned reasons of how physical identity influenced textual communication; "passing" required a deep understanding of the ways that one's identity affects speech (Turkle 1997, 212), not just editing a self-description. In other words, as mentioned above, one's physical identity could still come through even in text-based environments. However, it could also teach people about identity in the physical world. For example, "[w]hen men playing females are plied with unrequested offers of help on MUDs, they often remark that such chivalries communicate a belief in female incompetence" (Turkle 1997, 214). Bruckman (1996) noted the same, and also that sexual favors were often expected from female personae in exchange for assistance (320–21). Even in textual environments, the divorce of mind and body was not always total. In a phenomenological exchange, the body informed interactions and experiences in cyberspace, which in turn shaped how people saw physical identities.

Although users could be anonymous in early cyberspace under specific circumstances, they could never be truly disembodied, and this was not universally accessible even to those who could access cyberspace. Nor was it universally desired. This Cartesian "forgetting" of the body (Stone 1991, 113) was a narrative propagated by the cultural discourse and technical limitations of the time. Based on a naïve understanding of biological embodiment, it promised liberation but ignored the social realities of textual interactions and the fact that people wanted to anchor the people on the other side of the screen in a physical body. Instead, people's physical identities impacted their experiences online, and people used their experiences in cyberspace to shape their perceptions of others in physical space.

4.2.2. *Virtual Reality*

Virtual reality research was being conducted at the same time that cyberspace was developing, but the two were largely separate due to technological limitations.[49] Two independent narratives about its development arose: one from one of the founders of the field, and one from academia and science fiction that was picked up in popular discourse. Although now VR headsets are the most common VR device, the most prominent VR development company, VPL Research (founded in 1984), initially focused only on VR gloves and suits because computers were not fast enough to support headset graphics (Lanier 2017, 226–27). They eventually released the "EyePhone," a VR visor, but the initial focus on gloves and suits shaped VPL's VR approach to focus on experiences through creative methods of input rather than emulating physical bodily interactions with the physical world and high-fidelity depictions of it. VPL's founder, Jaron Lanier[50] (who coined the term "virtual reality," at least in English[51] (Lanier 2017, 410)), said that the initial focus on gloves and suits was "a blessing in disguise" because "Input is more important than display. Your input in VR is you" (Lanier 2017, 227), which shaped VPL's approach to VR to focus on experiences through creative methods of input rather than emulating physical bodily interactions with the physical world. VR was initially first-person and non-immersive; one manipulated virtual objects using VPL's DataGlove and observed the effects on screen. This contributed to a different view of VR than seen today. Lanier saw VR as a way for people to connect on a small scale, overcoming discord through experiences so engaging and unlike physical reality that they transcended differences (City Arts & Lectures 2022).

---

[49] While there were experiments in connected, interactive virtual worlds, neither VR nor the Internet were mature enough to support consumer versions of these experiences (Lanier 2017, 269). However, both were products of Silicon Valley, and some of the same people were involved in developing them (Lanier 2017, 249), which laid the foundation for the eventual linkage of the two in the form of consumer networked VR that will be discussed in Section 4.4.

[50] There were other VR companies active in the 1980s, such as Superscape and Virtuality, but VPL was the most prominent, and Lanier was the foremost spokesperson for VR (Jaron Lanier, "An Interview with Jaron Lanier," 1989, Whole Earth Review; Barlow 1990b). Thus, this section focuses primarily on VPL.

[51] The French dramatist Antonin Artaud wrote about "la réalité virtuelle" in a 1938 collection of essays (Artaud 1938). He used the term to refer to "a nonverbal form of theater that was intense enough to rouse depths of human experience and understanding beyond the reach of conventional language" (Lanier 2017, 410), which resonates with the initial intentions behind VR.

Some of these involved manipulating the body schema, such as by inhabiting a lobster body (Won et al. 2015) or by being without an avatar and experiencing the "whole world [as] your body" (Barlow 1990b).[52] These examples of "homuncular flexibility" (Won et al. 2015) featured diverse input methods, but all used the physical body as input in the style of reality-based interaction (RBI)[53] (Jacob et al. 2008). All required using the physical body as input, precluding the possibility of leaving it behind. Notably, these experiences were also intended to enhance our appreciation of the physical world, not replace them. VPL kept a flower in a vase and instructed people to look at it after they emerged, often slightly shell-shocked, from VR, to ground them back in the physical world (Lanier and Kelly 2014). Foreshadowing the narrative schism, some who tried VR interpreted it as a dissolution of the physical body (Barlow 1990a). However, for its founders, VR was a very embodied experience, and any leaving behind of the body was a side effect rather than the primary goal, in contrast to the goals of the pioneers of cyberspace.

The founders of VR saw it as serving a very different purpose than early promoters of cyberspace, although its purpose was similarly shaped by technological limitations. It was not intended to separate the mind and body in the Cartesian style. It was instead supposed to promote an appreciation of the physical world and connect minds, but on a small scale (which was all the technology could support at the time), and by engaging using the body, not abandoning it. As Lanier wrote, people working on VR at the time were thinking that "maybe we'd collectively create a global virtual space, but even then, the connection with another individual should remain more cherished" (Lanier 2017, 191). This required instilling a sense of presence, or "being there," created through the "place illusion" that made the user feel like they were in a real place, combined with the "plausibility illusion" that what was being depicted in the virtual environment was actually occurring (Slater 2009). Thus, in focusing on physical interaction, it was reminiscent of the phenomenological view of embodiment and experience. The focus on small-

---

[52] While these experiences manipulated the body schema and one's feeling of being physically embodied, they were not able to recreate the secondary effects of embodiment because they could not create the mental state of *being* an entity with a different state of consciousness and sensory apparatus; to echo Nagel, they could not help someone understand what it is like to be a bat (Nagel 1974).

[53] RBI is a diverse group of interaction forms that uses "actions that correspond to daily practices within the non-digital world" and includes XR interaction (Jacob et al. 2008) because of its sense of presence and direct manipulation of content in 3 dimensions (Johnson-Glenberg 2018).

scale connection differs technologically and philosophically significantly from the "metaverse" of today's discourse, which is intended to be this "global virtual space." This evolution will be discussed further in Section 4.4.

Early VR did not have avatars due to technical constraints and so were first-person experiences in a "floating point of view" (Balsamo 1996, 126). Users of VPL's system employed the DataGlove to manipulate the virtual environment, tying the physical body to the virtual experience. VR researchers quickly implemented avatars, although early ones were limited to a floating head or single hand due to computer speed limitations (Lanier 2017, 247). Eventually, blocky full-body avatars that could be driven with VPL's DataSuit were developed (Lanier 2017, 247). These served practical purposes in games, but also in VPL's mission to connect people. The "Reality Built for Two" (RB2) included avatars so that multiple people could cohabitate in a "virtual world" simultaneously (Lanier 2017, 14). These avatars were not meant to be a replacement for the physical body, but a different incarnation of them—a "thought body" or "virtual body" (Barlow 1990b) that changed the body schema and created a "transfixing" experience (Lanier 2017, 15–16). Furthermore, the RB2 system focused not on emulating real-world activities, but on building virtual worlds together (Blanchard et al. 1990), showing its goal to transcend the limitations of the physical world, rather than the physical body.

Even though it was being developed in small Silicon Valley labs, VR quickly captured the cultural imagination, and it became associated with the same rhetoric of disembodiment as early cyberspace, facilitated by science-fiction and cyberpunk novels that appealed to both hackers and the masses. Early works in the 1980s like *Tron* and *Neuromancer* featured characters entering immersive dataspaces of Gibsonian "cyberspace," but it was not until 1992's *The Lawnmower Man* that VR was shown as an immersive virtual world experienced through headsets and VR clothing (provided by VPL) with the user inhabiting an avatar (Drummond et al. 2014). The 1990s saw a proliferation in VR-related media—including depictions in popular shows like *Murder, She Wrote*—culminating in 1999's *The Matrix* (Drummond et al. 2014) and cementing the image of VR as a virtual world intended to emulate the physical world, rather than as a tool for small-scale connection. These media promoted the Cartesian mind-body split by merging Gibsonian cyberspace and VR and took a contemptuous view of the physical body. *Neuromancer* describes the protagonist's loss of his ability to enter immersive "cyberspace" as "the Fall," invoking the Biblical fall from the Garden of Eden (Gibson 1986, 8). The catastrophe is justified as so: "The body was meat. Case fell into the prison of his own flesh" (Gibson 1986, 8). This disdain for the physical body was common in cyberpunk literature and painted one's virtual embodiment as more important than the physical body with the goal of "reaching the eventual obsolescence of the body" (Ajana 2005)—indeed, it was often intertwined with the egalitarian discourse of hacker culture—and portended the later focus on full-body VR avatars.

As VR entered the public consciousness, it also entered the academic discourse, and the pop culture dialogue on the body was replicated. Lanier's borderline-spiritual views fell by the wayside after VPL filed for bankruptcy in 1990 (Kim 2015). The result was a promotion of disembodiment similar to that surrounding cyberspace, facilitated by the "representational" disappearance of the physical body (Balsamo 1996, 126). Penny (1993) wrote that "Virtual reality replaces the body with two partial bodies: the corporeal body and an (incomplete) electronic 'body image'… Virtual reality leaves the meat body on the chair. It is a confirmation of, rather than a liberation from, Cartesian dualism." This "electronic body image" is distinct from Lanier's "virtual body," which was linked to the physical body rather than independent. Though a dualist rather than phenomenologist approach, it also echoes Merleau-Ponty's body image, foreshadowing the attachment people would form to their avatars.

Just as quickly, criticism of this dualist perspective arose. Balsamo (1996) noted that "Even though some games may soon allow players to design personal avatars or puppets—simulations of oneself—more frequently VR is promoted as a body-free environment, a place of escape from the corporeal embodiment of gender and race" (Balsamo 1996, 123), similar to the discourse of early cyberspace. She went on to argue that even without avatars, VR is an inherently gendered concept because the promises of disembodiment, like in cyberspace, were more easily experienced by those of dominant identities. Indeed, she posited that white men may have desired disembodiment as an "enticing retreat from the burdens of their *cultural* identities" that they had to grapple with as American society increasingly confronted issues of gender and race (Balsamo 1996, 131).

While the founders of VR—who saw VR as quite embodied—did not explicitly express a desire to escape the inconvenient realities of their white male bodies, it was true that not everyone had the same experience in cyberspace, and whether or not we accept Lanier's claim that VR is an embodied medium by default, it is clear that it was embodied to some extent. First, one's physical body impacted how one responded to entering VR. Women more often experienced "cybersickness" (also called "VR sickness") (Hayles 1996), a problem that persists today (Kelly et al. 2023). There were also representational issues that meant that some people could not embody an avatar that looked like their physical body; many "generic" avatars still read masculine and, often, white (Green 1997, 65–67). There was limited disability representation and, since VR devices were still being developed, little accessible hardware, although some early VR applications were developed to help veterans with memory impairment, facilitate sign language, and provide aphasia therapy (Lanier 2017, 381).

While perceptions of cyberspace were shaped by pop culture, individuals often had little practical experience with VR. VR technology was so expensive that there was little consumer market. Some arcades installed VR games (Fowle 2015), but home applications remained limited. VPL's DataGlove cost $10,000 and required a $250,000 computing system, putting it out of reach of even early adopters. Consumer-targeted devices, did not live up to technological expectations and were rapidly discontinued. For instance, Mattel worked with VPL to create a $90 Power Glove intended to be used with the Nintendo NES. It was released in 1989 and sold hundreds of thousands of units in the US and Japan, but difficult setup and the lack of dedicated games caused it to be discontinued within a year (Rossen 2017). Similarly, Nintendo launched its "Virtual Boy" VR console in 1995 and discontinued it in 1996 after disappointing sales despite a $25 million marketing campaign (Boyer 2009), while Sega's "Sega VR" was canceled before its launch because of severe cybersickness issues (Vinciguerra 2015). Even VR arcade games were declining by the mid-1990s (Fowle 2015). Thus, people's perceptions of VR were shaped more by science fiction rather than their own experiences.

In the narrative clash of early VR, the portrayal of VR as a disembodying, Cartesian experience won out over the idea that VR was a pseudo-spiritual experience inherently tied to the physical body and intended to augment the physical world, perhaps because the former was easier to market in pop culture. Regardless of narrative, people's physical identities did impact their experiences in cyberspace for both biological and social reasons. However, VR proved not advanced enough for widespread adoption, and while it remained present in pop culture, there was little opportunity for most people to use VR in the ensuing decades.

4.3. Internet Summer, VR Winter

The late 1990s and early 2000s marked a pivotal transition in how people experienced embodiment in digital spaces. While the Internet flourished with increasingly sophisticated visual interfaces and avatar systems that promised new forms of self-expression, virtual reality technology retreated from public consciousness after failing to deliver on its ambitious promises. This period revealed a fundamental tension: as online platforms became more visually rich and accessible, they simultaneously imposed new constraints on how users could represent themselves, while the broader digital divide meant that experiences of virtual embodiment remained deeply unequal.

4.3.1. Internet

As technologies advanced beyond purely text-based interfaces and the invention of the World Wide Web and web browsers made accessing cyberspace less intimidating, platforms responded to users' desire to be embodied in cyberspace with different categorization and depiction methods. At the same time, barriers to access increased the digital divide.

The presence of graphical user representations made it clear that people were to some degree embodied online. The narrative reminiscent of Cartesian dualism faded, but the prevailing attitude became that although physical traits could be apparent online, they did not matter—especially race, where an explicit attitude of colorblindness dominated (Kang 2000), imported from American culture where a discourse of color- and class-blindness reigned and transferred into online interactions (Kendall 1998). However, as in the text-based cyberspace days, the reality was more complicated, and the social impacts of embodiment could not be escaped. People desired embodiment online for themselves and others, but this once again meant that people had unequal experiences in cyberspace.

As computers and Internet connections grew faster, transmitting images became feasible. Platforms increased embodiment online through graphical avatars, but mediated forms of embodiment through platform design. The term "avatar," derived from the Sanskrit "avatara" (referring to the "descent" of a deity adopting a physical, terrestrial form (Junghare 2012)), was first used to refer to an virtual character in the 1985 video game *Ultima IV: Quest of the Avatar* (de Wildt et al. 2020). However, it was used not to refer to a generic representation of a player, but in 1986, F. Randall Farmer and Chip Morningstar incorporated the term into Lucasfilm's *Habitat* to refer to the player's "online persona" (Britt 2008).[54] Neal Stephenson also used it in his 1992 novel *Snow Crash*, after which it began to be used to refer generically to online representations of people, whether pictorial or 3D, anthropomorphic or abstract, and static or dynamic (Nguyen 2023). For instance, chat program *The Palace*'s first avatars in the mid-1990s were bright green spheres with faces of different expressions (Carpenter 2018). Soon, though, customization arrived. Platforms including *The Palace* eventually allowed users to upload their own images, while others like *Second Life* had them customize a humanoid body. Eventually, static icons and pictures that were previously called "avatars" became "picons," "userpics," and "profile pictures" (Nguyen 2023), and "avatar" was reserved for dynamic full-body representations. An archive of "picons" shows that many were the faces of actual people (Picons, n.d.). In *The Palace,* using a "real face av" was seen as a gesture of intimacy, a way to "step out" of "anonymity" (Suler 2001) that implied that someone was embodying a character more like their physical self. Even though avatars that were not of a "real face" could be perceived as equally embodied—and there was no guarantee that what someone presented as a "real face av" was their real face—the physical body was still prioritized above virtual embodiments, just

[54] I'm grateful to an anonymous *Virtual Reality* reviewer for bringing this to my attention.

as it was in the BBS and MUD days when meet-ups in the physical world were ways to build trust in cyberspace. Eventually, social networks like Facebook would take advantage of this by encouraging people to use their real identities online, coupling the on- and offline identities tightly together; this will be discussed more in Section 4.4.

Although avatars may have offered a form of anonymity, even lower-fidelity representations were a form of embodiment—albeit an "alternative mode" (Ajana 2005)—and this promoted differential experiences in cyberspace. A study of pictorial avatars found that people preferred avatars that matched their gender and that more anthropomorphic avatars were seen as more attractive and more credible (Nowak and Rauh 2005). This shows that not only did people pick avatars to represent themselves, but they also made judgments about other users based on their avatars. Thus, there was still meaningful virtual embodiment, as there was in textual cyberspace. This allowed people to form genuine connections—*Second Life* was a true second life for many people, with a survey of Dutch players showing that 33% of respondents spent more than 30 hours per week in its virtual world (Leenes 2008)—but also increased the potential for negative experiences. Ajana (2005) argues that the Merleau-Pontian phenomenal body was extended into the virtual sphere, which implies that harm to one's online persona would be experienced as an affront to the physical self. Trauma reactions to harassment, even in text form, show that this was the case (Dibbell 1994); if the virtual persona was an insubstantial thing independent of the self, online experiences would not trigger such responses.

Having visual representation made harassment easier, although specific statistics are difficult to come by. Still, in 1998, 41% of female Internet users reported being sent unwanted pornographic material or being harassed or stalked online (Griffiths 2000), with many women reporting being deluged with sexual messages just because they had a female screenname (Döring 2000). To extrapolate, having a pictorial representation of an individual rather than having to read a textual description or sift through their posts would make targeting them much easier. Racial harassment in these spaces was also common (Kang 2000). Furthermore, sometimes platform affordances enabled new forms of harassment. For instance, in *The Palace*, one user would adopt an avatar that was "a pair of upside[-down] legs that he insert[ed] down the cleavages of unsuspecting women, giving the illusion of the rest of his body being inside their dresses" (Suler 2001).

More literature has focused on full-body avatars such as those in *Second Life,* where harassment and assault are acknowledged as two of the biggest issues facing the platform (Bugeja 2008). A database of reported incidents (both community standards and terms of service violations) between 8 June 2007 and 24 December 2010 showed 3,778 incidents of nine different kinds of harassment; 392 (10.4%) were classified as "sexual harassment" or "teen sexual harassment" ("Second Life Incident Reports Repository," n.d.). These fell disproportionately on women, with 60% of women reporting being harassed or stalked compared to 44% of men (Beck 2015). Even in the BBS and MUD days, people faced racist and homophobic comments, with some speculating that the same anonymity that to a certain extent concealed their identities empowered people to say things they would not in the physical world (Moser and MacLeod 1996). In the increasingly embodied Internet, people not only had anonymity, but also more accessible identity markers to use to target their attacks.

Platforms attempted to counter harassment through moderation, but also managed and mediated online embodiment through platform design in a way that implied that not all physical traits should matter or be represented in virtual contexts. While encoding identity options through tools like dropdown menus made categorizing users easier, it also restricted self-expression to the pre-defined categories chosen by the platform. Some platforms had many gender options—such as LambdaMOO, which included four different gender options in the 1990s (Nakamura 2002, 36) and ten in the 2000s (Fandom, n.d.)—while others adhered to a strict binary (Bruckman 1996, 318; Fizek and Wasilewska 2011). The move from textual descriptions to picons to avatars also restricted embodiment options; instead of being able to describe themselves or upload any image they wanted, users were restricted to options defined by the platform. This impacted not only representations of gender, but also of race and disability.[55] Linden Labs initially did not provide wheelchairs in *Second Life*, even as it coded different walking styles for male and

[55] Independent of representation, for visually impaired users, early text-based cyberspace was in fact the most accessible, as the introduction of graphical interfaces broke many screen readers (Perry et al. 1996).

female avatars (Fizek and Wasilewska 2011). One virtual space designed for teens, *Whyville*, was noted for having some non-white avatar heads but few bodies to match (Kafai et al. 2010). This encoded—literally—who could be embodied online and how, and non-white avatars were under-represented in virtual fantasy worlds (Higgin 2009). In some cases, this was due to a lack of representative avatar options. In others, as in the BBS days, it was because of a reluctance to embody an avatar that might subject them to more harassment. Sometimes these were linked; one participant in *Whyville* was told that her Black avatar "looked wrong" because most avatars were white (Higgin 2009).

Finally, as in the days of BBSs, the digital divide continued. While Internet service providers (ISPs) had sprung up in the US, lowering technological barriers to cyberspace access, they erected further price barriers, perpetuating economic and racial access disparities. In 1998, 36.0% of households of Asian/Pacific Islander descent and 39.8% of white households had access to the Internet, compared to 25.5% of Black households and just 12.6% of Hispanic households (Kang 2000). In the late 1990s, the digital divide was widening, not narrowing (Chon 2000). Furthermore, cyberspace was most accessible to those who spoke English, with three-quarters of websites hosted in the US and other English-speaking countries in 1996 (Chon 2000).[56] Physical characteristics not only affected experiences in cyberspace and VR but also were correlated with people's ability to access them. While the existence of virtual embodiment (reminiscent of phenomenological theories) was being acknowledged, it was in a passive way that did not inspire action to ensure equitable representation and experiences.

4.3.2. Virtual Reality

After the initial phase of hype, VR consumer technology was mostly dormant. Schroeder (1993) identified three strands of VR in the 1980s and early 1990s: art and entertainment, flight simulation and robotics, and military and space-related research. Of these, flight simulation and military applications found the

[56] This language imbalance has persisted to today, and resulted in large language models (LLMs) being more proficient in high-resource languages more represented in the Internet data that forms the bulk of their training datasets (Beyene et al. 2025).

most success, meaning that VR was largely out of the public eye. By the mid-1990s, consumer products and experiences had largely gone bust, and portrayals of VR in media slowed down in the early 2000s (Drummond et al. 2014). Flight simulations and medical VR research continued, driven primarily by the military. The US and British Air Forces developed VR flight simulators for pilot training, and the Defense Advanced Research Projects Agency (DARPA) funded the development of telepresence technology for surgeries (Lowood 2024). Still, from the perspective of the average Internet user, VR was a technology that existed mostly in science fiction, which promoted the full-body, total-immersion version of VR that was, at the time, still technologically infeasible.

4.4. VR Resurgence and Cultural Merging

By the 2010s, cyberspace had transformed, dominated by social media sites. These platforms encouraged people to use their real identities online, with Facebook initially implementing a "real name policy" (Facebook Help Center 2014)—later nuanced to require names users "go by in everyday life"—to promote "authenticity" and community accountability (Meta Transparency Center 2023). Although some platforms allowed anonymous accounts, many social media platforms were marketed to facilitate "authentic" connections, with authenticity predicated on real identities, reminiscent of "real face avs" and identity-confirming BBS meetups.

VR experienced a resurgence with the launch of the Oculus Rift on crowdfunding platform Kickstarter in 2012. Advances in 3D graphics and hardware made consumer VR headsets viable. With them came avatars that went far beyond the blocky heads and hands of early avatars, as well as "social VR" platforms called "metaverses." The term "metaverse" first appeared in Neal Stephenson's *Snow Crash* (Zenou 2022) and is often etymologically defined as "beyond universe," but according to Jaron Lanier in a 2022 interview, the term was an inside joke between Lanier, Stephenson, and Gibson. The use of "meta" referred to the meta key on programmer workstations, which was known as the "god key" for the extra functionality it enabled (Egan and Lanier 2022). Likely unaware of its tongue-in-cheek background, in 2021 Facebook rebranded as "metaverse-first" company Meta and launched its "metaverse" platform *Horizon Worlds* (Meta 2021a; Zuckerberg 2021).

Social VR platforms are a merging of cyberspace and VR. Essentially immersive social media platforms, they are now similar to the immersive virtual worlds called "cyberspace" in cyberpunk and other science fiction. As a result, we need to consider modern VR and its narratives in the historical context of both cyberspace and VR. While the technology's foundations lay in 1980s Silicon Valley labs, its ethos of authenticity and celebrating of identity is an evolution of cyberspace discourse. However, platform actions are often at odds with their rhetoric.

Embodiment in cyberspace has evolved from text to images and two-dimensional avatars to three-dimensional avatars piloted in a virtual world. While MUD research suggested that about half of people saw their online persona as a separate entity from themselves (Turkle 1994), users in VR identify strongly with their avatars and often use them to explore aspects of their identity by modifying their virtual self-presentation (Freeman et al. 2022), showing the connection between the virtual phenomenal body and the physical body. Platforms have taken note and implemented a wide range of avatar options. Social VR platform *VRChat* is notable for having a wide range of humanoid and more creative avatars, including a hot dog (VRChat 2023). *Horizon Worlds*, on the other hand, focuses on humanoid avatars, reflecting Meta's focus on "authenticity," although Facebook's real name policy does not extend into *Horizon Worlds*. Meta has consciously focused on enabling users to create any depiction of themselves that they want.[57] Chief Diversity Officer Maxine Williams wrote that "*you* should be able to be authentically present" in VR; there were over 1 quintillion possible avatars in 2022 (Williams 2022). Meta's Codec Avatars aim to go beyond this by creating a photorealistic model of the face and, eventually, the entire body (Ma et al. 2021), essentially translating bodily self-presentation entirely into virtual reality.

Platforms, acknowledging that displaying physical traits is unavoidable in social VR, now insist that user diversity is something to be celebrated. This is a shift from the discourse of cyberspace that held

[57] People often create idealized avatar representations of themselves (Ducheneaut et al. 2009), raising questions about the relationship between avatar creation and body image that should be further explored.

that physical traits were not conveyed through text and the early Internet that insisted that while they could be displayed, they were irrelevant, and reflects the changing American discourse, which instead of ignoring race and gender now recognizes that it exists and creates different social experiences. The focus on "authenticity" echoes the "bring your whole self to work" movement (Inam 2018), which Sheryl Sandberg, former Chief Operating Officer of Meta, called her "central management message" (Frier 2017). The philosophy endorses showing all aspects of your identity to work and having them be celebrated. For individuals to be able to authentically express themselves in VR, they cannot be subject to differential treatment based on those identity characteristics. However, as in earlier online platforms, they often are, and the way platforms have responded to issues of harassment and accessibility cast doubt on their claims of experiential equality and imply that they are adopting an oversimplified position similar to that of early cyberspace pioneers.

Online harassment is not a new issue and was known to be a problem in VR before *Horizon Worlds* launched (Frenkel and Browning 2021). Despite promises from Mark Zuckerberg that safety would be "built into the metaverse from day one" (Meta 2021b), harassment instantly became a problem on *Horizon Worlds*. A female beta user was surrounded and groped by male avatars, and Meta responded by implementing a "personal boundary" feature, but an investigation of *VRChat* found that most harassing behavior did not involve contact (Lawson 2022). Chief Technology Officer of Meta, Andrew Bosworth, questioned whether keeping VR safe is even possible (Frenkel and Browning 2021), which is debatable because VR combines the immersion and presence that makes harassment in the physical world damaging with the anonymity of cyberspace that encourages it. As a result, racist, sexist, and homophobic harassment remain rife on social VR platforms (Outlaw 2018; Frenkel and Browning 2021; S.B. et al. 2024).

One thing that users are not harassed about are markers of physical disability—because they often do not exist in VR, despite the emphasis on representation. Meta promoted their release of hearing aids, cochlear implants, and wheelchairs for avatars, but wheelchairs are only available for avatar stickers, not for the actual avatars (Meta Accessibility 2022), and prosthetic limbs and amputees cannot be represented, echoing the initial lack of options in *The Sims*. Although the fact that there are some representation options is a step up from the early days of VR games and social platforms—*VRChat* launched with a single avatar, "Karl," a white male (VRChat 2019)—there remains work to be done. Lack of accessibility is often an economic question, as regardless of the ethics of not having representation, if something costs more to implement than the value the platform perceives, the platform will not implement it. However, as Perry et al. (1996) noted, "part of the problem is lack of imagination." The same applies to hardware. VR hardware and software are not designed for people with physical or cognitive disabilities, meaning that people with disabilities are excluded from bringing their authentic selves to VR, even though they may be more inclined to want to use VR (French 2017). Furthermore, as with computers in the early days of networked computing, price remains a significant factor, with consumers hesitant to spend the equivalent of hundreds or thousands of US dollars on still-maturing technology.

Social VR is still emerging, but it seems poised to have an impact on many people even if it does not become the universally accessed virtual world portrayed in science fiction. Because it carries many of the features of social media, including the possibility of anonymity, combined with the immersive nature and embodied interactions that are similar to the physical world, its potential impact on users is significant, making it all the more important that we analyze who is deciding who gets to be embodied and how. Social VR is attempting to overcome the issues of physical society by insisting that everybody and every body is celebrated, but as in the physical world, saying so does not make it so, and active intervention is necessary to ensure that it is an environment where everyone can have an equitable experience.

4.5. Conclusion

Over forty years, cyberspace and VR have evolved and now, merged. While the modes of interactions and technologies have changed, one thing that has remained constant is that the "male, white, straight, able-bodied and ruling class" cybersubject is also the one with an outsized role in defining the technology and culture (Moser and MacLeod 1996), representing the plurality of technology workers, especially at the executive level (Fury 2023). While the narrative has evolved from one of a Cartesian split between the mind and body to a more accurate phenomenological understanding that online experiences are embodied, the shift from denying how bodies influence cyberspace experiences towards attempting to celebrate them has not changed that the realities of the "shadow halves" of the dominant identities are often overlooked (Moser and MacLeod 1996), including—and especially—when they have disparate experiences that call the dominant narrative into question. This matters because as embodiment in virtual spaces—both immersive and non-immersive—increases, so too does the potential for harm that is not virtual harm, but real harm.

The early days of cyberspace offer opportunities and cautionary tales. On the one hand, social VR might allow for increased trust online if avatars are seen as an acceptable substitute for the physical body, and could facilitate the identity-oriented spaces that provided a haven for marginalized groups. On the other, it may offer the ultimate combination of anonymity and targetability that encourages harassment, a problem that is already developing. Conversations around platform policies and design should acknowledge the embodied nature of XR and how "online" experiences have offline impacts. As XR development continues, more research should explore who is able to be embodied in modern XR, expanding beyond VR to include AR and MR and exploring governance models to address how to balance anonymity, safety, and self-expression. Ultimately, though, the history of embodiment in the virtual sphere and the consistency with which marginalized groups have worse experiences show that these issues are fundamentally human ones. Rather than throw up our hands at the flaws in human nature—or worse, deny their existence—we must take action to counter them in our new virtual worlds just as we try to do in the physical world. Racism, sexism, ableism, and other forms of discrimination will not vanish just because we interact with each other in a virtual space.

It must be acknowledged that in 2024 and early 2025, platforms including Facebook and X (formerly Twitter) began moving away from content moderation, particularly in the US, leading to increases in hate speech targeting vulnerable groups (Hickey et al. 2025; Kaplan 2025). These trends are concerning and may foreshadow a shift to a new era: one where platforms acknowledge that one's body impacts online experiences, and yet do not consider it their responsibility to address. Though research is still emerging about the concrete effects of these changes, those increases in hate speech, plus incidents of explicit deepfakes of female celebrities going viral on X—with one of Taylor Swift being seen over 47 million times before being taken down (Aubrey 2024)—raise concerns about platforms' commitment to protecting people of marginalized identities. This was exacerbated by an upgrade to X's native generative AI tool, Grok, creating a "spicy" mode that generated nude deepfakes of celebrities without the user prompting (Weatherbed 2025). The law has turned against the exploitation of women's bodies online; the US passed the TAKE IT DOWN Act in the US (TAKE IT DOWN Act 2025), which requires that platforms remove reported content within 48 hours. The EU's directive on violence against women[58] (set to be implemented by member-states by 1 June 2027) criminalizes non-consensual pornographic deepfakes (Desmarais 2025). However, the law is one thing; online culture is another. If online culture continues to exert this ownership over the bodies of marginalized groups to the extent that it filters into XR, it becomes all the more imperative to protect those vulnerable individuals because of the increased potential for harm in XR.

This chapter will conclude with a perhaps naïve argument: regardless of law, platforms *do* have a moral obligation to moderate content and behavior to protect vulnerable users, and we have an obligation to treat our fellow humans better, whether they are in a physical body or a virtual one. The next chapters will commence this thesis's fundamental rights analysis, building on this impact-centered view of XR.

[58] (Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on Combating Violence against Women and Domestic Violence 2024)

Part III: Fundamental Rights Analysis

Overview

Having laid out my theoretical framework arguing for the stakes of IXR as a potentially highly impactful technology and a theoretically fruitful one, Part III shifts from conceptual groundwork to a rights-centered analysis. Taking XR as a fundamentally mediated and embodied reality, it asks how core rights travel across realities and how EU law addresses potential harms. Thus, this section addresses two research questions:

RQ2: What are the positive and negative impacts of IXR on fundamental rights?

RQ3: How does the extant EU legal regime address the fundamental rights impacts of IXR?

Working within a UDHR-grounded, GELSI-informed frame and focusing on immersive extended reality (IXR), the analysis operates within the sociotechnical, experience-centered frame of IXR established in previous chapters to analyze how users' rights—and sometimes those of bystanders—are impacted by this emerging technology.

Throughout this section, I assume that regulation should primarily focus not on a specific technology—even if it is an important factor that needs to be considered—but on the kinds of experiences that technologies enable (Floridi 2020a). This approach mitigates the risk that regulation would quickly become outdated. It informs my broad focus on aspects of extended reality, rather than specific XR technologies.

The threats to fundamental rights posed by IXR are channeled through two main avenues: by amplifying the psychological and physiological impacts of virtual experiences and by enabling the increased collection of personal data, particularly sensitive and biometric data. In the context of other emerging technologies, such as AI, these two pillars have also been topics of concern for the EU. For instance, the AI Act highlights how AI poses a threat to individual data privacy, as well as the potential to increase surveillance (Recitals 27, 110). It also bans AI that uses "subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques" in a way that causes them to make a decision they otherwise would not have in a way that causes "significant harm" (Art. 5), thereby attempting to prevent negative psychological impacts from technology.[59]

Chapter 5 maps IXR's impacts on safety and privacy. It argues that immersive realism and pervasive biometric data collection are the principal channels through which IXR creates novel risks and amplifies familiar ones, then assesses these risks against emerging EU approaches and likely extraterritorial effects.

Chapter 6 turns to the freedoms of assembly and expression. Building on taxonomies from the human-rights literature and UN General Comments, it shows how IXR both facilitates and endangers these freedoms as embodiment, presence, and interactivity make online experiences more like offline ones.

This section's purpose is practical: to surface a policy-relevant threat landscape, assess the (partial) fit of current EU instruments, and orient recommendations. There is a necessary imbalance in the degree to which each chapter addresses benefits versus risks. **Chapter 5** on safety and privacy is primarily risk-oriented, while **Chapter 6** on freedoms of assembly and expression weighs both benefits and risks. The asymmetry follows from the structure of the rights at issue and from the account of infrastructure and embodiment developed in Part II. Following Hohfeld (1917), safety and privacy can be classified as *multital rights*—that is, claims that we as individuals hold against an indefinite number of people, which imposes a corresponding duty to refrain from actions that would violate that right. Thus, my primary concern is for the actions of others that may violate those rights. Though Hohfeld gives the example of assault and the non-consensual publishing of a picture of someone, new technologies offer new ways to potentially infringe on these rights. Freedoms of assembly and expression, on the other hand, are

[59] It should be noted that what constitutes "subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques" is unclear and that this focus may distract from more dangerous systems (Boine 2025).

privileges—freedoms to act a particular way without being legally punished for doing so. They are something that can be actively exercised, and also that can be infringed upon. Thus, we must consider both how they can be supported and hindered by emerging technologies.

Together, these chapters operationalize the theoretical commitments of Part II: if infrastructures constitute experience and embodiment is consequential, then fundamental rights analysis must meet XR at the level of reality construction. This orientation sets the stage for Part IV's prescriptive work on governance and design interventions.

Horizontal EU Instruments: Background and Governance

The analysis in Chapters 5–6 draws on a common toolkit of EU measures that cut across sectors: device and platform safety (the General Product Safety Regulation and Product Liability Directive), cybersecurity risk management (the NIS2 Directive), data protection and communications secrecy (the General Data Protection Regulation and ePrivacy Directive), platform governance (the Digital Services Act), AI-specific prohibitions and transparency (the AI Act), audiovisual obligations for video-sharing platforms (the Audiovisual Media Services Directive), and consumer-protection rules against unfair commercial practices (the Unfair Commercial Practices Directive). Rather than re-introducing each instrument in every chapter, I cite only the provisions that change the outcome for the right at issue. Chapter 5 applies the toolkit to safety and privacy; Chapter 6 applies it to assembly and expression. Where background on harms is needed in Chapter 6, I cross-reference Chapter 5 instead of repeating it.

General Product Safety Regulation (GPSR) (Regulation (EU) 2023/988)

Scope & Key Definitions

The General Product Safety Regulation (GPSR)[60] is the horizontal safety net for consumer products not fully covered by sectoral harmonization rules. It became applicable in December 2024, replacing the General Product Safety Directive[61] "in light of the developments related to new technologies and online selling." It defines a "product" as "any item… supplied or made available… including in the context of providing a service" intended for or foreseeably used by consumers (Art. 3). Products must be evaluated for safety; the assessment must consider "state of the art and technology," consumer expectations, and (where applicable) standards (Arts. 3, 7–8, 9). Recitals emphasize the risks of new technologies (Rec. 89, 91) and that individual fundamental rights must be protected (Rec. 75).

Applicability to IXR

Consumer XR headsets, controllers and embedded software are considered "products." Manufacturers must thus perform pre-market risk analysis and maintain technical documentation; safety assessments should expressly account for software behavior, connectivity, foreseeable updates and cybersecurity vulnerabilities. Post-market duties (incident handling, recalls, consumer remedies) apply. Where sectoral rules (e.g., radio equipment, machinery, medical) govern specific risks, the GPSR fills remaining gaps.

---

[60] (Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on General Product Safety, Amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and Repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (Text with EEA Relevance) 2023)

[61] (Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on General Product Safety (Text with EEA Relevance) 2001)

New Product Liability Directive (PLD) (Directive (EU) 2024/2853)

Scope & Key Definitions

The updated Product Liability Directive (PLD),[62] which entered into force in December 2024, modernizes strict liability for defective products and explicitly includes physical products, software, components (tangible or intangible), and "related services" integrated into or inter-connected with a product (Art. 4). Liability applies to manufacturers when a product defect is due to a related service, software, or a lack of software updates (Art. 11). "Damage" now includes personal injury "including medically recognised damage to psychological health," and destruction or corruption of non-professional data (Art. 6). Assessment of defectiveness must consider reasonably expected safety, including safety-relevant cybersecurity requirements and the effect of learning systems (Art. 7; Recitals 30–35).

Applicability to IXR

Defects in XR hardware, firmware, platform software, software updates, or integrated digital services can ground strict liability if they fail to provide the safety the public is entitled to expect. Cybersecurity weaknesses (e.g., vulnerabilities allowing harmful outputs or unsafe device behavior) are expressly relevant to defectiveness. Data corruption (e.g., loss of user-generated XR assets not used for professional purposes) and medically recognized psychological harm are compensable forms of damage. Online platform providers may also be liable in certain circumstances analogous to distributors (Art. 8(4)).

[62] (Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on Liability for Defective Products and Repealing Council Directive 85/374/EEC (Text with EEA Relevance) 2024)

NIS2 Directive (Directive (EU) 2022/2555)

Scope & Key Definitions

The 2022 NIS2 Directive,[63] which went into force in January of 2023, imposes cybersecurity risk-management and incident-reporting obligations on "essential" and "important" entities across listed sectors. Annex II expressly includes "social networking services platforms" as a critical sector with accompanying cybersecurity risk-management and reporting obligations.

Applicability to IXR

An IXR service whose core functionality includes large-scale social networking (e.g., public profiles, social spaces, messaging, and content feeds) can fall within the "social networking services platform" category, defined as "a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations" (Art. 6). The "multiple device" requirement may provide a loophole by which immersive VR social worlds do not qualify, but many are likely to be accessible from or have other functions (e.g., messaging) available on other devices. Entity size is to be taken into account when considering risk management measures (Art. 21), meaning that, like the DSA, IXR platforms may be too small to be of significant concern. Still, where in scope, the provider must implement security measures (including policies, vulnerability handling, and supply-chain security) and inform a Member State computer security incident response team (CSIRT) of significant incidents.

[63] (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive) 2022)

General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

Scope & Key Definitions

The General Data Protection Regulation (GDPR),[64] which entered into force in 2016 and mandated full compliance by May 25, 2018, harmonizes EU rules on processing personal data to protect individuals' rights while enabling the free movement of data within the Union. The GDPR deals with "personal data," defined as "any information relating to an identified or identifiable natural person" (Article 4(1)). "Biometric data" is personal data resulting from specific technical processing of physiological or behavioral characteristics that allow for unique identification (4(14)). The GDPR applies to any processing of personal data by a controller or processor established in the EU or offering goods/services to, or monitoring, data subjects in the EU (Art. 3).

Applicability to IXR

Most IXR telemetry (account identifiers, social graphs, user-generated content, voice, hand and body motion traces, eye-gaze, spatial maps) will be "personal data" whenever it can be linked to a user, often directly or by reasonable means. If the XR stack captures or infers unique identifiers from physiological patterns (e.g., iris, face, or gait), this can be "biometric data," triggering special-category treatment depending on purpose and Member-State rules. Controllers must satisfy a lawful basis, respect purpose limitation, data minimization, and implement DPIAs where high risk is likely (Arts. 5, 6, 35). Controllers must also provide plain-language information to users about their data processing measures and when personal data is collected from users (Arts. 12-13). Given multi-jurisdiction deployments and remote services, Art. 3 ensures coverage even for non-EU providers targeting EU users.

If XR technologies are considered "new technologies" and the processing they entail is considered "likely to result in a high risk to the rights and freedoms of natural persons," then a data

[64] (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) 2016)

protection impact assessment (DPIA) is mandatory (Art. 35(1)). A DPIA is also mandatory when automated processing results in "a systematic and extensive evaluation of personal aspects relating to natural persons" and "on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person" (Art. 35(3(a))), when special-category personal data—including data revealing an individual's race or ethnicity, health-related data, and "biometric data for the purpose of uniquely identifying a natural person"—is processed on a "large scale" (Art. 35(3(b))), or when "a publicly accessible area" is systematically monitored "on a large scale" (Art. 35(3(c)).

ePrivacy Directive (2002/58/EC), read together with the EECC (2018/1972)

Scope & Key Definitions

While the GDPR governs "processing," the Directive on Privacy and Electronic Communications (ePrivacy Directive)[65] defend the communications layer and the device itself. The ePrivacy Directive went into force in 2002 and was amended by Directive 2009/136.[66] IXR equipment likely qualifies as "terminal equipment" under the ePrivacy Directive because it connects to the Internet (Vale and Berrick 2023); in the Directive on Competition in the Markets in Telecommunications Terminal Equipment,[67] "terminal equipment" is defined as equipment that "directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information." IXR devices store biometric and other sensitive information, including metadata automatically generated by users' interactions with the platform. Article 5(1) of the ePrivacy Directive requires Member States to ensure the confidentiality of communications and related traffic data in public communications networks and publicly available

[65] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)* 2002 OJ L 201, 31.7.2002, p. 37.

[66] (Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws (Text with EEA Relevance)Text with EEA Relevance 2020)

[67] (Commission Directive 2008/63/EC of 20 June 2008 on Competition in the Markets in Telecommunications Terminal Equipment (Codified Version) (Text with EEA Relevance) 2008)

electronic communications services (ECS); Article 5(3) governs storing and reading information on terminal equipment.

This applies to all "electronic communications services" (ECS), which are defined in the Directive 2018/1972 establishing the European Electronic Communications Code (EECC)[68] (which supplanted the originally referenced Framework Directive 2002/21/EC) to include (a) Internet access services; (b) number-based interpersonal communications services (ICS); (c) number-independent interpersonal communications services (e.g., over-the-top (OTT) messaging); and (d) transmission services "used for the provision of machine-to-machine services and for broadcasting" (Art. 2). It excludes services "which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service" (Art. 2(5)), which could possibly include services like comments on videos. The inclusion of OTT messaging services, which do not rely on mobile networks like traditional text messaging services, was much debated and subject to multiple clarifications to ensure their inclusion (Fazlioglu 2018; 2021) Furthermore, the recitals expressly contemplate services provided "over the Internet" (Rec. 6, 20).

Applicability to IXR

If an IXR provider offers user-to-user messaging or voice communication within the service, those layers can be considered an ICS under the EECC (so long as they are not deemed "minor ancillary features"); where offered to the public, they are "publicly available" ECS, and ePrivacy Art. 5(1) confidentiality obligations attach to the communications layer. Separately, any IXR app or SDK that stores/reads data from users' headsets/phones (for telemetry, profiling, measurement, etc.) must meet Art. 5(3) conditions (that is, the provision of clear information with the right to refuse, subject to narrow transmission and

[68] (Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 Establishing the European Electronic Communications Code (Recast) (Text with EEA Relevance) 2024)

strictly-necessary exceptions). The EECC does not displace ePrivacy's duties; rather, its definitions frame whether a given IXR feature is an ECS for ePrivacy purposes.

Digital Services Act (Regulation (EU) 2022/2065)

Scope & Key Definitions

The Digital Services Act (DSA),[69] which entered into force in November of 2022, creates a single-market, due-diligence framework for intermediary services and online platforms to make the online environment safer and more transparent. Most XR services likely fall under the DSA's definition of "intermediary services" under the category of "hosting services," defined as "the storage of information provided by, and at the request of, a recipient of the service" (Art. 3(g)(iii)). Where they curate or disseminate user content, as many social VR platforms and some AR services do, they are likely also considered "online platforms,"[70] a subset of hosting services. Very large online platforms (VLOPs) are designated based on an average monthly active user threshold (45 million) with accompanying duties to counter systemic risks (Art. 33).

Applicability to IXR

An IXR platform that stores and publicly disseminates user-generated worlds, assets or streams is a "hosting service," and if dissemination to the public is a core function, an "online platform." That triggers notice-and-action, statement-of-reasons, and recommender-system transparency duties; at scale, VLOP obligations on systemic risk assessment/mitigation, independent audits and data access for vetted

---

[69] (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) 2022)

[70] An "online platforms" are defined by the DSA as "a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation" (Art. 3(i)).

researchers apply. IXR app stores and marketplace layers likewise fall within platform duties where they host user listings/content. However, currently no IXR platform meets the VLOP threshold.

Digital Markets Act (DMA) (Regulation (EU) 2022/1925)

Scope & Key Definitions

The Digital Markets Act (DMA),[71] which entered into force with the DSA in November 2022, is an ex-ante competition instrument that applies only to undertakings which the European Commission designates as "gatekeepers" for one or more core platform services (CPS); obligations then attach service-by-service to the designated CPS. CPS include online intermediation services (e.g., app stores/marketplaces), online search engines, social networking services, video-sharing platform services, number-independent interpersonal communications services (NI-ICS), operating systems, web browsers, virtual assistants, cloud computing services, and online advertising services provided by a CPS provider (Art. 2). In parallel with the operative text, the Commission has designated initial gatekeepers (Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft) and later added iPadOS (Apple, April 29 2024) and Booking.com (May 13 2024) ("DMA Designated Gatekeepers," n.d.), illustrating the service-specific nature of designation.

Applicability to IXR

In the IXR stack, a headset or spatial-computing OS supplied by a designated gatekeeper is a CPS under the definition supplied by the DMA. However, though Apple and Meta—both IXR companies—are designated gatekeepers, none of their IXR products are listed as designated CPS of concern. Should they be, the DMA imposes significant obligations. Article 5(2) limits cross-service combination and cross-use of personal data absent specific, GDPR-grade consent. Article 6(4) obliges that provider to permit and

[71] (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) 2022)

enable the installation and effective use of third-party apps and third-party app stores, including access paths other than the gatekeeper's own store; Article 6(7) further requires the gatekeeper to expose the same device capabilities—such as cameras, IMUs, hand-/eye-tracking sensors, passthrough and spatial-mapping interfaces—on terms equivalent to its own services, save for narrowly justified integrity/security limits.

Where an IXR provider also runs an XR app store or marketplace as a designated CPS, Article 5(4) prevents anti-steering and thereby protects developers' ability to communicate and conclude off-store offers without charges imposed by the gatekeeper. If the IXR environment includes in-world messaging or voice messages furnished by a designated NI-ICS, Article 7 can compel baseline messaging interoperability on request, reducing communications lock-in for coordination of IXR experiences. And where the same gatekeeper controls multiple relevant CPS across the stack (such as an app store, operating system, and IXR platform), Article 5(2) circumscribes cross-service profiling across the IXR stack absent specific opt-in consent, operating alongside the GDPR; these data-combination limits have been an explicit focus of Commission guidance and proceedings. All of these duties apply only after designation for the specific CPS at issue, which the Commission has been expanding incrementally through formal decisions.

Audiovisual Media Services Directive (AVSMD) (Directive 2010/13/EU),[72] as amended by Directive (EU) 2018/1808)

Scope & Key Definitions

The amended Audiovisual Media Services Directive (AVMSD),[73] adopted in 2018 and implemented by Nation-States by September 2020, coordinates national rules for audiovisual media to protect the public,

[72] (Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the Coordination of Certain Provisions Laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) 2010)
[73] (Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 Amending Directive 2010/13/EU on the Coordination of Certain Provisions Laid down by Law, Regulation or Administrative Action in

particularly minors, and support a functioning single market. It defines "video-sharing platform services" (VSPs): services where the principal purpose—or a dissociable section or an essential functionality—is to provide videos, GIFs, and/or user-generated videos for which the provider does not have editorial responsibility but organizes content (e.g., by algorithms). Article 28b requires "appropriate measures" to protect minors and the public from harmful content and incitement, including flagging systems, age verification, and media literacy measures.

Applicability to IXR

If an IXR platform's principal purpose or an essential functionality is public sharing of user video (e.g., persistent rooms, mixed-reality streams, or short-form VR videos), it may qualify as a VSP. If this is the case, it must implement Article 28b measures proportionate to risks, alongside oversight by the competent media regulator under country-of-origin rules.

Unfair Consumer Practices Directive (UCPD) (Directive 2005/29/EC), as interpreted by the Commission's 2021 Guidance

Scope & Key Definitions

The Unfair Consumer Practices Directive (UCPD)[74] is a full-harmonization regime for unfair business-to-consumer (B2C) commercial practices "before, during and after" transactions. It covers "products," defined as "any good or service including immovable property, digital service and digital content, as well as rights and obligations" (Art. 2). It outlaws misleading/omissive and aggressive practices (Art. 5-9). The

Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) in View of Changing Market Realities 2018)

[74] (Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market and Amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA Relevance) 2005)

Commission's 2021 Guidance[75] confirms that interface "dark patterns"— "a type of malicious nudging, generally incorporated into digital design interfaces" that "distort the economic behavior" of a consumer[76]—can be unfair practices, depending on context and effects on average consumers.

Applicability to IXR

IXR onboarding flows, consent prompts, in-app purchasing and subscription management must avoid materially distorting consumer behavior (e.g., hidden defaults, obstructive cancellation, and manipulative nudge architecture). Disclosures (ads, sponsored placements, influencer content in XR) must be clear and timely in the immersive environment. However, what "dark patterns" look like in IXR has yet to be determined. Enforcement is coordinated through the Consumer Protection Cooperation Network and national authorities (European Commission, n.d.).

Artificial Intelligence Act (Regulation (EU) 2024/1689)

Scope & Key Definitions

The AI Act[77] lays down harmonized rules for the placing on the market, putting into service, and use of AI systems and general-purpose AI (GPAI) models in the EU. It adopts a layered approach: (i) a list of prohibited practices (Article 5) that apply early in the timeline; (ii) high-risk AI duties triggered either because the AI is a safety component of a product covered by specific Union harmonization legislation in Annex I (e.g., machinery, medical devices, and radio equipment) or because the use case is listed in Annex III's list of high-risk use cases (Article 6); (iii) transparency obligations for certain AI, including

[75] (Commission Notice – Guidance on the Interpretation and Application of Directive 2005/29/EC of the European Parliament and of the Council Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market (Text with EEA Relevance) 2021)
[76] (Commission Notice – Guidance on the Interpretation and Application of Directive 2005/29/EC of the European Parliament and of the Council Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market (Text with EEA Relevance) 2021)
[77] (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) 2024)

content-generation/manipulation and emotion recognition (Article 50); and (iv) a discrete regime for GPAI models (Chapter V). Prohibitions apply from 2 Feb 2025, the GPAI and governance chapters from 2 Aug 2025, and most remaining obligations (including Article 50) from 2 Aug 2026.

Applicability to IXR

For IXR hardware and embedded software, the AI Act is impactful when an AI module is a safety component of an Annex I product (for example, a headset within the radio equipment framework or an XR device used as an accessory to machinery or medical devices) and that product is subject to third-party conformity assessment: in such cases, the AI is high-risk and the provider must meet design, data-governance, human-oversight, robustness, documentation, and CE-marking obligations before placement on the market. This is a role- and module-specific analysis keyed to Article 6(1) and Annex I.

IXR features that process bodies and behavior (eye-gaze, facial dynamics, voice) engage the AI Act's prohibitions and transparency layers. In particular, the AI Act bans AI systems that (i) infer emotions in the workplace or education settings (subject to narrow medical/safety carve-outs); (ii) perform biometric categorization to deduce sensitive attributes (e.g., political opinions or sexual orientation); and (iii) create or expand facial-recognition databases via untargeted scraping of facial images from the internet or CCTV. Separately, deployers of AI that generates or manipulates content so that it appears authentic must label or otherwise make such generation apparent to users under Article 50. These constraints are directly relevant to avatar-mediated classrooms, enterprise collaboration in XR, and mixed-reality capture/publishing tools.

Certain platform-side IXR uses can also be high-risk under Annex III—for example, where XR is used in education and vocational training, in employment/worker management, for access to essential services, or for biometric identification/categorization. In those cases, the deployer and provider roles determine who must perform a fundamental-rights impact assessment, implement risk-management and data-governance controls, keep logs, and ensure human oversight, with registration and post-market monitoring for Annex III systems.

Finally, many IXR stacks embed GPAI (e.g., for generative scene/asset creation or multimodal assistants). From 2 Aug 2025, GPAI-model providers must supply technical documentation and other artefacts to downstream integrators; additional duties apply to GPAI with systemic risk. IXR providers that integrate such models must use those artefacts to comply with their own obligations under the Act and adjacent law. The EU AI Act's risk-based approach and focus on fundamental rights align with broader European efforts, notably the Council of Europe's legally binding Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, which seeks to establish common principles across signatories regarding AI, human rights, democracy, and the rule of law (Council of Europe 2024). However, since the Framework Convention is not directly applicable on companies (rather, it obligates states to apply it through their domestic legislative processes), I do not analyze its specific provisions.

Chapter 5: Safety and Privacy in Immersive Extended Reality

Note: This chapter is based on a peer-reviewed journal article published in *Digital Society* (see (Hine, Rezende, et al. 2024)).[78] I have edited it in several ways, including by updating the legal analysis to account for developments in EU legislation and by revising the text to be more cohesive with the rest of the thesis.

5.1. Introduction

In this chapter, I analyze risks to safety and privacy posed by IXR technologies. Safety and privacy are among the most critical aspects implicating the protection of fundamental rights and the quality of experiences in IXR and must be addressed early in the design, deployment, and regulation of IXR technologies. Safety is essential to having a good experience in IXR; privacy issues are relevant to both IXR users and non-users. Furthermore, biometric data collection may be fundamental to IXR platforms' business models and thus must be given special attention. The right to privacy is outlined in Article 12 of the UDHR,[79] while safety is threaded throughout, including in Article 3, which states that "everyone has the right to life, liberty, and security of person." In the context of the Internet, "online safety" has been a significant topic of concern, including in the European Declaration on Digital Rights and Principles for the Digital Decade.[80] Thus, this chapter adopts "safety" as an interpretation of the spirit of the UDHR, following the acknowledgement that, as a security right, "being physically secure is a necessary condition for the exercise of any other right" (Shue 1996, 21–22).

This chapter draws on several rights-related documents. The foundational document is, of course, the UDHR. As a reiteration, to inform and justify EU-focused policy recommendations, this chapter also incorporates the Charter of Fundamental Rights of the European Union ("the Charter") and the

[78] The original article was written in collaboration with Isadora Neroni Rezende, Huw Roberts, David Wong, Mariarosaria Taddeo, and Luciano Floridi. For author statements, see Appendices 1-5. I would like to thank Patrick Grady and two other individuals for commenting on an early version of the original article.
[79] (United Nations General Assembly 1948b)
[80] (European Declaration on Digital Rights and Principles for the Digital Decade 2023)

European Convention on Human Rights (ECHR), which protect many of the same rights as the UDHR but have special, justiciable status within the EU legal order. The ECHR—overseen by the Council of Europe, which continues to develop standards on new technologies and human rights—was directly inspired by the UDHR, albeit limited to civil and political rights (European Parliament 2018). The Charter is also related to the UDHR by being based on the ECHR and Member State law (Equality and Human Rights Commission 2021). These documents help inspire this chapter's conceptualization of "safety" and "privacy."

The importance of safety and privacy is reflected in several EU policy documents that foreground these rights, including the Charter and the ECHR. The EU has also acknowledged their importance in XR and to facilitate other rights. "Online privacy and safety" is a crucial pillar of the EU "Digital Decade" initiative (European Commission 2021), and both are included in the European Declaration on Digital Rights and Principles for the Digital Decade.[81] These high-level goals manifest in a European Parliamentary Research Service (EPRS) report on the "metaverse" (Madiega et al. 2022), which highlights the importance of physical and mental health issues and data privacy, while the July 2023 "EU initiative on Web 4.0 and virtual worlds" recognizes challenges to "personal data and privacy," cybercrime, and cyber violence (European Commission 2023a). The Council of Europe has also directly warned about the possibility of XR technologies to negatively impact individuals' safety and privacy through nudging, manipulation, and harms that fall outside of existing laws (Vinders 2023).

I will turn now to the structure of the chapter. Section 5.5.2 explains my methodological approach. Section 5.5.3 outlines the theoretical conception of safety and privacy grounding the rest of the chapter. Sections 5.5.4 and 5.5.5 use historical VR literature and the most recent wave of XR research to discuss safety and privacy risks in IXR. Section 5.5.6 discusses how parts of the aforementioned EU legislative toolkit succeed or fail in mitigating those threats. Section 5.5.7 concludes the chapter.

[81] (European Declaration on Digital Rights and Principles for the Digital Decade 2023)

5.2. Methodology

This chapter employs an iterative narrative literature review (Jahan et al. 2016). In line with the policy orientation of this thesis, the goal of this chapter is to map the landscape of XR safety and privacy risks, rather than comprehensively classifying or ranking the likelihood of all possible risks. Although less methodologically rigorous than systematic literature reviews, a narrative literature review is thus appropriate and warranted. Notably, they do not require reporting search terms, databases, numbers of results, or inclusion and exclusion criteria. However, I elected to report many of these anyway to maximize research transparency.

The initial search phase, conducted in January of 2023, used Google Scholar's search function to identify relevant articles based on combinations of XR-related terms and privacy and safety keywords. Initial search terms included:

- Extended reality privacy
- Extended reality safety
- Virtual reality privacy
- Virtual reality safety
- Augmented reality privacy
- Augmented reality safety
- Mixed reality privacy
- Mixed reality safety

I read titles and abstracts of returned articles and filtered them for relevance based on whether they substantively discussed privacy or safety related to IXR. Inclusion criteria for risks are those that have manifested in the physical world or existing Internet and are technologically plausible considering the current technological trajectory of IXR, and novel risks that are technologically plausible. As discussed in this dissertation's introduction, articles speculating about more remote or theoretical risks of IXR (such as those relying on yet-to-be-developed technology or not grounded in an accurate understanding of IXR technology and development) were excluded, as discussing these would distract from the policy-oriented goals of this chapter. The search continued until theoretical saturation was reached (Saunders et al. 2018), meaning that no additional risks were being identified. Where appropriate, additional articles and documents were added on an *ad hoc* basis to provide further context to the examples identified in the literature search.

5.3. Conceptualizing Safety and Privacy

Safety has been a concern since the early days of VR development, when studies focused mostly mainly on the physical effects of VR. This made sense when headsets weighed four kilograms and often caused severe discomfort (Wilson 1996; Costello 1997). Now, additional risks are emerging regarding mental safety and social stability. I use a three-part definition of "safety" encompassing physical, mental, and social elements, which is informed by the EU's conceptualization of the term.[82] The rights to physical and mental safety derive from Article 3 of the Charter, and the EU has begun to address these rights in the digital context with measures aimed at ensuring the safety of hardware and software.

Historically, product safety legislation, like the 1985 Product Liability Directive,[83] has focused on preventing physical harm and material damage. Recently, the European Council and Parliament have begun acknowledging the mental aspects of safety in product liability legislation; the revised 2024 Product Liability Directive allows individuals to claim damages for psychological harm.[84] The Digital Services Act (DSA)[85] also includes provisions protecting mental and physical health. It addresses harassment, hate speech, discrimination (Recital 40), and "serious negative consequences to a person's physical and mental

---

[82] In this article, I consider some security-related issues, but only within the context of individual safety. Thus, cybersecurity issues are not central to our analysis. The reader interested in this topic may find the following publications relevant: (Kulal et al. 2022; Abraham et al. 2022; Sethi 2022; Huang et al. 2022; Wang et al. 2022; Chen et al. 2022).

[83] (Council Directive 85/374/EEC of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products 1985)

[84] (Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on Liability for Defective Products and Repealing Council Directive 85/374/EEC (Text with EEA Relevance) 2024)

[85] (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) 2022)

well-being" (Recital 83). It also begins tackling the threat of digital technology to social stability. Although social stability is not construed as a fundamental individual right, because living in a safe and stable society is arguably necessary for proper physical and mental safety, EU legislation works to promote it. One of the DSA's fundamental premises is that diverging national laws on "illegal content, online disinformation, or other societal risks" negatively affect the internal market (Recital 2); it goes on to outline the systemic risks that platforms must address to ensure that fundamental rights are protected, implying that social stability is an important facilitator of individual rights.

In digital contexts, privacy (enshrined as a fundamental right in Article 12 of the UDHR, Articles 7 and 8 of the Charter, and Article 8 of the ECHR) has primarily been viewed in the context of communications and personal data protection (Renieris 2023). However, privacy also encompasses aspects of one's physical being, home, and lifestyle. As an immersive and often embodied experience, IXR brings elements of physical privacy into the virtual domain. It facilitates the flow of information within our broader information environment; in more philosophical terms, IXR tends to lower the ontological friction in the infosphere (Floridi 2005). Thus, it cannot be regulated solely as a matter of data and communications privacy.

In the early days of VR and AR, privacy was often an afterthought or disregarded. Jaron Lanier (the founder of one of the most prominent early VR companies) cautioned: "If there's a total acceptance of the right to privacy, there's also a danger of too much isolation developing in the long term" (Lanier and Biocca 1992). At the same time, some argued that VR would facilitate "strong privacy" through encryption (Friedman 1996). These reflect two aspects of privacy: that of the body or self and that of communications. Recent IXR research—including studies examining privacy in "proto-metaverses" like Second Life (Leenes 2008)—focuses more on data privacy and physical privacy, likely because of increased commercialization since 2010 (Kulal et al. 2022); see (Falchuk et al. 2018; Spiegel 2018; Sethi 2022; Huang et al. 2022; Bavana 2021; Abraham et al. 2022; Martin 2022; Bagheri 2016). I draw on all of these aspects of privacy to provide a comprehensive overview of the risks below.

Unlike safety, privacy lacks a unique EU legislative framework conceptualizing its different aspects in digital contexts. The General Data Protection Regulation (GDPR)[86] offers a framework for data protection. However, privacy concerns in IXR extend beyond data protection. Thus, I adopt Beate Roessler's definition and taxonomy of privacy: "Something counts as private if one can oneself control the access to this 'something'. Conversely, the protection of privacy means protection against unwanted access by other people" (Roessler 2005, 8). This conception of privacy applies across three dimensions, or "possibilities for exercising control over 'access'": informational privacy, decisional privacy, and local privacy (Roessler 2005, 9). It covers data protection, communications, and embodied aspects of privacy, and also corresponds to interpretations of Article 8 of the ECHR,[87] which, according to the Guide on Article 8 of the European Convention on Human Rights ("the Guide"), involves the home (local privacy); correspondence, image and reputation protection, surveillance issues, health information, and data protection (informational privacy); and family life, physical/psychological/mental integrity, and identity and autonomy issues (decisional privacy) (European Court of Human Rights 2022). Roessler's three-pronged definition allows us to simplify my taxonomy while hewing close to the EU context. Table 1: Privacy Breakdown provides a side-by-side comparison of the category of privacy, the part of the UDHR's Article 12 that corresponds to it, and then the ECHR's interpretation from Article 8, as well as relevant language from the Guide.

Table 1: Privacy Breakdown

Roessler Taxonomy	**UDHR Article 12**	**ECHR Article 8/Guide**
Informational Privacy	"Arbitrary interference with his… correspondence"	"right to respect for his… correspondence" • Letters/post • Data

[86] (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) 2016)

[87] Article 8 of the ECHR appears to be inspired by Article 12 of the UDHR, which states that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation" (United Nations General Assembly 1948b).

		• Electronic communication
Local Privacy	"Arbitrary interference with his… home"	"right to respect for his… home" • A place that the occupant has "sufficient and continuous links" to • Business premises
Decisional Privacy	"Arbitrary interference with his… family"	"right to respect for his private and family life" • Contextual; "real existence in practice of close personal ties" • Cohabitation

5.4. Threats to Safety

In this section, I outline the main threats to safety posed by IXR as identified by the narrative literature review. I consider both amplifications of existing harms and those novel and unique to IXR. Not every risk that IXR poses is unique; for instance, any electrical device poses a risk of malfunction. Some of the risks, such as stalking, are translations of those present in the physical world (though note that they are novel in terms of their immersive digital translation). Others, like the potential to encourage alcohol misuse, appear to be unique to IXR. In terms of harm, these distinctions are not particularly important, but in terms of the potential that legislation can or already addresses a specific risk, it is highly relevant, as novel risks are less likely to be considered in policy.

5.4.1. Threats to Physical Body

The physical bodies of users of IXR immersed in a virtual environment are still involved in the experience and thus are potentially at risk. I classify the physical harms of IXR into two categories: incidental and intentional.

Incidental harms arise during the normal use of IXR technology, without any malfunctioning or interference. For instance, "cybersickness" is a well-documented side effect of using VR headsets; symptoms include nausea, headaches, fatigue, and vomiting (Palmisano et al. 2020). Since the 1990s, it has been known to affect women disproportionately (Hayles 1996; Jasper et al. 2020). Potential reasons include increased susceptibility to motion sickness, greater postural instability, and the interpupillary distance (IPD) of VR headsets, often calibrated to the typical male IPD range (Kelly et al. 2023). This is the first example of how IXR disparately affects specific groups, which could be exacerbated if activities in IXR become widely adopted and/or mandatory (for example, in work environments), although techniques are being developed to address it (Ang and Quarles 2023). Regarding acute physical injury, IXR headsets also often obscure users' views of their surroundings, which could cause collisions with nearby objects, pets, or bystanders (Needleman and Rodriguez 2022). IXR devices also often contain electronics close to users' heads, which could cause serious bodily injury or brain damage if malfunctional (Bagheri 2016), although product safety standards seem to have prevented this so far.

Intentional physical harm may follow if devices are hacked to cause malfunction (Wang et al. 2022) or if malicious individuals or applications alter users' perception and lead them into dangerous situations (Abraham et al. 2022). Users could suffer physical harm if they are targeted by other users—for example, by "strobing" or "startling" epileptic or otherwise vulnerable users[88] (Lemley and Volokh 2017). Hacking is already illegal according to laws implemented under Directive 2013/40/EU,[89] but these malicious user actions are an additional avenue in technology-facilitated physical assault.

[88] In the US, an author with epilepsy was targeted with a strobing GIF on Twitter (now X) and consequently suffered a seizure. The perpetrator was charged with aggravated assault, and a judge permitted a lawsuit for battery to proceed despite the "novelty of the mechanism by which the harm was achieved" (Fernandez 2019). Additionally, the Epilepsy Foundation's Twitter account was hacked and used to Tweet strobing GIFs at the account's followers (Fernandez 2019).

[89] (Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA 2013)

5.4.2. *Threats to Mental Health*

Because experiences in IXR trigger the same nervous system and psychological responses as experiences in the physical world (Parsons et al. 2009), psychological harm to users in virtual environments can cause genuine distress and suffering. I consider harms perpetuated by other IXR users before moving on to those perpetuated by IXR platforms and technologies. Some may have associated physical effects, but I categorize them based on their primary impacts.

Online harassment could be exacerbated in IXR because of its immersive nature and the unavoidable presence of identity signals. Physical harassment (bodily interference with an avatar) and verbal harassment are already proving especially problematic in IXR (Outlaw 2018), although Blackwell et al. (2019) also raise the possibility of environmental harassment using the affordances of VR worlds. The Center for Countering Digital Hate identified one violating incident in *VRChat* every seven minutes (Frenkel and Browning 2021). Sexual harassment is especially prevalent, but platforms struggle to proactively address it. Meta and QuiVr only introduced "personal boundary" features after women publicized how other users groped them (Basu 2021). However, Meta's boundary, which was intended to "establish standard norms for how people interact in VR" (Robertson 2022), can now be turned off (Perez 2022). As in the physical world, observable identity signals—e.g., of age, gender, sexuality, race, and disability status[90]—are used to target verbal and physical harassment (Blackwell et al. 2019). A 2018 survey of VR users found that 49% of female respondents had experienced sexual harassment, while 30% of male respondents had experienced racist or homophobic harassment (Outlaw 2018). Stereotyping may be increased because online presentations are generally less nuanced than offline presentations (Axelsson 2002, 198). Thus, individuals' experiences may be significantly worse depending on how they present themselves. In addition to historically marginalized groups, children are another group of concern. If IXR becomes widespread among youth, it could endanger children's mental health by

[90] As noted in Chapter 4, identity markers, especially those related to disability, are not yet available in IXR. Meta's Horizon Worlds has cochlear implants for avatars, but not wheelchairs or canes (Meta Accessibility 2022). Furthermore, although members of the disabled community may be more inclined to use IXR (French 2017), IXR devices are often not accessible for users with disabilities (Stoner 2022), which risks creating a world where members of the disabled community are simultaneously shut out, erased, and subject to increased harassment.

exacerbating the impacts of cyberbullying to resemble physical bullying. 37% of American children ages 12-17 have been cyberbullied (Patchin 2019), but children rarely talk to adults about bullying online (Reed and Joseff 2022).

The subsequent three concerns are more speculative, but grounded in plausibility. IXR offers a new avenue for cyberstalking (Sethi 2022; Falchuk et al. 2018; Canbay et al. 2022). Stalkers embodied in avatars could make their targets feel even more threatened due to the feeling of physical presence. Cyberstalking causes real psychological damage (Chemaly 2014) and can spill into the physical world (potentially utilizing AR functionalities to track people), endangering physical and mental safety.

IXR could open new avenues for financial and identity fraud, causing emotional and dignitary damages (Merritt 1989) via "social engineering hacking" (Falchuk et al. 2018) and other kinds of phishing.[91] Avatar identity theft could enable impersonation and fraud (Wang et al. 2022), but also inflict emotional trauma if users identify with their avatars (Madary and Metzinger 2016).

Concerningly, deepfake avatars or characters in immersive experiences may be used as "non-consensual virtual sexbots" (Kalpokas and Kalpokienė 2023, 100) or in highly realistic "revenge pornography." Revenge pornography is currently created using non-immersive deepfake technology, but immersive revenge pornography is likely to follow (Kalpokas and Kalpokienė 2023, 105). Exploiting "body-to-avatar rendering data"—or simply clever design—could create deepfake avatars for an even more violating kind of revenge pornography (Kalpokas and Kalpokienė 2023, 100). Approximately 98% of existing deepfake videos are pornographic, and 99% are of women (Home Security Heroes 2024). This could create situations where deepfake avatars perform vulgar or defamatory actions in widely accessible VR spaces (or projected in AR). Deepfake pornography could cause victims emotional harm and reputational damage, creating both acute and long-term harms.

[91] There have been many scams related to non-fungible tokens (NFTs) and cryptocurrencies, which are often associated with IXR, but are not inherent to it. However, how property and intellectual property rights will function in IXR have yet to be settled. The fact that digital goods could be delinked from purchased NFTs (Marinotti 2022) and that platforms may retain the copyright to everything created in the platform (Bagheri 2017) could create insecurity that harms users, even if they are not subject to scams or deceptive purchases.

Moving on to harms facilitated by IXR platforms and technologies themselves, IXR could exacerbate psychological disorders. Traditional social media has been linked to eating disorders and self-harm (Turner and Lefevre 2017; Jacob et al. 2017), with an especially grave impact on children and teenagers (Wells et al. 2021). Since images have a greater potential to trigger self-harm than text (Jacob et al. 2017), immersive pro-self-harm or eating disorder content (or immersive environments promoting harmful behavior) could feasibly be even more dangerous, but should be researched more.

Another under-investigated issue is how IXR could encourage alcohol misuse. There is a body of literature on how VR can be used to assess and treat alcohol use disorders (Ghiţă and Gutiérrez-Maldonado 2018), but thus far, no studies on how it could exacerbate alcohol misuse. However, anecdotal reports suggest that the nightlife—which in reality is 24/7 because of IXR's global nature—in some social IXR platforms, especially *VRChat*, encourages people to drink while physically alone, even to the point of alcohol poisoning (The Virtual Reality Show 2022; Visual Venture 2023). Some people report that VR causes them to drink more and that it is difficult to know how drunk they are when sitting down wearing a headset (The Virtual Reality Show 2022). In IXR, excessive consumption of alcohol may be perceived to be safer because specific physical hazards, like driving, are removed, but it introduces new risks. While IXR may not directly cause these problems, how it can promote alcohol abuse should be investigated.

While it is more speculative, there is evidence that IXR could trigger psychological disorders based on its potential for unhealthy engagement and addiction. Such addiction is seen in 2D gaming (WHO Team 2020). Studies of compulsive VR use are limited but suggest that addiction rates are currently similar to traditional gaming and social media use but that the affordances of VR positively predict addiction, meaning that as embodiment and immersion increase, so too might addiction (Barreda-Ángeles and Hartmann 2022). It is also hypothesized that using biometric data to target and refine experiences could increase engagement and addiction (O'Brolcháin et al. 2016). Clinically, "gaming disorder"[92] and depersonalization and derealization dissociative disorders are associated with 2D gaming

---

[92] In 2018, the WHO designated "gaming disorder" as a diagnosable disorder that causes "significant impairment in personal, family, social, educational, occupational or other important areas of functioning" (WHO Team 2020).

(WHO Team 2020; De Pasquale et al. 2018) and could be more prevalent in IXR. Subclinical "video game addiction" can also be harmful (Digital, Culture, Media and Sport Committee 2019), and readjustment difficulties have been reported when exiting virtual worlds (Spiegel 2018; Madary and Metzinger 2016). Additionally, online games can encourage excessive spending, particularly by children and cognitively disabled users (Kleinman 2019). In immersive contexts, AR advertising has been shown to increase customers' willingness to pay (Pozharliev et al. 2022). An immersive context may also add a sense of "unreality" (virtualization or gamification) of financial consequences. Together, these factors can create harmful consumption environments that consumers are not adjusted to.

Compulsive IXR use can also have physical effects in addition to mental and financial ones. Bodily neglect is associated with gaming addiction, and parents suffering from video game addiction have neglected their own physical health and their children's (Spiegel 2018). Furthermore, people in fits of "gamer rage" have injured or killed children (Madary and Metzinger 2016). While these issues are not unique to IXR, they could be exacerbated if IXR proves to be more addictive than traditional online interactions.

Children's vulnerability extends beyond cyberbullying and bystander impacts, as IXR may interfere with children's development and well-being. Exposure to sexually explicit media in early adolescence is related to risky sexual behavior in early adulthood (Lin et al. 2020). Already, IXR platforms host adult content. Age gating measures are often ineffective—a reporter discovered children in a virtual strip club displaying explicit content (Campoamor 2022)—and IXR's immersive and interactive nature could endanger children. Minors have reported being groomed and forced to perform virtual sex acts (Crawford and Smith 2022). There could also be subtler impacts on development. Children in a VR experience displayed worse impulse control than children using two-dimensional video (Bailey et al. 2019), and VR can implant false memories in children (Segovia and Bailenson 2009), although the long-term effects of this are unknown. Children tend to perceive conversational agents—even disembodied ones like Amazon's Alexa and Apple's Siri—as "alive" (Lovato et al. 2019), but treat them as "servants" and use tones not appropriate for interpersonal communication (Bylieva et al. 2021).[93] Future research should investigate whether IXR could lead to harmful, parasocial relationships and how that could affect children's ability to function in physical society or disrupt kinematic development (Miehlbradt et al. 2021).

The final issue in this section is platforms' direct manipulation of users' psychological states. Tactics similar to those used in the Facebook "emotional contagion" experiment, where the platform manipulated users' emotional states by tweaking the amount of positive and negative content in their news feeds (Del Vicario et al. 2016), could influence users' moods and behaviors. That impact could be amplified using biometric tracking, emotion capture, and brain-computer interfaces (O'Brolcháin et al. 2016). While experiments are permissible under specific ethical principles (Polonioli et al. 2022), informed consent cannot be obtained via a clause buried deep in the terms of service (Koops 2014), which would significantly violate user autonomy.

5.4.3. Threats to Social Stability

Threats to social stability can be split into three categories: threats to social order, security, and democracy. Though it requires further study, the large-scale impacts of some of the issues mentioned above could affect social order. One deserving special attention is the normalization of harassment. Harassment in social IXR experiences risks creating a society on- and offline where specific people do not feel welcome and could become more widespread and harmful than in the traditional Web, as embodied identity markers are more accessible to observe in IXR. While changing an avatar's identity signals can mitigate harassment, it comes at a cost to the freedoms of personality and expression of the victim. If harassment becomes normalized like toxic behavior has in the gaming community (Beres et al. 2021), IXR could create a virtual community that embeds and encourages bias and discrimination against already-marginalized communities, which could then increase such bias and discrimination across the

[93] This could be a problem for adults as well; men have created chatbot "girlfriends" and then proceeded to verbally abuse them (Bardhan 2022). In addition to the concerning possibility that online abuse could transition offline, the broader psychological implications of human-AI relationships—which are increasing—should be further studied (Kalpokas and Kalpokienė 2023, 66).

Internet (Schmitz et al. 2022) and in the physical world (Chan et al. 2016). All this would further exacerbate the digital divide within communities.

IXR presents novel, albeit unrealized, security risks via the unique opportunity for extremist recruiting (O'Brolcháin et al. 2016; Doctor et al. 2022), training (Wang et al. 2022), and indoctrination (Madary and Metzinger 2016). Groups such as ISIS already use traditional social media for recruiting (Awan 2017), and just as the US Navy has found VR effective for recruitment and training (Chang 2018), so might terrorist groups. Furthermore, immersive environments could act as a "virtual office" facilitating coordination between individuals who may be prevented from traveling by sanctions or conflict. Terrorists could use IXR to build AR or VR training scenarios, perhaps using a "digital twin"—a highly realistic digital replica—of a potential target (Doctor et al. 2022; World Economic Forum 2022), putting people at risk of injury and even death in an attack.

Like social media, IXR, if widely adopted, could destabilize democratic institutions by altering our perception of reality and interactions with each other. Social media has been linked to political polarization (through both exposure to partisan content and uncivil political exchanges) and the spread of mis- and disinformation, negatively impacting the stability and norms of political institutions (Tucker et al. 2018). IXR could exacerbate both problems through "Reality Distortion Filters" (Zallio and Clarkson 2022). Instead of selecting what content you scroll past on a social media screen or what ads you see on a sidebar, algorithms could select what billboards you see, what objects appear around you, and what other avatars you encounter, whether in a virtual context or augmenting the physical world. The latter includes the potential for AI-powered avatars—what Rosenberg (2022a) calls "elves" but here I dub "artificial avatars"—that, similar to video game non-player characters (NPCs) exist in the virtual context but are controlled by the platform itself. These interactions could be continuously adjusted based on the users' micro-reactions, offering a potentially potent tool of persuasion (Rosenberg 2022c). In traditional social media, one can easily access content beyond what is targeted to them. However, targeting in IXR could result in two avatars in the same virtual or physical location seeing completely different things. When, say, one user sees advertisements for one soft drink, and another sees advertisements for a different soft drink, this could be relatively innocuous, but when one is surrounded by content promoting a conspiracy theory and the other is not, there is a concerning incongruity, difficult to monitor, that endangers both users. Resolving political differences becomes even more difficult when users do not know that their baseline realities may differ. The entire immersive reality can become individually tailored; polarization thus transcends users' social media feeds to pervade their perceived realities.

5.4.4. Conclusion

This section has discussed the safety threats of IXR, including incidental and intentional threats to the physical body; threats to mental health caused by other users, IXR technologies, and IXR platforms; and threats to social stability through impacts to social order, security, and democracy. Particularly concerning are the increased threats to vulnerable groups, including children, who are more susceptible to harms in immersive environments and from using immersive technologies, and individuals of marginalized identities, who are less likely to be able to access IXR and more likely to be harassed within it. Possible mitigations will be discussed in Chapter 7.

5.5. Threats to Privacy

Roessler's taxonomy describes privacy violations as "illicit surveillance," "illicit interference in one's actions," or "illicit intrusions in rooms or dwellings" (Roessler 2005, 9). In IXR, I will be considering virtual actions and dwellings in addition to physical ones, but this does not make violations any less concerning. In some ways, the potential infringements are more severe because surveillance can be built into the fabric of IXR itself.

5.5.1. Informational Privacy

Informational privacy is the "right to protection against unwanted access in the sense of unwanted interference in personal data about themselves" (Roessler 2005, 9). "Personal data" refers to information about oneself, as well as control over one's self-presentation and the "right to be left alone" and not have every action, even in public settings, scrutinized, in order to facilitate an "authentic life" (Roessler 2018, 138–39). Informational privacy issues are not unique to IXR; however, the biometric data that IXR devices can collect magnifies privacy and data protection issues.

IXR devices and platforms can collect an enormous amount of biometric data relating to an individual's physical, physiological, or behavioral characteristics. While I will primarily discuss how this impacts individual privacy, data collectors can aggregate and anonymize such data using so-called "privacy-enhancing technologies" before using them to derive insights about human behavior for the same ends as individual data collection (including for targeting and personalization), creating concerns for group privacy (Renieris 2023, 105; Floridi 2017). IXR devices can track physical movements like facial expressions, eye movements, gestures, gait, and posture; breathing patterns; voice and faceprints; haptic responses; and environmental data like location, background, and surrounding noise or visuals (Pahi and Schroeder 2022). Because many IXR platforms are partly, if not primarily, funded by advertising, they can exploit biometric data to target advertisements through a process dubbed "biometric psychography" (Heller 2020). Tracking can be embedded in platform operation, which has been called "surveillant physics" (McStay 2023) and facilitates a "[totalization] of surveillance" (Kalpokas and Kalpokienė 2023, 21–22). Meanwhile, biometric data can be aggregated to create an individual, identifiable "kinematic fingerprint" (Spiegel 2018). While much of these data are generally considered non-identifiable, as Schroeder (2010, 235) predicted, these data are so complete that users can be uniquely identified with high accuracy based on just seconds of IXR movement data (Nair et al. 2023), meaning that conceptions of personal and non-personal data require revision. The GDPR definition of biometric data only covers data that can uniquely identify an individual and offers face and fingerprints as examples (Article 4). However, as technology advances, so do identification techniques. Since pieces of otherwise non-identifiable data can be aggregated to uniquely identify individuals, most data "relating to the physical, physiological or [behavioral] characteristics of a natural person" (Article 4 GDPR) could be considered biometric data under the GDPR.[94]

Besides revealing an individual's identity, biometric data and other XR data can infer sensitive or protected characteristics (Abraham et al. 2022; Bagheri 2016), including health conditions such as Alzheimer's disease (Fristed et al. 2022), and monitor affective state and cognitive processes (Abraham et al. 2022), which builds on surveillance concerns. Some suggest that eye tracking and voice analysis can reveal information about identity, personality, emotions, drug consumption, socioeconomic status, and health (Kröger et al. 2020). While the scientific robustness of many of these technologies is questionable (Roberts 2022), they could have ramifications in the physical world. If, for example, a person working in a homophobic environment was inferred to be gay from biometric data or behavioral observation in IXR (Rupp and Wallen 2007; Logan 2018), disclosing that information—regardless of its accuracy—could cause professional ramifications. Moreover, misleading inferences based on incorrect data could cause adverse discriminatory or health outcomes, speaking to the importance of facilitating user access to their personal data.

Awareness of constant surveillance may limit how comfortable people feel expressing themselves in IXR and their ability to explore different identities. Users may conceal some private information, but one's biometric data and involuntary reactions cannot be concealed from platforms (Heller 2020). Surveillance can have "chilling effects" where individuals self-censor behavior, which impacts freedom, creativity, and self-development (Solove 2006). For example, after revelations about the US National Security Agency's (NSA) mass surveillance emerged, Internet traffic to sensitive Wikipedia articles decreased (Penney 2016).[95] This empirical evidence shows that individuals need to be aware of

[94] It should be noted that, at the lowest level of abstraction, fingerprints and retina scans are also essentially just collections of datapoints. This analogy could be expanded to "kinematic fingerprints" as well.

[95] Issues related to biometric data straddle the line between informational and decisional privacy, but I chose to categorize them under informational privacy because they relate more to general surveillance concerns. Issues associated with the monitoring of avatar actions, however, will be discussed under decisional privacy because the primary impact of that surveillance is deterring certain actions.

surveillance for it to have a chilling effect. Studies indicate that IXR users are often unaware of how many data are collected about their activities and interactions in IXR (Abraham et al. 2022), partly because of terms and conditions designed to keep them uninformed (O'Brolcháin et al. 2016). However, as the post-NSA chilling of Wikipedia traffic suggests, once users become aware of the existence and extent of data collection, they may modify their behavior, possibly becoming less willing to use avatars that accurately represent their identity, engage in specific activities, or to use AR devices in specific places. In addition to covert surveillance, overt interrogation can also cause behavioral chilling. Interrogation could involve excessive requests for user information by the platform—either on signup or during use—or users badgering others with personal questions. If users feel pressured to provide information, even if they refuse, it is still a discomfiting invasion of privacy (Solove 2006), and children may be more prone to oversharing personal information (Reed and Joseff 2022). Overall, chilling effects will impact everyone uncomfortable with surveillance, but especially those who need to keep some aspect of their identity private, including activists and people exploring their identity.

Surveillance can also be performed by other IXR users, workplaces and schools, and hackers. Like stalking, individuals in IXR could follow others around virtual worlds and observe their activities. Alternatively, they could exploit technological means, such as the "bugs" used in the Second Life platform to monitor others' conversations (Leenes 2008) or recording functionalities (Blackwell et al. 2019), some of which might be built into the platform. If people work in IXR environments (such as Meta's *Horizon Workrooms*) or use work-provided devices (such as an AR device to provide guidance in a warehouse), employers could monitor employees' physiological data and use it in performance evaluation—for example, using eye tracking as a proxy for attention—and hiring or firing decisions (Madiega et al. 2022). The same could be done for online schooling, extending surveillance into private virtual and physical spaces. The resulting biometric datasets represent a treasure trove for hackers, who could access stored biometric data or IXR equipment, including recording devices used for motion capture (O'Brolcháin et al. 2016). This creates new opportunities for identity theft, blackmail, and other fraud. Furthermore, the sensitivity of biometric data means that its breach would be uniquely damaging to users' physical and mental safety, as they would know that they are more vulnerable to identity theft and other ramifications, and that a platform entrusted with their data—or, worse, one that collected it surreptitiously—had allowed it to leak (Solove 2006).

5.5.2. Decisional Privacy

Decisional privacy concerns the freedom from unwanted interference in decisions and actions (Roessler 2005, 9). It covers privacy of the body, personal relations, and decisions regarding them (Roessler 2018, 139), all of which relate to IXR.

An issue related to, but distinct from, individual biometric data privacy is the privacy of avatar movements, specifically, where an avatar goes and when, as well as who they choose to interact with, or with whom they are sharing an experience. Using a Web browser together, for example, to watch a movie or do some shopping, does not present the same risk. People often choose to be anonymous online using private browsers and/or anonymous profiles to explore aspects of themselves that they wish to keep private (Lauri and Farrugia 2020). However, currently, there is no "incognito mode" in IXR, even if no identity verification is required, because biometric data can link "burner" avatars to the owner's primary account and even to their physical person. Therefore, a platform and other interested parties can always determine where an avatar or person goes and how they behave, threatening user autonomy and self-expression. Regulations like the UK's Online Safety Act requiring age verification to access "harmful" content exacerbate this (Ball 2025), particularly when age verification is implemented in a non-privacy-preserving way. This demonstrates some of the tensions between safety, privacy, and freedom of expression; while safety can theoretically be ensured by full surveillance of everything done and said in virtual spaces, we would reject this (even if technically feasible) because of the infringement on privacy that it would entail.

Another threat to autonomy is the possibility of platforms using individual micro-reactions to "nudge" users to take actions or make decisions they would not otherwise have (Rosenberg 2022c).

Regardless of the significance of the decision made, this kind of artificial influence via feedback loop is an enormous violation of individual decisional privacy and autonomy, especially when it exploits knowledge of personal preferences—potentially inferred from IXR data—that makes people more "nudgeable" (de Ridder et al. 2022). Violations could also result from automated decision-making using IXR data. For instance, employers could monitor attentiveness using eye-tracking data and feed it into an employee's annual review. Regardless of whether such data leads to accurate inferences about individuals (Roberts 2022), the algorithms used to make these inferences may be biased against specific groups. For example, facial recognition historically performs poorly for women and people with darker skin tones because training datasets are often skewed towards men and people with lighter skin tones (Buolamwini and Gebru 2018), and thus they may have worse outcomes in these assessments (Pahi and Schroeder 2022). Decisional privacy enshrines the idea that individuals should be free to make decisions about their lives and bodies as they see fit, but IXR could subject users to automated decision-making that infringes on that.

5.5.3. Local Privacy

Local privacy is the right to have a space where one can "do just what [they] want, unobserved and uncontrolled." It involves solitude and the protection of family communities and relationships (Roessler 2018, 140). While this has historically only applied to the physical world, people will need the same protection in immersive worlds because the same concerns about observation and lack of privacy apply in IXR, if not even more so. Just as in physical reality, people in VR may desire a virtual space where they can be alone or limit who else can access it, such as the "estates" of the non-immersive virtual world *Second Life* (Leenes 2008). A failure to see such spaces commonly implemented could lead the entire IXR to become a "global village" where everyone's business is public (O'Brolcháin et al. 2016). That said, even the implementation of spaces providing privacy from other users would not be truly private if users still feel subject to platform surveillance.

This surveillance also threatens physical local privacy. One would not feel comfortable at home if they knew that their every movement was being recorded and datafied. This scenario is an actual concern, as IXR devices gather information about the user's environment, including data about one's physical space (e.g., their home, office, or wherever they are using the IXR devices) and about bystanders, whose personal and biometric data could then be collected without their knowledge (Pahi and Schroeder 2022).[96] Just as inferences can be made about individuals based on their online data footprints (Wachter and Mittelstadt 2019), data about physical locales could be used similarly. While some degree of physical local privacy can be achieved by shutting off IXR devices, during use, platforms and hardware manufacturers can compromise the local privacy of IXR and the local and informational privacy of other individuals.

IXR threatens not only the privacy of users' virtual and physical spaces but also their relationships in those spaces, implicating group privacy (Floridi 2017). One's communications with others could be observed in IXR, but biometric data could facilitate more subtle invasions. Researchers in a Stanford class held in VR used biometric data to infer information about group dynamics and relationships between users (Stanford HAI 2022). The same could be done based on observing an individual's interactions with bystanders not using IXR. The IXR environment is never fully detached from the physical space within which it is experienced. Any interactions in the physical space, e.g., words exchanged with a co-worker who enters the office, may also be shared in the IXR environment.

5.5.4. Conclusion

This section has outlined the possible privacy infringements of IXR, expanding beyond the traditional notion of privacy as data protection—although biometric data privacy is a major concern in IXR—to consider decisional and local privacy. IXR opens new avenues for surveillance and persuasion, in the

[96] This is similar to Facebook's "shadow profiles," which are datasets collected by Facebook about the web browsing activity of non-Facebook users (Aguiar et al. 2022).

physical and virtual worlds. How extant EU legislation may address these concerns is the topic of the next section.

5.6. Applicability of EU Legislative Toolkit

Existing EU legislation may mitigate some safety and privacy concerns outlined above. I consider the applicability to IXR of six areas of relevant legislation drawn from the horizontal toolkit outlined above. While other areas of sectoral legislation may apply to specific IXR applications, I focus here on more broadly pertinent legislation based on my analysis of the specific risks inherent to IXR. In the field of consumer protection, I primarily examine the DSA, as it is intended to protect people in the face of technological developments. Other pieces of consumer protection legislation, such as those prohibiting deceptive advertising, unfair commercial practices, and unfair consumer contracts, will also apply to IXR. However, there is not enough evidence that IXR creates enough unique issues in these areas to justify the inclusion of these regulations here (Madiega et al. 2022; Maciejewski 2023); future work should investigate whether and how they may be implicated.

5.6.1. Product Safety Legislation

Legacy and new product safety legislation will apply to IXR equipment, like headsets. The General Product Safety Regulation[97] (GPSR) notes that "[n]ew technologies might pose new risks to consumers' health and safety or change the way the existing risks could materialise" (Recital 21), indicating that the GPSR is attentive to the novelty of IXR and could help address some of the physical, mental, and even some social safety impacts of IXR technology. The NIS2 Directive supports this, requiring Member States to include cybersecurity training in their national cybersecurity strategy (Article 7(2)(f)). "Essential

[97] (Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on General Product Safety, Amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and Repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (Text with EEA Relevance) 2023)

and important entities," which include online marketplaces, search engines, and social media platforms, will have to ensure that network and information systems are secured, and implement and oversee cybersecurity risk management measures (Article 11), helping prevent informational privacy harms related to data breaches.

Regarding other legislation, the revised Product Liability Directive[98] aims to protect user safety by addressing liability for software (including AI systems) and digital services, including those provided by online platforms. Although currently untested, it will allow individuals to claim damages not just for physical injury, but also for "medically recognised harm to psychological health," which could apply to harms caused by IXR platforms. It would also hold software companies responsible for harms caused by the updates (or lack thereof) or learning capabilities of their products (De Luca 2023). However, while it eliminates the €500 threshold for claimable property damage, it does not provide a remedy for social harms or damages to mental health that do not rise to the threshold of "medically recognized."

The AI Liability Directive,[99] which was withdrawn in in February of 2025 (European Commission 2025a), would have also been potentially useful for addressing some of the possible safety harms of IXR. This Directive would have protected victims whose privacy or safety has been harmed by AI, which many IXR platforms will likely utilize for content moderation and creation, among other purposes. It would have also created rules for accessing evidence to establish damages and relieve claimants from directly proving that the system's lack of compliance directly caused the damages suffered, which is beneficial given the opaque nature of many AI systems. These measures would have helped ensure that individuals are not harmed further by data exclusion that would impede their case and enable just outcomes when safety has been violated. Though this was a promising Directive, any future version of this proposal must also address the "information gap" so that individuals actually know when they have been harmed by an automated system (Ziosi et al. 2023).

---

[98] (Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on Liability for Defective Products and Repealing Council Directive 85/374/EEC (Text with EEA Relevance) 2024)

[99] (Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive) 2022)

5.6.2. General Data Protection Regulation (GDPR)

It is unclear how effectively the GDPR will apply to IXR and protect informational, decisional, and local privacy. The European Parliament briefing on the metaverse acknowledges that the distinction between a data controller and data processor (Articles 24-28) will become blurred, which raises questions about where to collect user consent (Articles 6-7) and display privacy notices (Articles 12-13), especially if data collection will be "involuntary and continuous" (Madiega et al. 2022).

Additionally, because VR platforms will have users from across the world intermingling in a shared space, the questions of jurisdiction and data transfers become difficult, although adequacy decisions between the EU and third countries can partially solve the data transfer conundrum. Since a privacy law "jurisdiction selection clause" likely would not hold up (Artzt 2022), this could lead to a powerful Brussels Effect where platforms default to the strongest mandated protections, depending on how specific clauses of the GDPR are interpreted.

Article 6 provides different legal bases for personal data processing, including "consent," but also the "performance of a contract" (Article 6(1)(b)) and pursuing "legitimate interests" of the controller or a third party, unless "overridden by the interests or fundamental rights or freedoms of the data subject" (Article 6(1)(f)). When applied to targeted advertising, these bases are controversial. The European Data Protection Board (EDPB) ruled that the contract clause cannot be used to justify targeted advertising,[100] prompting Meta to shift to the "legitimate interests" clause (Meta Newsroom 2023). However, when TikTok tried to switch from consent to "legitimate interests" as a basis for targeted advertising, the Italian Data Protection Authority ruled that TikTok's "legitimate interests" were not sufficient to justify processing for targeted advertising (Lomas 2023; Italian Data Protection Authority 2022). Shortly after this ruling, Meta also switched to consent as its legal basis for targeted advertising, citing how the Irish Data Protection Commission "is now interpreting GDPR in light of recent legal rulings, as well as

[100] ("Binding Decision 3/2022 on the Dispute Submitted by the Irish SA on Meta Platforms Ireland Limited and Its Facebook Service (Art. 65 GDPR)" 2022)

anticipating the entry into force of the Digital Markets Act" (Meta Newsroom 2023). One justification for the "legitimate interests" basis as a user-friendly method of processing was that it required users to be able to opt out of the processing (Bryant 2023), providing additional protection to users should it be implemented effectively, but this was inadequate to the data protection authorities. Together, these would seem to indicate the necessity of more active user involvement to consent to targeted advertising, including in IXR.

Although the GDPR's consent regime seemingly creates a highly legitimate justification for processing, issues have emerged, with consent dialogues often presenting information deceptively and exhausting users with their quantity (Utz et al. 2019)—so-called "cookie fatigue" (Talus 2023). Thus, when presented with an ostensibly valid consent choice, users could end up involuntarily consenting to more or different data collection than they intended to. Because of the different affordances of IXR environments compared to traditional Web ones, new consent mechanisms will be necessary, and for optimal user privacy and outcomes, they must be designed to avoid similar issues.

Processing biometric data "for the purpose of uniquely identifying a natural person," as well as processing data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership" or data regarding one's health, sex life, or sexual orientation (Article 9(1)), is also banned unless explicit consent has been obtained (Article 9(2)(a)). As previously argued, some IXR biometric data can be aggregated to uniquely identify a person, so this article likely applies; platforms would thus be required to obtain consent in order to process it. This clause might protect bystanders from having their data collected and used to create "shadow profiles," but this could be clarified.

Among the exceptions to the processing restrictions, IXR platforms may try to leverage the exception permitting nonconsensual processing of "personal data which are manifestly made public by the data subject" (Article 9(2)(e)). The "manifestly made public" clause has little legislative guidance surrounding it (Dove and Chen 2021), but high-level guidance requires it to be "construed strictly and as requiring the data subject to deliberately make his or her personal data public" (EU Agency for Fundamental Rights 2018, 162). However, platforms might argue that an individual occupying a virtual or physical public space while using IXR devices makes at least some of their biometric data public, which could give platforms *carte blanche* to process it and identify people. While this argument may be reasonable when applied to, say, the appearance of an avatar, extending it to body-based biometric data collected by IXR equipment becomes more concerning. It likely could not be applied to internal biometric measurements like blood pressure or heart rate. Still, platforms could argue that avatar movement data or movement data while using an AR device are public. However, while one's movements are technically observable in public in the physical world, one does not expect them to be constantly monitored (Schroeder 2010, 235). Observation at the level of an IXR platform—which could record precisely where a person or avatar goes, who it interacts with, the details of those interactions, and how the user's body is moving—is far more privacy-invasive.

Article 20, which establishes the right to personal data portability, could create a right to interoperability by proxy, allowing users to transfer their personal data from one IXR platform to another. However, this would require new data standards for IXR-specific data. If realized, this could enable users to "vote with their feet" and transfer their data to another IXR platform if they do not like the practices of a given platform. This would not, however, establish standards for digital purchases and NFTs, because although transaction data may qualify as personal data, the digital items themselves likely would not.

As previously discussed, DPIAs may be mandatory for IXR—which would help pre-emptively protect user privacy. Participants can object to certain processing (Art. 21), and where decisions with "legal or similarly significant effects" are based solely on automated processing, including profiling (say, automated exclusion of protest avatars from "public squares"), Article 22 supplies an additional set of safeguards.

Enforcing rules and laws in IXR will significantly impact user safety. Under Article 22, data subjects have the "right not to be subject to a decision based solely on automated processing" which produces "legal effects" or "similarly significantly affects" them (Article 22(1)). This would preclude purely automated content moderation and rule enforcement in IXR, unless subject to explicit consent, a contractual necessity exception, or a "rights and freedoms" exception (which could be quite likely).

One promising ruling for user privacy came in the CJEU's *OT v Vyriausioji tarnybinės etikos komisija*,[101] which found that the processing of personal data that could *indirectly* reveal "sensitive information concerning a natural person" is subject to the Article 9(1) prohibition on processing when it could identify the person (unless an Article 9(2) exception applies) (O'Shea 2022). As aggregated and non-personal data falls outside the GDPR's purview, this ruling could protect IXR users from having sensitive inferences made about them without their knowledge, although they remain vulnerable to the use of anonymized or synthetic data based on data to mine behavioral insights at a group level (Renieris 2023, 120). This could then be used to target content, train surveillance technology, or otherwise refine the surveillant physics and extractive behavior of IXR platforms (McStay 2023), facilitating large-scale invasions of privacy (Renieris 2023, 84–88).

Other potentially relevant rulings include the State Commissioner for Data Protection Lower Saxony's decision to fine a company €10.4 million for video-monitoring its employees over two years and retaining recordings for up to 60 days at times (LfD Lower Saxony 2021), and the Deliberação/2021/622 of the Portuguese DPA,[102] which ruled that using proctoring software to monitor students via browser, camera, and facial analysis violated their privacy rights. This will augment the AI Act's designation of workplace and educational AI monitoring systems as high-risk. Together, they hold promise for curtailing employee and student monitoring because surveillance in IXR could be even more comprehensive than video recordings (Martin 2022), and would include even more of the biometric analysis that the Portuguese DPA objected to.

[101] Judgement of 1 August 2022 (OT v Vyriausioji tarnybinės etikos komisija 2022).
[102] ("Deliberação/2021/622" 2021)

5.6.3. ePrivacy Directive

The ePrivacy Directive[103] is highly relevant to IXR, particularly data privacy, because devices store biometric and other sensitive information, including metadata automatically generated by users' interactions with the platform. Article 5 of the ePrivacy Directive requires service providers to maintain the security of services and confidentiality of information and gain explicit consent to store or access information on a device. Consent is not required when this is strictly necessary for the service. Though the ePrivacy Directive offers some protection to data stored on IXR devices, it does not cover data once it leaves the device. In this case, data could be transmitted to another entity for non-essential (i.e., commercial) purposes, provided the GDPR consent regime is also satisfied.

This data could also be subject to national data retention legislation, albeit with certain constraints. Article 15 of the ePrivacy Directive allows Member States to derogate from confidentiality requirements and retain data for specific security objectives (e.g., combating serious crime and ensuring national security). The Court of Justice of the European Union (CJEU) ruled that the unfettered retention of metadata, for a limited timeframe, is proportionate only to address genuine and foreseeable threats to national security.[104] Fighting other serious crimes only justifies retaining data with a specific link with a threat to public security.[105] The limits set by this jurisprudence, and the boundaries between the concepts of *national* and *public* security, are still subject to discussion (Eskens 2022; Mitsilegas et al. 2023). Therefore, without clear definitions for valid security threats, it may be challenging to hamper the expansion of surveillance based on IXR data retention,[106] especially considering the aforementioned possibility of using IXR to facilitate terrorism.

---

[103] (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) 2002)

[104] CJEU, La Quadrature du Net and Others v Premier ministre and Others, judgment of 6 October 2020, joined cases C-511/18, C-512/18 and C-520/18, §136.

[105] Id., §144.

[106] However, generalized access to content data would be irreconcilable with the essence of the right to privacy; see CJEU, *Maximillian Schrems v Data Protection Commissioner*, judgment of 6 October 2015, Case C-362/14, §94. Given the sensitivity of the inferences possible from IXR metadata, their retention would not comply with the proportionality principle.

The proposal for an ePrivacy Regulation[107] would have expanded privacy rules to electronic communications services such as WhatsApp (and presumably messaging in IXR environments) and guarantee the confidentiality of communications content and metadata (European Commission 2022b). The law would unambiguously cover machine-to-machine communications (Recital 12), protecting the transmission of IXR data generated outside the context of interpersonal communications. Adopting the ePrivacy Regulation would help protect communications and other data from interception, but it was withdrawn in February of 2025 alongside the proposed AI Liability Directive (European Commission 2025a).

5.6.4. Digital Services Act

The DSA may impact how IXR platforms deal with illegal content and targeted advertisements, aiding physical and social safety. The DSA was intended to create a safer digital sphere, protect fundamental rights, and unify regulation and enforcement. It establishes a "notice and action" system for removing illegal content, with platforms required to establish mechanisms for users to report illegal content (Article 16) and to prioritize responses to "trusted flagger" entities who detect illegal content (Article 22). Additionally, under the "Regulation on addressing the dissemination of terrorist content online" ("Terrorism Regulation"),[108] terrorist content must be removed within one hour. However, due to the pan-jurisdictional nature of IXR, determining the audience for which content must be removed could be difficult (Hine 2023). Removing content that violates a specific jurisdiction's regulations for a version of a social media website based in that country or for users of a website geo-located to that country does not significantly impact the use of that site for users; it is merely another piece of information that they may or may not encounter on a static, two-dimensional feed of content. When users from different jurisdictions are encountering content that violates laws in one of their jurisdictions but not the other,

[107] (Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 2017)

[108] (Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online 2021)

and those users are contemporaneously co-existing in the same virtual space, the question of content moderation becomes much more difficult. Removing the content for all users is simpler, but risks reducing all content available in IXR to the lowest common denominator and violating other users' freedom of expression and access to information; this will be discussed further in the next chapter. Removing it for only users in locations where it is violative is technically more difficult and also undermines shared reality, as discussed above (Hine 2023).

The DSA bans ads targeted at minors (Article 28) and based on sensitive characteristics (Article 26), although how this applies to inferred characteristics is unclear. Ads should display in real time the advertiser, sponsor, and how the ad is targeted (Article 26). This may be difficult to implement in IXR, where ads may not be static experiences on a sidebar or within a feed. IXR advertising is instead much more like advertising in the physical world. While some ad formats, like those in the pages of a (physical or virtual) magazine lend themselves to this kind of disclosure, transient ads, like billboards glimpsed from a moving car or ads displayed on a moving vehicle, do not. Thus, clarification of how ad disclosures should work in immersive settings will be required. However, if implemented effectively, Article 26, combined with the requirement that "very large online platforms" (VLOPs) and "very large online search engines" (VLOSEs) keep a user-accessible repository of ads (Article 39) could help protect user autonomy by informing them about how they are being targeted. It is worth stressing that if information is obscured or users cannot easily access the ad repository, the DSA may face the same problems as the GDPR's consent regime. The requirement that platforms not impair users' ability to make "free and informed decisions" through manipulative design (Article 25) is also intended to protect user autonomy. This accompanies Recital 67, which clarifies that this includes "dark patterns." While the EDPB has issued guidelines on recognizing dark patterns on social media platforms,[109] they will have to be adapted to account for immersive environments. This could be facilitated by Article 40, which requires that VLOPs allow vetted researchers access to data for research on systemic risks, or the proposed Digital

[109] ("Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them" 2022)

Fairness Act, which is intended to address dark patterns from a consumer protection perspective in 2026 (European Parliament 2025).

While the DSA offers promising protections for users, many of its requirements, including annual systemic risk analysis (Article 34) and independent compliance auditing (Article 37), only apply to VLOPs and VLOSEs. This risks creating a regulatory blind spot for "risks disseminated by platforms below the VLOP-threshold" (Laux et al. 2021) of 45 million monthly active EU users, meaning that IXR platforms—none of which currently meet the threshold—could slip through the regulatory cracks and cause significant harm.

5.6.5. Digital Markets Act

The Digital Markets Act (DMA)[110] has some implications for IXR privacy insofar as IXR platforms act as markets. Article 5 prevents gatekeepers from non-consensually combining personal data from their core platform service with data from other services or third-party sources and from cross-using personal data from the gatekeeper's other services (Article 5(2)). This may prevent specific informational privacy harms by hampering platforms from creating larger aggregated datasets and mining them for behavioral insights. The European Commission will have auditing powers to ensure compliance (Article 23). However, the DMA faces the same scope issues as the DSA as it only applies to large companies (Article 3(2)), meaning that smaller platforms could still combine and cross-use data in concerning ways.

5.6.6. Artificial Intelligence Act

The Artificial Intelligence Act (AI Act)[111] will impact how AI systems can be used in IXR because the definition of an "AI system" includes those that influence "virtual environments" (Article 3). Its primary

[110] (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) 2022)
[111] (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013,

relevance to safety and privacy comes in how it deals with biometric identification. While the banning of real-time biometric identification in public spaces was much debated, in the end, it was implemented only for law enforcement—not for private companies—with exceptions so broad they could become the rule (Article 5(1)(h), (2)). Additionally, this ban would only apply to physical spaces (Recital 19). Therefore, while AR devices could not generally be used for real-time identification in physical spaces by law enforcement—although I will discuss this further in the next chapter—biometric identification could still be done in virtual environments with similar effects.

However, other clauses may offer more privacy protection in IXR. Emotion recognition systems will be banned in places of education and work, which could provide a foundation to ban them in corresponding IXR environments (Article 5(1)(f)). Moreover, the use of biometric categorization systems that categorize people based on biometric data "to deduce or to infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation" is banned (Article 5(1)(g)). This could limit profiling using IXR biometric data, although it does not apply to "lawfully applied biometric datasets" in law enforcement (Article 5(1)(g)). However, biometric categorization based on "sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics" is permitted as a high-risk system (Annex III(1)(b)), implying that profiling based on protected characteristics that are not "race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation" (such as sex, age, and nationality) is permissible.

The AI Act could be relevant to other uses of AI in IXR. Systems that could subliminally distort human behavior in ways that cause "significant harm" will be banned (Article 5(1)(a))). This could offer protection from manipulation in IXR, but it depends on how "significant harm" is interpreted. While emotion recognition in workplaces and educational institutions will be banned (Article 5(1)(f)), AI systems that monitor worker performance (Annex III(4)(b)) and student behavior during assessments (Annex III(3)(d)) are permitted, albeit classified as "high-risk." All permissible biometrics-based systems

(EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) 2024) are also high-risk (Annex III(1)), and scraping facial images from the Internet or CCTV footage for facial recognition databases will be banned (Article 5(1)(e)), but scraping non-facial biometric data or using an AR device to capture data in real-time would be permitted. This creates informational and decisional privacy risks through the possibility for chilling effects.

5.7. Conclusion

In this chapter, I have outlined the risks to safety and privacy in IXR and analyzed how extant EU policy may mitigate—or fail to mitigate—these risks. Some of these risks already exist in the physical or digital worlds but could be exacerbated by IXR, while others are novel. Many will disproportionately impact marginalized and disabled users, who should receive particular consideration. I do not presume to have covered all risks, but I hope my proposed policies may provide a flexible basis to address emergent risks.

Harmonization will be necessary in the governance of IXR because it involves companies and users from across the globe. Regardless of the ultimate approach, there are tensions that will have to be considered when contemplating how to safeguard fundamental rights, such as trade-offs between safety and freedom of expression. It is these rights that will be the topic of the next chapter. Although the rights in question are different, what remains the same is that regulation will have to carefully consider how to balance conflicting rights.

Chapter 6: Assembly and Expression in Extended Reality: Transposing Human Rights Across Realities

Note: This chapter is based on a peer-reviewed journal article published in the *Interactive Entertainment Law Review*,[112] which itself was based on a paper presented at the 2024 conference "Towards a Responsible Development of the Metaverse" at the University of Alicante (see (Hine, Cowls, et al. 2025; 2024)). I have revised it in several ways to bring it in line with Chapter 5's format, including adding EU legal analysis, foregrounding the methodology, and shifting the human rights framework discussion to Chapter 8.

6.1. Introduction

This thesis now continues its exploration of RQ2 and RQ3, turning from safety and privacy to two other rights: freedoms of assembly and expression. As privileges rather than multital rights (Hohfeld 1917), these are rights that can be actively exercised by individuals—and also infringed upon by the platforms that control how individuals can exercise those rights. Because of the increased similarities of experience to the physical world, there is a heightened, though not novel, responsibility for platforms to uphold human rights. This chapter discusses the risks and benefits of XR to the freedoms of assembly and expression, then analyzes the applicability of six areas of EU legislation. In this chapter, as with the previous chapter, I focus on "immersive extended reality" (IXR) (Hine, Rezende, et al. 2024), which includes XR applications where the user's visual field is wholly mediated by a device. Other sensory experiences, such as audio and haptics, may accompany this. This includes "immersive" VR and AR applications but excludes non-immersive applications, such as smartphone AR. This chapter also fits into the UDHR-based framework, relying on Articles 19 and 20 for its high-level definition of freedoms of assembly and expression.

[112] The original article was written in collaboration with Josh Cowls and Luciano Floridi. For author statements, see Appendices 1 and 2.

The realism of IXR also increases the likelihood of it being used to augment or replace events in the physical world, such as concerts held in VR spaces (Nwanji 2024) and AR enhancing gaming experiences in the physical world (Signorelli 2018). As the technology advances, it is likely that its cross-cutting use in the physical and virtual spheres will intensify. In 2022, the first "metaverse" protest was held in the *Decentraland* virtual world protesting consumerism outside the Samsung virtual headquarters (Garrity 2022; Macaraniag 2022), and activists have made banned books available on proto-metaverse[113] platform Minecraft ("The Uncensored Library – Reporters without Borders," n.d.). While this would seem to indicate that these technologies can help enable free assembly and expression, they also create obstacles and risks. Because of the immersion, presence, and interactivity that makes VR experiences more like those in the physical world (Mütterlein 2018), human rights can be exercised more like they can in the physical world, and this, plus the potential for AR to interweave into the physical world, means that the possible impact on people from their restriction or abuse is correspondingly greater, in turn creating greater responsibilities for platforms to protect these rights.[114]

My analysis is informed by the idea that IXR is a fundamentally mediated reality, as discussed in Chapter 3. In particular, devices, hardware manufacturers, and platform companies stand between individuals and their experiences of IXR. As a result, these factors define the technological and platform affordances that impact people's IXR experiences. They also define who can access IXR, potentially creating a new digital divide both by erecting cost barriers and by making others unable or unwilling to use it because of unmet accessibility needs or negative experiences. While private companies exert control over freedom of expression on their platforms and contribute to "new-school" speech regulation (Balkin 2014), in IXR, they influence a broader range of rights, similar to how governments have power over rights—and thus a responsibility to protect them—in the physical world. This is particularly pronounced when considering rights like the freedoms of assembly and expression, which, as privileges rather than multital rights (Hohfeld 1917), are traditionally the purview of governments to protect.

---

[113] Proto-metaverses are connected spaces where users can interact that do not depend on XR technology (Ball 2022).

[114] I primarily address commercial applications of IXR, but governments are increasingly adopting IXR for different purposes, giving them the responsibility to uphold human rights within their country's national contexts as well.

Through two semi-systematic literature reviews, this chapter first synthesizes a taxonomy of freedoms of assembly and expression in XR based on existing sources, then analyzes the scant available literature on those rights in XR, laying the groundwork for Chapter 8's discussion of how businesses, governments, and civil society groups can conceptualize private-sector responsibilities for upholding human rights in IXR.

This chapter considers assembly and expression as distinct but complementary rights. In the Western democratic context, the two have separate histories but are co-constitutive (Hamilton 2020; Salát 2015, 5–7; 2015, 10–19). Verbal and symbolic expression often occurs *within* or *during* assemblies, but assemblies can be expressive actions in and of themselves by conveying a message about a group and a cause, even if no words are spoken. This was displayed in the 2024 Russian presidential election when the late dissident Alexei Navalny called for Russians to show up at polls and cast their ballots at noon on the final day of voting (Faulconbridge and Osborn 2024). Even without explicit protest in the form of speech, placards, or other actions, the participants still conveyed a message of solidarity and implicit protest.

The remainder of the chapter proceeds as follows. Section 6.2 outlines the methodological approach of the chapter. Section 6.3 lays out the risks and benefits to freedom of assembly; Section 6.4 does the same for freedom of expression. Section 6.5 discusses the applicability of the toolkit introduced at the beginning of this section to the freedoms of assembly and expression; Section 6.6 concludes.

6.2. Methodology

To identify existing articles about freedoms of assembly and expression and XR, I used a semi-systematic literature review (Wong et al. 2013; Snyder 2019). Semi-systematic reviews are effective when "wanting to study a broader topic that has been conceptualized differently and studied within diverse disciplines" or to "combine perspectives to create new theoretical models" (Snyder 2019), as is the case here. I searched Google Scholar in late February and early March of 2024 for the following search terms, with no date restrictions:

- (“virtual reality” OR “augmented reality” OR “mixed reality” OR “extended reality” OR metaverse) AND “freedom of assembly”
- (“virtual reality” OR “augmented reality” OR “mixed reality” OR “extended reality” OR metaverse) AND “freedom of expression”
- (“virtual reality” OR “augmented reality” OR “mixed reality” OR “extended reality” OR metaverse) AND “freedom of speech”

My inclusion criteria were:

- Peer-reviewed paper, chapter, or conference paper
- Dealt substantially with XR and freedom of assembly or freedom of expression
- Written in English
- Full access possible

The search proceeded to theoretical saturation (Low 2019), meaning that I continued the search until results were not adding any relevant information. Table 2 includes full search terms and number of results obtained for each search.

Table 2: Search terms and number of results for freedoms of assembly and expression

Search Term	**Number of Results**
(“virtual reality” OR “augmented reality” OR “mixed reality” OR “extended reality” OR metaverse) AND “freedom of assembly”	388
(“virtual reality” OR “augmented reality” OR “mixed reality” OR “extended reality” OR metaverse) AND “freedom of expression”	8,720

("virtual reality" OR "augmented reality" OR "mixed reality" OR "extended reality" OR metaverse) AND "freedom of speech"	6,690

While I started with over 15,000 results, only 9 papers were identified that met all inclusion criteria. Many papers discussed XR topics only tangentially. The papers were heavily (though not exclusively) US- and First Amendment-centric, covering general freedom of expression in the "metaverse" (Fornasier 2024), VR (Bagheri 2016), and AR (O'Hagan et al. 2023); content moderation in XR (Hine 2023); terroristic content in VR video games (Hupf 2014); obscenity (Zenor 2014); child sexual abuse material (Wagner 2019; Esposito 2018); and legal issues raised by location-based non-immersive AR games (Signorelli 2018). These sources are referenced throughout the chapter when relevant topics are discussed. Where necessary, these were supplemented with auxiliary sources.

To create taxonomies of the freedoms of assembly and expression, I conducted a second semi-systematic literature review. Sources were obtained from Google Scholar in March of 2024 and identified based on the following search pattern:

- "freedom of [expression/speech/assembly]" + "types of [expression/speech/assembly]"
- "freedom of [expression/speech/assembly]" + types of [expression/speech/assembly]
- "freedom of [expression/speech/assembly]" + theory

Table 3: Search terms and number of results for taxonomy search

Search Term	**Number of Results**
"freedom of assembly" + "types of assembly"	49
"freedom of expression" + "types of expression"	1,880
"freedom of speech" + "types of speech"	6,700
"freedom of assembly" + types of assembly	28,800

“freedom of expression” + types of expression	271,000
“freedom of speech” + types of speech	304,000
“freedom of assembly” + theory	26,700
“freedom of expression” + theory	284,000
“freedom of speech” + theory	445,000

The number of sources returned from each search is available in Table 3: Search terms and number of results. While these search terms may not be exhaustive, they provided an overview of theoretical and taxonomizing work on the topic at hand. Inclusion criteria were:

- Peer-reviewed paper, chapter, conference paper, or book
- Provided a taxonomy or other breakdown of the right in question
- Written in English
- Full access possible

The search again proceeded to theoretical saturation. Eleven sources were identified that met all the inclusion criteria. Books were considered in this search because of the existence of several books intended to provide a general overview of a specific right, which included breakdowns of the rights in question. These sources were supplemented by the UN General Comments nos. 34 (United Nations Human Rights Committee 2011) and 37 (United Nations Human Rights Committee 2020) on the rights to freedom of opinion and expression and the right to peaceful assembly, respectively, as these documents provide insight into global interpretations of the specific rights. While these documents specifically discuss the International Covenant on Civil and Political Rights (ICCPR), the ICCPR and UDHR are two of the three parts of the International Bill of Human Rights; the ICCPR is an implementing treaty of the UDHR and its phrasing for the relevant rights is substantially similar (OHCHR, n.d.-b). Thus, it is broadly relevant in the context of the UN and global human rights and appropriate to leverage to support interpretations of the UDHR. However, the ICCPR has not been ratified by as many countries as the UDHR has, hence the dissertation's framing around the UDHR as a whole.

6.3. Risks and Benefits to the Freedom of Assembly

Article 20 of the UDHR states that "[e]veryone has the right to freedom of peaceful assembly and association. No one may be compelled to belong to an association" (United Nations General Assembly 1948b). In the context of the ICCPR, the UN has recognized that the right to assembly extends to private and public spaces, as well as online (United Nations Human Rights Committee 2020), meaning it also applies in IXR. Based on sources from the literature review, I consider how IXR could be used to reshape the *time*, *place*, and *manner* of assembly, including in public and private spaces both physical and digital (Salát 2015; Stamps 1942; Hamilton 2020). These three fundamentals are often the locus of state restrictions on the right of individuals to assemble (Salát 2015, 1). Rather than attempting to elucidate every possible type of assembly, using this level of abstraction (Floridi 2008) helps foreground benefits and impacts, focusing on the embodied aspects of assembly rather than expressive content, which will be covered in Section 6.6.4. While some jurisdictions primarily protect expressive assemblies and consider public and private assemblies differently, in this chapter, I adopt the definition from Salát's book *The Freedom of Assembly: A Comparative Study*, which takes a wider view of assembly as "contemporaneous common presence of at least two persons in a common space" (Salát 2015, 7), in keeping with my jurisdiction-agnostic approach. My analysis will first assess the logic of restrictions in the physical world, then identify possible benefits to virtual and, if applicable, physical assembly, followed by possible risks, in each of the three aspects examined.

6.3.1. Impacts on Time

Restrictions on the timing of assemblies vary by jurisdiction, but motivations include protecting the sanctity of special days, preserving public order (such as by restricting the frequency of disruptive assemblies), and suppressing dissent around sensitive events (such as elections (Burrows et al. 2024)) (Salát 2015, 194–99). These are less relevant for fully virtual assemblies, as the atmosphere of the physical-world holidays and events meant to be protected by these restrictions need not be factors in IXR. In fact, IXR could enhance freedoms of assembly and expression by allowing for assemblies during forbidden times in a way that amplifies a group's message in a way that would not be possible due to physical world restrictions (e.g., if the assembly is about the holiday itself). Additionally, fully virtual IXR assemblies allow for spontaneous assemblies ranging from gatherings with friends to protests because no travel time is involved. This can be accomplished via VR avatar assemblies or with AR projections of people and messages.

VR and AR devices also offer intriguing possibilities for *post facto* engagement with both physical and virtual assemblies by "recording" them for later participation, as with a Minneapolis-St. Paul Black Lives Matter protest ("Behind the Scenes of 'IN PROTEST' with Alton Glass and Adam Davis-McGee," n.d.). This can facilitate research and education, creating a participatory historical record that could enhance understanding of assemblies and their dynamics.

However, these potential benefits are far from assured, owing to the mediating role of XR platforms, which can arbitrarily and illegitimately restrict the timing of assemblies, whether through onerous permitting or notification regimes, or simply by encoding restrictions on how many avatars can be in proximity to each other. They could also prohibit specific assemblies from forming at any time through arbitrary moderation enforcement if, for instance, there was a cause the platform disapproved of or saw as too controversial. Many kinds of assembly are controversial, but in "content-neutral" regimes, governments cannot prohibit assemblies based on their content (Salát 2015, 59–69). Thus, sometimes assemblies that might be offensive to the general public are permitted by law to go ahead, such as the Nazi march planned in Skokie, Illinois in 1978 (*National Socialist Party of America v. Skokie* 1977). This runs contrary to the terms of service of many platform companies, which often ban groups that center around white supremacist topics; Reddit banned thousands of subreddits for promoting hate speech (worstnerd 2020), while Facebook also bans similar groups (Meta Transparency Center, n.d.).

While I accept that traditional social media platforms can legitimately restrict expression,[115] in the embodied context, there is often greater tension between human rights and the goals of content moderation, which will be further explored in this and subsequent chapters.

6.3.2. Impacts on Place

The reasons for restricting restrictions in specific places are more varied than those for time. Some are similar, such as upholding public order and the sanctity of specific spaces, but there are also additional restrictions on where assembly can occur, such as to protect privacy, public property rights, or the "managerial function" of government (Salát 2015, 255–82). The degree to which this logic translates into IXR depends on the function of virtual spaces. For instance, if city services are provided in a specific VR space or "office," as Seoul plans to do through "Metaverse Seoul" (Seoul Metropolitan Government 2023; "Metaverse Seoul," n.d.), or if platform administrative functions take place in defined spaces, similar arguments for restricting assembly nearby may apply, although platform affordances could make assemblies less disruptive. However, this raises questions about the legitimacy of both the restrictions and the entity issuing them. Not all countries restrict assembly around government buildings, so if governments attempt to do so in IXR, they will potentially be applying more restrictive assembly standards to people who are not physically located in their jurisdiction. While states can apply their laws to anyone, citizen or not, *physically* within their borders, the virtual and transnational nature of IXR raises jurisdiction and thus legitimacy questions.

Other physical world logic may translate into virtual IXR assemblies. Safety concerns could still apply, not necessarily out of concern for bodily harm, but to prevent people from being verbally or emotionally harassed. Platforms may also have an interest in restricting assembly around private virtual

[115] Laws in Florida and Texas that would have effectively forestalled content moderation were both remanded to lower courts by the US Supreme Court, with Justic Kagan's majority opinion indicating that the laws were likely unconstitutional but ultimately ruling that the lower courts had not adequately assessed First Amendment implications (*Moody v. NetChoice, LLC* 2024). The Texas case was in turn remanded from the court of appeals to the district court (*NetChoice vs Paxton* 2024). After an amended complaint and was filed in the *Moody* case, the state of Florida filed a motion to dismiss the case, but as of 1 September 2025, no ruling had been issued on the dismissal (Marchese 2023).

property or significant spaces. However, some of this could be mitigated by the affordances of IXR, which could keep people from interacting with an assembly through, for example, avatar invisibility or teleportation, or by blocking it out altogether.

When looking at virtual assemblies themselves, there are clear benefits regarding place. Similar to time, there is no need to travel for a virtual gathering, meaning that individuals and groups from across the world who otherwise would not be able to assemble can participate in a more embodied way. Beyond increasing the number of assemblies a person can participate in, IXR assemblies could have environmental benefits by obviating the need for travel. IXR assemblies are also more accessible, lowering the cost of participation for all and decreasing barriers to access for individuals with physical disabilities (provided XR equipment is accessible, which is not a given (French 2017)). For demonstrations and other expressive public assemblies, organizers could leverage mediation by crafting the surrounding environment to promote the message of the assembly. This could be done with AR in physical assemblies to augment, for example, a speaker's talk. AR could also guide people or enhance communication in mass gatherings.

However, like time, place is vulnerable to platform interference. Platforms could encode arbitrary place restrictions in VR settings or interfere with the appearance of surroundings for different users. This is also a risk in physical, AR-enable gatherings. Additionally, some jurisdictions have objected to people assembling to play AR games and moved to prevent such assemblies (a form of restriction that was ruled to be unconstitutional in the US (Signorelli 2018)). Existing IXR platforms may have to deal with similar attempted restrictions.

6.3.3. Impacts on Manner

The "manner" of assembly can refer to the use of symbolic expression, noise pollution, and aesthetic harm (Salát 2015, 200), but will be expanded here to cover the general means and character of assembly. Restrictions aim to mitigate the impacts of these factors on other people, but the way they translate into

IXR varies. In virtual assemblies, no physical destruction is possible, which may be a benefit for other people who use the platform—depending on the rules of the world, any "destruction" could be instantly repaired—but a drawback for, say, protestors, who may want to leave a physical footprint as a marker of their group action. Similarly, other people in a VR environment could potentially block out the sight or sound of an assembly, which would render a protest, rally, or individual speaking to a crowd irrelevant. Symbolic expression could still cause offense to others who opt to see it (or are unable to opt *not* to see it, if the platform does not allow for blocking of this kind), but the use of masks to conceal identity is largely moot (Salát 2015, 227). Virtual avatars can be changed at will, concealing identity from other participants and bystanders, but platforms can link avatars to accounts and possibly physical-world identities, meaning there may only be limited privacy possible at virtual assemblies.

Despite these potential drawbacks, IXR seems to be opening new possibilities for assembly. For instance, a demonstration was held in *Horizon Worlds* in 2023 to protest what participants perceived as Meta prioritizing its own events over those of the creator community (TheRodParticle 2023). Notably, one user claimed this was the first protest he had ever been to out of fear for his safety in the physical world, indicating that VR may be able to increase participation in political assemblies (TheRodParticle 2023).

There are also potential transformative effects for physical assemblies. AR could provide a new avenue for dynamic symbolic expression projected onto other participants" AR devices without the need to bring the physical symbols—whether on placards, uniforms, or other forms—to an assembly. This speaks to other ways AR could enhance assembly, from private gatherings of friends to public mass gatherings, whether by aiding navigation (Phandroid 2013), recording (Apple 2023), or overlaying information about one's surroundings (Davis 2023). Organizers or law enforcement equipped with AR image recognition devices could also identify weapons and banned or protected symbols.

Such practices create privacy concerns through the extension of AR image recognition to facial recognition. While footage of protests has been analyzed after the fact to identify and target individual protestors (Loucaides 2024), law enforcement doing live facial recognition could lead to the real-time targeting of protestors. Already, it is possible to link non-AR "smart glasses" to publicly available face databases to identify strangers on the street (Hill 2024), and Meta is reportedly planning to include facial recognition natively in future iterations of its smart glasses (Huang and Perloff 2025). This risk to human rights is what led the EU to ban real-time biometric identification for law enforcement in *physical* spaces in the new AI Act,[116] but it is still permitted in many other jurisdictions. Virtual spaces could also facilitate similar biometric recognition, which would not be banned under the AI Act or in other jurisdictions. This constant observation and corresponding threat of interference may create a chilling effect that makes people less likely to participate in virtual protests, especially considering the extensive data trail left in IXR that could be obtained by law enforcement via court order (Hine, Rezende, et al. 2024). Although the *physical* impact of preventing an avatar from participating in a virtual protest would be less than detaining a person, the psychological impact on the individual and social impact on the protest may be similar.

This admittedly depends on whether virtual protests are as effective as physical ones. Virtual protests could turn into a new form of "clicktivism," a coin termed to describe the act of clicking a button to sign an online petition (Halupka 2014), which raised concerns that it would supplant physical activism (Morozov 2024). Although the true impact of clicktivism on activism is debated (Halupka 2014), virtual protests could potentially supplant physical world activism as a less politically effective alternative. While real people committing their time to an assembly would seem to preserve the essence of what makes an assembly consequential, platform and avatar mediation means that people could feasibly send an avatar to attend without being present themselves, similar to how Google is integrating an AI-powered "attend for me" function into its product suite (Google Workspace Blog, n.d.). Furthermore, some assemblies are dependent on bodily presence in a physical space, such as the series of pro-Palestinian encampments established at universities across the globe in the spring of 2024 (Gleeson 2024). Their message is tied to

[116] (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) 2024)

the physicality of the encampments and protestors and would thus be less effective in a virtual setting. While virtual assemblies offer the opportunity to overcome practical obstacles of time and place, as well as state restrictions on the same, their ephemeral footprint and lower barrier to entry imply that virtual protests and other forms of public expressive assembly may be more accessible yet less effective.

The possibility of physical violence is why the right to assembly was not legally recognized outside the US (where it was linked to the right to petition) until the mid-19th century (Salát 2015, 11). Even today, only "peaceful" assembly is protected, and many time, place, and manner restrictions aim to reduce the possibility of violence.[117] Virtual assembly, which reduces the possibility of physical violence, may eventually cause us to reconceptualize assembly or see it evolve into something else altogether, just as it grew out of the right to petition. Physical assembly may be affected by IXR technologies but will still retain its essential character. Incorporating IXR technologies into physical assemblies can help augment the experience for participants, but also create concerns about biometric observation by law enforcement and interference by platforms. While virtual assembly is not precisely the same as physical assembly, the similarities—as well as the potential for IXR-enabled physical assembly—require protection, especially considering the UN's acknowledgment that online assembly is deserving of protection. In the next section, I will discuss the implications of IXR for freedom of expression.

6.4. Risks and Benefits to the Freedom of Expression

Freedom of expression is a complex and nuanced subject. The UDHR's Article 19 states that "[e]veryone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers" (United Nations General Assembly 1948b). The phrase "through any media and regardless of frontiers" would seemingly include IXR within the scope of the right; indeed, the UN

[117] This standard is sometimes but not always applied to freedom of expression, although it is more difficult to determine its scope. For instance, incitements to violence are not protected in most jurisdictions. However, hate speech is criminalized in the EU but protected by the First Amendment in the US (Douglas-Scott 1998; Peršak 2022).

interprets it to include “electronic and internet-based modes of expression” (United Nations Human Rights Committee 2011, 34), but what qualifies as protected speech—including online and possibly in IXR—varies from jurisdiction to jurisdiction (Bagheri 2016). Still, the Council of Europe echoes the UN, emphasizing in its Recommendation CM/Rec(2022)13 that freedom of expression applies fully in the digital environment and calling on states and platforms to protect it against undue interference, including through algorithmic systems and content moderation practices (Committee of Ministers 2022).

Based on sources from the taxonomy literature review, I categorize expression as “commercial,” “political,” and “other,” which includes both “controversial” and “non-controversial” expression (Barendt 2007; Scanlon 1978; Guinn 2005; Zeno-Zencovich 2008). While in some cases there may be overlap with freedom of assembly, this section focuses on the purpose and content of expression, which also covers the expressive content of assemblies while separating it from the modality of assembly discussed in the previous section. I will again first look at potential benefits, then risks.

6.4.1. Impacts on Commercial Expression

VR and AR are already being used in commercial expression in a variety of contexts. AR is used in non-immersive contexts to bring static physical advertisements to life and to showcase advertiser content through filters (Heller and Bar-Zeev 2021), like Snapchat’s Sponsored Lenses (Business Help Center, n.d.). AR has also been combined with e-commerce to show potential customers how an IKEA product would fit in their home or a Nike shoe look on their feet (Heller and Bar-Zeev 2021; Future Stores 2024 2024; Ayoubi 2017). These non-immersive examples provide precedent for immersive AR advertising applications, which would make them even more immersive and potentially involuntary. Companies including Meta—and reportedly Apple—are developing AR glasses, meaning that this will become increasingly relevant as the technology advances (Pritchard 2025; Meta Emerging Tech, n.d.).

VR advertising also takes several forms, including those similar to the physical world (e.g., virtual billboards (Schmälzle et al. 2023)), immersive equivalents to traditional web advertising (e.g., video pre-roll ads (Oculu Video Platform 2014)), and branded experiences or events (e.g., immersive franchise experiences, virtual product placements, and virtual spokespeople (Heller and Bar-Zeev 2021; Rosenberg 2022a)). The sale of virtual goods can also be construed as advertisements for a brand's physical goods, exemplified by luxury brands' sale of non-fungible tokens (NFTs) during the "Web 3.0" boom (Berardo 2024).

However, these technologies could compromise individuals' autonomy by becoming overly coercive and nudging. Immersive, mediated contexts make advertising disclosure, required in many jurisdictions, extremely difficult: how does a platform notify an individual that a person or avatar near them only appears to be wearing a branded shirt because that brand paid for it (Rosenberg 2022a)? These scenarios raise questions about the nonconsensual distortion of reality, both virtual and physical, and the possible infringement on individual freedom of expression if their bodies and property are used in effect as advertising canvases. Other risks of IXR advertising include misleading experience marketing (where the virtual representation of a product or experience is doctored), inducing artificial emotions, targeting consumers in a vulnerable state, and emotional manipulation through hyper-personalization (Mhaidli and Schaub 2021). Many of these risks implicate consumer protection and unfair commercial practices legislation that vary by jurisdiction. While these advertising practices could be construed as permitting corporate freedom of expression, they could infringe on individual autonomy and decisional privacy (Rosenberg 2022a; O'Hagan et al. 2023; Hine, Rezende, et al. 2024), and (along with other manipulative techniques) be thought of as a violation of the freedom to "hold opinions without interference" as mentioned in Article 19 of the UDHR (United Nations General Assembly 1948b).

6.4.2. *Impacts on Political Expression*

IXR may offer new ways to engage in political campaigns. For instance, Indian Prime Minister Narendra Modi has appeared in physical places as a hologram (Welch 2014); a similar strategy could be employed in VR or with AR devices. Furthermore, AR could augment political speeches or debates, and VR could allow for immersive attendance from afar. As mentioned above, government-owned IXR platforms could also serve as places for government services and thus may be places where political expression is restricted. IXR may also be a place where government employee expression is restricted, such as how the UK requires civil servants to remain politically impartial (GOV.UK, n.d.), which would restrict their ability to participate in political expression in IXR.

As discussed above, IXR can facilitate physical protests and create new modalities of virtual protest that could promote political expression, although it may also create a new form of "clicktivism" that decreases the efficacy of virtual political expression. Furthermore, political expression in IXR is also subject to the whims of the mediating platform, which could restrict specific individuals, media outlets, or movements; social media platforms have already been accused of targeting critical newspapers for decreased content distribution (Morrow 2024). Platforms have a commercial incentive to disallow specific forms of speech to remain palatable to their userbase. This is why, even though hate speech is not illegal in many jurisdictions (including the US), many platforms nonetheless ban it. However, there are often discrepancies between what is allowed on a platform and local laws, such as *lèse-majesté* (offense against the state or head of state, illegal in parts of Southeast Asia (Holmes 2022) and Europe (Zimmerman 2021)) or LGBTQ+ expression (criminalized in various forms in Russia, Uganda, and multiple other countries (Wareham 2023; Hine 2023)). While content can be restricted on country-specific versions of social media platforms, the international nature of modern VR platforms makes localized content restrictions more difficult (Hine 2023; Fornasier 2024). This may lead to states pressuring IXR platforms to remove otherwise permissible content on threat of restriction or banning, which they may accede to in order to preserve their market share (Hine 2023). This threatens not only individual freedom of expression, but also the right to "receive and impart information and ideas." If content is restricted more widely than is legally necessary, then both the expressor and those rendered unable to access their ideas suffer.

Whatever decisions platforms make about what expression is permissible can trigger further political expression by users that leverages the platform itself, as seen in the aforementioned *Horizon Worlds* protest that was protesting Meta's own policies. If IXR platforms end up being community-governed, a possibility I discuss more in Chapter 8, political participation may become normalized and widespread as in the physical world, rather than one-off events.

6.4.3. Impacts on Other Expression

Other forms of expression include what here I dub "controversial expression," which is often *not* protected by different countries' interpretations of freedom of expression, and expression that is non-commercial and not explicitly political, which *is* protected to various degrees in different jurisdictions.

6.1.1.1. Controversial Expression

Cases under the umbrella of "controversial expression" involve unprotected expression in jurisdictions that otherwise protect expression from interference, such that it can be regulated by the state even in relatively unrestrictive regimes. Thus, although there is overlap with political expression, there is less agreement on its permissiveness. Some of this expression is criminalized in some or many jurisdictions; much of it is prohibited on existing online platforms. Controversial expression can be categorized based on normative coherence and legislative thresholds. Some expression is universally agreed to be illegal (such as child sexual abuse material (CSAM)), while other lacks such agreement (such as Holocaust denial). Within these, some issues have strong substantive convergence in legislation—either near-universal criminalization or agreement on how other countries should regulate it—while others lack such agreement (Internet & Jurisdiction Policy Network 2021); see Table 4: Matrix of controversial expression regulation, adapted from the Cross-Border Content Moderation Toolkit (Internet & Jurisdiction Policy Network 2021) for a matrix outlining examples of each.

Table 4: Matrix of controversial expression regulation, adapted from the Cross-Border Content Moderation Toolkit (Internet & Jurisdiction Policy Network 2021)

	Universal agreement on illegality	**No universal agreement on illegality**
Agreement on threshold/legislative criteria	CSAM	Holocaust denial
No agreement on threshold/legislative criteria	Defamation	LGBTQ+ expression

Hate speech and targeted harassment based on identity signals are already a widespread problem in IXR, specifically on social VR platforms (Hine, Rezende, et al. 2024; Hine 2024b; Blackwell et al. 2019). At the root is the nature of IXR as a mediated platform. The online disinhibition effect (Suler 2004), which sees people behave worse online when they are anonymous, and the "just a game" mentality (Cross 2014), where people dismiss harmful impacts in virtual environments, together facilitate harassment. Countering this form of harassment is difficult, even allowing for the possibility of automated content moderation, because in IXR, content moderation is actually *conduct* moderation, which is inherently more challenging than moderating content. Platforms can train machine learning (ML) models to detect images of nudity, violence, terroristic speech, or other prohibited content, and images are cross-checked against databases of known CSAM and copyrighted images (Internet & Jurisdiction Policy Network 2021). While some IXR content, such as AR overlays, is well-defined enough for technical measures to potentially be effective, other forms of content are more difficult.

Consider, for example, the "Qniverse" (also discussed in Chapter 3), created by *Buzzfeed* journalists as an experiment in Meta's *Horizon Worlds* social VR platform (Baker-White 2022). This virtual world was festooned with conspiratorial phrases and soundtracked to conspiracy theorist Alex Jones, who (along with his company *InfoWars*'s pages) had previously been banned from Facebook (Darcy 2019). This seemed to go against Meta's Terms of Service, but despite reporting the virtual world to Meta twice, no action was taken. The platform was likely relying primarily on human moderation, perhaps because training an ML model to detect VR worlds that violate content standards is too difficult, especially considering the importance of context and the potential for parody or satire. Still, even human moderators can have difficulty accounting for these, and human moderation is more difficult to scale. These limitations are especially pronounced when dealing with live conduct, which faces the technical issues of live streaming combined with the social issues of interactive, immersive social platforms. Existing live interaction platforms already struggle with harm prevention. Live audio platform Clubhouse relies mostly on individual reporting and volunteer moderators, resulting in a system that prioritizes post-facto remedies (Clubhouse Blog 2020). While some platforms and companies are working on technical solutions for audio and/or video monitoring (VerifyMyContent, n.d.; Yubo, n.d.), these do not solve the social problems like the online disinhibition effect that encourage antisocial behavior in IXR.

Beyond antisocial behavior like that seen in the physical world, IXR also creates a new avenue for harassment and defamation through avatar deepfakes. Rather than creating a fake image or video of an individual, a realistic full-body avatar could be created to show an individual in explicit or compromising situations (Zenor 2014). 98% of existing deepfake videos are pornographic, and 99% of those are of women (Home Security Heroes 2024); deepfake avatar content will likely be similarly targeted. Additionally, several sources from the literature review reference the use of IXR for child sexual exploitation (Wagner 2019) and the creation of CSAM (Esposito 2018). This falls under the category of expression that is widely banned and widely accepted as not deserving of protection, as does speech inciting terrorism, which one source argues should not be prohibited in VR video games (Hupf 2014). However, due to its immersive and embodied nature, IXR could be a tool for not just "terroristic speech" but terroristic planning and training and thus must be considered differently from traditional video games and social media (Hine, Rezende, et al. 2024). Along with CSAM, the detection of this content often carries the legal duty for platforms to report it to national authorities.

As a result of these difficulties, controversial expression may proliferate in IXR. While some may claim that it is their right to engage in such expression, most jurisdictions agree that things like CSAM are not only not protectable expression, but are illegal because of the harm that they cause. Still other forms of expression, such as hate speech, may be protected by the state, but banned by most online platforms because they make the online platform a worse place to be. Were platforms to allow unfettered freedom of expression on IXR platforms, they would be dangerous places for the vulnerable groups who are often the targets of controversial expression. Thus, even when we accept the protection of this kind of expression in the physical world, we need not accept it in a virtual world. Unlike assemblies, which are restricted in part for fear of physical harm and damage, expression can be harmful regardless of venue, creating compelling reasons to restrict it and thus more implicit legitimacy for platforms to make that trade-off. As a result, while IXR may have fewer justifiable restrictions on assembly, it may have more on expression.

6.1.1.2. Non-Controversial Expression

IXR opens up new modalities and opportunities for visual art, performance art, and storytelling (Fornasier 2024).[118] Artists have used IXR to virtually display art in public spaces, augment existing art, and create immersive galleries (Mortice 2022; Down 2023; Charr 2024). Musicians including Doja Cat ("Experience Doja Cat's Concert in VR" 2024), Imagine Dragons (Meta Quest, n.d.), and Blackpink (Nwanji 2024) have already held concerts in VR, using them as an opportunity to provide exclusive experiences to fans and create different concert experiences than would be possible in the physical world. This "embodied spectatorship" immersive performances facilitate is hailed as a new way to "explore spaces between intimacy and distance, between different modes of perception, between the actual and the virtual" (Wilson 2020), offering artists new ways to express themselves and create their work, and audiences a new way to experience it (Smith 2018).

Because of its intimacy and immersiveness, IXR performance art begins to bleed into storytelling, but there are more specific storytelling efforts at both the macro and micro levels. IXR has been used to promote tourism and cultural experiences, telling historical tales and the stories of groups of people (Beck et al. 2019). VR has often been hailed as an "empathy machine" (*Chris Milk* 2015) that allows individuals

[118] I separate artistic expression from political expression while acknowledging that at least some artistic endeavors are political and that there is some debate about whether art is inherently political (for a fuller discussion, see Ramzan (2023)).

to "walk in someone else's shoes" through immersive storytelling, but experimental evidence for its efficacy over that of other media is limited (Sora-Domenjó 2022), and it has been suggested that VR "automates" racial empathy by outsourcing "labor of compassion" and trafficking in new forms of identity tourism (Nakamura 2020). Still, IXR is unique in that it enables high levels of representational, participatory, affective, and narrative immersion, which makes it an effective storytelling tool and perhaps one that *can* create empathy, albeit when designed with similar levels of care and thoughtfulness as empathy-inspiring traditional media (Balcerak Jackson and Balcerak Jackson 2024), offering new opportunities for creatives to present their stories to the public.

While IXR offers new opportunities for artists to express their artistic visions and connect with their audiences, it also creates potential obstacles to freedom of expression, especially regarding individual self-expression. IXR can enhance self-expression by allowing people to selectively convey information about their identities and adapt their appearance to specific contexts through AR filters and VR avatars (O'Hagan et al. 2023). The mediating platform company decides what avatar customizations are possible and thus who can express their identities in IXR (Hine 2024b); differential access to embodiment and the corporate mediation of that embodiment is discussed more fully in Chapters 3 and 4. Additionally, as discussed in the previous chapter, hate speech and harassment are rife on IXR platforms, which chills people's willingness to embody avatars that represent their true identities (Hine 2024b; Schulenberg, Freeman, et al. 2023). As a result, even when technologically possible, not everyone is able to express themselves with equal levels of protection, meaning that some are able to more fully exercise their freedom of expression than others. This line of reasoning is similar to the one around state actors discussed above, but on this level deals with user behavior and platform culture rather than government beliefs and priorities.

The final topic I will discuss related to IXR and expression is another risk that may be an opportunity. With the introduction of new technologies has often come a panic about how it will change standards of social interaction in the physical world. At the root of this fear are uncertainties around evolving self-expression. When commentators suggest that a man in an Apple Vision Pro ad must not be a good father because he is wearing a headset to take photos of his children, they are saying that his self-expression does not match the expected self-expression of an active father (Patel 2023). However, as our perceptions of people wearing smartwatches and headphones in public changed (from "rude" to normalized), so too may our perceptions of people wearing IXR devices in public (Hine 2024a). While this may not appear to be an extremely pressing concern, the idea that IXR may change standards of self-expression and thus who is able to express what and where is one that should be taken seriously.

6.5. Applicability of EU Legislative Toolkit

In this section, I analyze the applicability of six areas of EU legislation to freedoms of assembly and expression in IXR: the GDPR, ePrivacy Directive, DSA and DMA, AI Act, AVMSD, and UCPD. Due to the nature of the rights and what needs to be protected, these differ slightly from those discussed in the previous chapter on safety and privacy.

6.5.1. General Data Protection Regulation (GDPR)[119]

IXR is a sensor stack: eye gaze, facial micro-movements, voice, body pose, hand tracking, geolocation, and device mapping can all be recorded. As discussed in the previous chapter, much of this is personal data (Art. 4(1)), and some becomes biometric data when able to uniquely identify a person (Art. 4(14)). If a platform uses face geometry, iris patterns, gait, and/or voiceprint to identify or authenticate an avatar, that is "special category" data—its processing is prohibited unless an Article 9(2) exception applies (e.g., explicit consent, contractual agreement, or narrow public-interest bases under law) (Art. 9(1–2)). Controllers must also follow the core principles in Article 5 (lawfulness, fairness, and transparency; data minimization; storage limitation; integrity; and accountability), and build privacy by design and by default (Art. 25). These constraints could dampen chilling effects at XR assemblies by making the default *not* to

[119] (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) 2016)

identify participants without a strong, transparent legal basis. Finally, levers like DPIAs and profiling objections (Arts. 22, 35) collectively discourage covert identification, profiling, or de-ranking of assembly content.

6.5.2. ePrivacy Directive[120]

While the GDPR governs "processing," the Directive on Privacy and Electronic Communications (ePrivacy Directive) defend the communications layer and the device itself. Article 5(1) protects the confidentiality of communications—prohibiting listening, tapping, storage, or other interception without user consent or a lawful basis. If, as previously argued, communication layers in IXR qualify as ICS, the ePrivacy Directive provides a baseline level of communications privacy and reassurance around the confidentiality of communication within assemblies, particularly private ones. Article 5(3)—the "terminal equipment" rule—forbids storing or accessing information on a user's device without prior consent (subject to narrow, strictly necessary exceptions). For head-mounted displays and AR glasses that have local caches, geolocation data, or attention telemetry, this ostensibly prevents silent, non-consensual harvesting through local storage or device APIs. Article 6 adds guardrails for traffic data, requiring it to be anonymized or deleted when no longer needed to transmit communication (Art. 6(1)). Together, these provisions can be cited to challenge covert extraction of in-headset data that could chill expressive participation, although Article 5 and 6 provisions can be restricted for the aforementioned Article 15 national security derogations.

[120] OJ L 201, 31.7.2002, p. 37.

6.5.3. Digital Services Act (DSA)[121] & Digital Markets Act (DMA)[122]

The DSA has significant content moderation transparency provisions that may protect freedom of expression: online platforms must provide publicly available, plain-language "information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint handling system" (Art. 14(1)). Notably, fundamental rights are a chief concern when considering the enforcement of these provisions; intermediary services must act "in a diligent, objective and proportionate manner" when enforcing content moderation provisions and do so "with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter" (Art. 14(4)). Disclosure of content and account restrictions and the way they are enforced may help curtail vague, speech-chilling conduct. Users whose content or avatars are demoted, de-indexed, geoblocked, or removed must receive a statement of reasons—what was taken down, under what platform rule or law, and whether automation was used (Art. 17)—so they can contest moderation, which may be particularly valuable around XR protests or political art when meaning and acceptability are contested. The DSA then mandates two remedy options: internal complaint-handling and certified out-of-court dispute (Arts. 20–21). These procedural guardrails matter in IXR because moderation often blends enforcement with aesthetic or spatial judgments (e.g., blocking a virtual march route), and the DSA's due-process steps make removals reviewable instead of opaque.

Where XR platforms reach "very large online platform" (VLOP) scale (though none as of yet have reached this threshold), the DSA tilts even more toward fundamental-rights-preserving design. VLOPs must annually assess systemic risks to civic discourse and fundamental rights (including freedom of expression) that flow from their recommender systems, interface design, and ad tech, and then adopt

---

[121] (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) 2022)

[122] (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) 2022)

proportionate mitigation measures (Arts. 34–35). That is a lever for addressing the potential risks to freedoms of assembly and expression outlined above, but with the critical caveat that it would only apply to the largest of IXR platforms—and applies to none right now. VLOPs are also subject to independent compliance audits, data access for vetted researchers to study these systemic risks, and a crisis-response mechanism that must itself be fundamental-rights-proportionate (Arts. 36-37, 40). The DSA has been in force since 17 February 2024, so these duties already apply.

The DSA also reaches manipulative XR interface patterns. Article 25 bans designing or operating interfaces that "deceive or manipulate" users or materially distort choice. Though it is unclear exactly what form these "dark patterns" could take, examples could include pop-ups that repeatedly steer users away from civic events, or friction that makes starting a political broadcast difficult. Article 25 even names examples like prominence-skewing defaults and obstructive pop-ups. Though what dark patterns look like in IXR have yet to be defined—as previously discussed—this provides a lever for users should they arise.

The DMA, as a market competition regulation, has limited relevance to freedoms of assembly and expression around IXR. However, provisions preventing platforms from prioritizing their own events over those of third parties (which *Horizon Worlds* users have accused Meta of doing (Peters 2023)) may facilitate more equal access to assembly (Art. 6(5)). Cross-service data combination restrictions may also address the chilling of expression that could result from pervasive tracking across platforms and devices (Art. 5(2(b)).

6.5.4. Artificial Intelligence Act (AI Act)[123]

Some XR risks stem from how AI mediates presence and perception. The AI Act imposes transparency duties that matter directly for assembly and expression. The most salient prohibitions include: (i) AI that

[123] (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013,

uses subliminal, manipulative or deceptive techniques beyond a person's consciousness to materially distort behavior (Art. 5(1)(a)); this could potentially include subtle field-of-view warping, haptics or audio cues that could steer users away from a rally space); (ii) creating or expanding facial recognition databases through untargeted scraping of images from the internet or CCTV (Art. 5(1)(e)); and (iii) constraints on real-time remote biometric identification in publicly accessible spaces for law enforcement, with judicially-controlled exceptions and fundamental rights impact assessment requirements (Art. 5(1-3)). The latter two have clear interactions; the prohibition of expanding facial recognition databases could protect assembly by inhibiting AR-based recognition even when permitted by the AI Act, and prohibiting real-time remote biometric identification will stave off the potentially inhibitory effects on physical assemblies. On the transparency side, Article 50 requires that deployers of emotion-recognition or biometric categorization systems inform natural persons exposed to them—important if an XR venue scans faces or voices to infer mood or classify users—and it also contains labeling duties for certain synthetic media. For protest contexts—virtual or AR-overlaid—these rules help keep persuasive environments from crossing into prohibited manipulation, and they force visibility when sensitive inferences are in play. (Note the staged applicability: prohibitions apply as of February 2, 2025, while other pieces phase in through 2025–2026.)

6.5.5. Audiovisual Media Services Directive (AVMSD)[124]

Where XR platforms function like "video-sharing platforms," the AVMSD's Article 28b compels "appropriate measures" to protect minors and the public from certain illegal or harmful content, while forbidding general ex-ante upload filters and requiring proportionate, practicable tools (which may include flagging, complaint mechanisms, age assurance, and parental controls). Importantly for expression, the AVMSD calls for transparent, user-friendly reporting and reason-giving systems and out-

(EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) 2024)

[124] (Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the Coordination of Certain Provisions Laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) 2010)

of-court dispute mechanisms, which may help prevent user protection mechanisms from becoming arbitrary speech suppressors. That package mirrors, and can complement, the DSA's procedures in mixed XR/video environments.

6.5.6. Unfair Commercial Practices Directive (UCPD)[125]

Assembly and expression can be chilled by design, not just moderation. The UCPD's general ban on unfair practices—misleading actions/omissions and aggressive practices (Arts. 5–9 and Annex I)—applies to "business to consumer" (B2C) interfaces and marketing inside XR. This allows regulators and courts go after "dark patterns." Though what "dark patterns" look like in IXR has yet to be established, one could imagine subtly corralling users away from political gatherings, masking the commercial nature of "counter-speech" sponsorships, or using undue influence in immersive ad formats to manipulate civic behavior. The DSA's Article 25 ban on manipulative online interfaces augments the UCPD, making it easier to address XR nudges that distort expressive or associative choice as unlawful commercial practices as well as platform-governance violations.

6.6. Conclusion

In this chapter, I have discussed how the freedoms of assembly and expression translate into IXR. As recognized by the UN through the Guiding Principles, businesses have a responsibility to respect human rights and remedy violations, a crucial question considering the immersive and embodied nature of IXR that brings the rights closer to their physical equivalents. While the UN has also recognized that human rights apply online as well as offline, how this translates into human rights due diligence by corporate

[125] (Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market and Amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA Relevance) 2005)

actors remains unclear. Though public and cooperative entities may also play a role in IXR governance, IXR development dynamics strongly favor large companies.

As the UN itself acknowledges, we do not leave our human rights at the virtual door. However, the precise extent to which IXR presents truly novel concerns about freedoms of assembly and expression is difficult to ascertain. While freedoms of assembly and expression should be acknowledged in virtual environments, including in IXR, allowing unfettered expression in IXR will cause disparate impacts for vulnerable communities and threaten the usability and commercial viability of IXR platforms. However, any restriction on fundamental rights is, understandably, a weighty topic. While some restrictions are accepted in some online spaces, like traditional social media platforms, they pose increased concerns in IXR. Just as safety and privacy are of greater concern in IXR than on social media because of its immersiveness and interactivity (Hine, Rezende, et al. 2024), IXR provides a more dynamic way to exercise freedoms of assembly and expression, and so restricting them correspondingly restricts those opportunities.

There will always be trade-offs between different rights, and as platform embodiment grows, so too should government oversight of how platforms are upholding these rights. However, unless this oversight comes at an international level, it will subject platforms to the same jurisdictional conflicts and politicization that they currently face at a smaller scale. Additionally, when discussing human rights, questions of representation come into play. According to Article 21 of the UDHR, “everyone has the right to take part” in government (United Nations General Assembly 1948b) meaning that some form of representative or cooperative governance may be required to ensure that human rights are upheld in a legitimate way. In this thesis’s conclusion, I will address IXR governance proposals and outline a novel framework for the governance of virtual spaces. The next chapter, however, addresses policy recommendations to the European policymaker.

Chapter 7: Recommendations to the EU Legislator

This section details my recommendations to EU legislators based on the previous risk and legal analyses. These recommendations are not exhaustive, but only a contribution to the ongoing debate, and when possible, I refer to other sources that make similar suggestions. Not all identified risks merit new hard law, as locking in regulations centered on specific provisions may be detrimental. Some could be implemented by creating or modifying primary law, some could be based on secondary legislation, and some could involve regulatory or judicial interpretations. Others do not specifically relate to hard or soft law, such as funding research initiatives, but all will fill gaps in existing policy to uphold safety and privacy in IXR. I first address recommendations to protect safety and privacy, then freedoms of assembly and expression. Within each specific right, recommendations for new policies are first, followed by proposals to modify current legislation, and finally regulatory and non-legislative recommendations.

Although I provide recommendations to EU policymakers, my map of risks and some of my recommendations may also apply to other jurisdictions. Because IXR is a global and pan-jurisdictional phenomenon, I hope this chapter will contribute to a more extensive discussion of how safety and privacy protections can be harmonized in other contexts.

While existing initiatives focus on non-legislative solutions, it is reasonable to anticipate that the EU will pass legislation on IXR in the near future.[126] At least some aspects of EU regulation on IXR will be "exported" to other markets by companies and governments who follow EU regulation because of its regulatory competency and market size—the so-called "Brussels Effect" (Bradford 2020). The private sector is likely to play a crucial role in translating regulations to practice, and I hope that IXR companies anticipating my recommendations in their own self-regulation and codes of practice will help fulfill their human rights obligations (United Nations Human Rights Office of the High Commissioner 2011b) and avoid potentially disruptive adaptations when legislation is passed.

[126] Some XR-related policy proposals have already been made in the American academic context (Spiegel 2018), but legislation has not been forthcoming.

7.1. Physical Safety

1. Legal requirements should be introduced to provide users with easy access to safety tools that allow them to:
    a. Mute other users and/or blur their avatars to mitigate verbal and physical harassment.
    b. Prevent other avatars from entering their personal space.
    c. Quickly enter an out-of-world "safe zone" where they cannot be followed, seen, or interacted with (like the *Horizon Worlds* "Safe Zone"), and re-enter the world at a previewable location of their choosing. Note that this would not entail invisibility, but entering a location removed from the virtual world.
    d. Report malicious behavior by other users. Report patterns should be monitored to ensure that spam or vindictive reports are not used to target individuals or communities.
2. Access to "digital twins" that may provide intelligence for groups planning attacks should be restricted by law and/or their owners (World Economic Forum 2022).
3. Assault and battery laws should be clarified, or new laws enacted, to explicitly cover virtual attacks where no physical contact takes place, as discussed by the Council of Europe (Vinders 2023).
4. The Terrorism Regulation should be clarified, by amendment or judicial interpretation, to establish that immersive environments where terrorist or extremist groups gather, or ones constructed to promote their ideology, are also subject to removal and reporting to authorities.
5. In concert with IXR platforms, EU Member States should create initiatives or augment existing ones to promote safe drinking habits surrounding IXR, especially targeting "nightlife" areas.

7.2. Mental Safety

1. To protect user autonomy, and according with the Council of Europe's concerns about digital manipulation and XR (Vinders 2023; Committee of Ministers 2019), new legislation should be introduced to require the following:

a. Artificial Avatars should be prominently labeled ("PwC Digital Ethics for Responsible Metaverse" 2022) whenever they could be feasibly confused with a human-powered avatar, and users should be able to request, easily and effectively, that such avatars immediately cease contact with them. In situations such as games where players expect to encounter Artificial Avatars, a disclosure mechanism may be suitable. Legislation requiring this will build on the DSA's disclosure requirements by empowering users to avoid potentially manipulative Artificial Avatar behavior.
b. Surroundings that may appear different from what other users see should include a visual disclaimer to that effect.
c. Platforms should be prohibited from undertaking any research or experimentation aimed at manipulating users' emotional or mental states unless such studies explicitly and informatively recruit participants, with appropriate, ethical, legal, and human subject research measures and informed consent.
d. To maintain user awareness of how content in IXR can differ from person to person, users should be able to view the perspective of another user, with that user's permission, to see what that person's IXR and their own presence in it look like. Differences (i.e., in user-targeted content) should be highlighted on request. Content deemed illegal based on a user's jurisdiction should still not be visible in this mode.
e. Platforms should be prohibited from accepting payments from users displaying signs of compulsive buying behavior that could be linked to Internet or gaming addiction (Granero et al. 2016), nor should they engage in manipulative promotion of goods or services.
f. To help prevent addiction, VR platforms should be required to encourage users to take a break after some threshold time has been reached.
    i. This threshold time should be further studied. Every 30 minutes, as enforced by the Stanford VR class (Stanford HAI 2022), may be excessively paternalistic, but

every hour (as advocated by some Horizon Worlds moderators (Hill 2022)) could be a reasonable starting threshold. Empirical reporting suggests that it is easy to lose track of time in VR (Hill 2022), so these nudges should also indicate the current time.

2. Until research establishes what risks IXR may pose to children, platforms and hardware manufacturers should be required to establish mechanisms to prevent children under 13 from access. That age is a conventional standard set by an American data protection law from 1998 (Canales 2022), but it could be an effective starting point if recommended enforcement measures are operationalized. This is technically the minimum age for using some devices, including Meta's Oculus headsets, but it is not enforced (Hill 2022). Additionally, IXR experiences should be able to set age restrictions for entry, and any with explicitly adult content should not allow access to children.

    a. Age verification should happen at both the account and device level to prevent a young person from using an adult's account. Account-level verification could involve credit card or state-issued ID verification; for example, in line with how Google interprets the Audiovisual Media Services Directive[127] for access to age-restricted content (Google Account Help, n.d.). Instagram has been testing face scans to verify age (Malik 2023), which can be effective; the contractor claims that its model's mean absolute error is 1.4 years for ages 6-12 and 1.5 years for ages 13-17, although some gender and skin tone discrepancies remain (Yoti 2023). If the model cannot determine the user's age confidently, photo identification could be requested as a fallback (and should also be a primary option for those who do not want to provide biometrics); trusted third parties and/or zero-knowledge proof techniques could assist with making this more secure. This accords with recommendations from an International Telecommunication Union (ITU)

[127] (Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the Coordination of Certain Provisions Laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) 2010).

working group on data protection (ITU Focus Group on Metaverse FGMV-12 2023). Device-level verification could involve facial or retinal authentication via the device, with scans encrypted and stored only locally on the device, similar to how Apple stores Face ID data (Apple Legal, n.d.). Additional research should explore verification measures for those without state-issued IDs. All scans and images used for age verification should be deleted promptly by all parties involved after verification is complete.

3. People of age should be able to register on IXR platforms without providing identification (although this may still require a photograph for age verification, and anyone suspected of being under 13 must prove their age; this is necessary to balance privacy with children's protection). Avatars using a real person's name should be able to request free identity verification and furnish proof of identification corresponding to the name of the avatar, or that the avatar's name is a plausible alias also used in the physical world. Verified avatars should be labeled as such. Avatars representing brands should also be able to request verification that they work with that brand, similar to how Twitter's legacy brand verification worked ("Legacy Verification Policy," n.d.). VR spaces should be able to limit access to verified avatars.
4. To prevent the propagation of deceptive clones, near-clones, and deepfakes in IXR, legislation or judicial interpretation should clarify that the right to one's image extends to an avatar and virtual environments.
5. Due to their unique risks, provisions in the DSA and DMA on advertising, dark patterns, data processing, and portability should be expanded to all IXR platforms regardless of size.
6. Advertisement archives, as laid out in Article 39 of the DSA, should be required to include information on exactly where and how an ad was displayed or performed (in the case of an Artificial Avatar promotion) in an IXR environment.
7. Targeted transitive and subliminal advertising (e.g., transforming all beverages into a specific soft drink or ads on passing cars) should be prohibited because of the potential for violating user autonomy and the impossibility of effective user interaction with the disclosures required by the

DSA. This could be clarified in the AI Act (Franklin et al. 2022). Non-targeted ads of this nature may be permitted due to their similarity to mass campaigns and sponsored events in the physical world, but the user must have easy access to the general ad archive as well as to a summary of what ads they were presented with and other information that would be included in the DSA archive.

8. How intellectual property protections and property law apply to IXR should be clarified, by legislative amendment or judicial interpretation, to prevent IP theft and loss of purchased digital items (Maciejewski 2023).
9. EU Member States should fund research into the long-term and addictive effects of IXR, especially how they may differentially impact children and marginalized groups.

7.3. Social Stability

1. Standards of accessibility for hardware and software should be created and enforced by legislation like the Web Accessibility Directive[128] to ensure that individuals with physical and cognitive disabilities can access IXR.
2. Competent authorities under the DSA should require platforms to institute effective automated content moderation systems. Details of these systems should be clearly communicated to users, even if contractual necessity is used to justify the use of automation rather than user consent (Article 22 GDPR), as should sanctions for violating content policies. I acknowledge that automated content moderation has not always proved sufficiently flexible and pluralistic in its implementation, especially for marginalized communities (Oliva et al. 2021). Thus, when a user is sanctioned, a full explanation of how their content violated a specific policy should be provided, as should an appeals mechanism that allows for human review of their case. As acknowledged by the Council of Europe, this balance will be highly culture-dependent (Vinders 2023).

[128] (DIRECTIVE (EU) 2016/2102 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2016 on the Accessibility of the Websites and Mobile Applications of Public Sector Bodies L 327/1 2016)

3. EU Member States should fund initiatives to research harassment in IXR and digital and IXR literacy campaigns to help users understand the potential risks and benefits of IXR. Ensuring that users are informed will help guard against new scams and other risks to safety.
4. Member States should be aware that, due to the pan-jurisdictional nature of IXR, platforms may face pressure from governments—both within and outside the EU—to ban some forms of content and expression in ways that conflict with expressed EU values. For instance, governments that restrict LGBTQ+ expression could pressure IXR platforms to censor LGBTQ+ content (Hine 2023). Member States should be prepared for possible political pressure on EU-based platforms and governments.

7.4. Informational Privacy

1. Biometric data should only be used in real-time for the functionality and refinement of IXR experiences and therapeutic or research-related experiences with explicit consent and ethical-legal approval. They should never be retained by platforms, hardware providers, employers, or schools, even in anonymized or aggregate form. Users in IXR experiences should be able to opt out of biometric data use (except for what is strictly necessary for functionality, e.g., for avatar motion) and have a similar experience. This will go beyond the provisions in the AI Act to prevent the construction of "kinematic fingerprints" that could be used for autonomy-violating content or ad targeting (Spiegel 2018) and the construction of aggregated or anonymized datasets that could be used to mine group-level behavioral insights (Renieris 2023). Biometric data also should not be used to make inferences about other characteristics of a user, including about their affective states or cognitive processes, regardless of whether those characteristics are protected. This should be mandated by new legislation or revision to the GDPR.
2. Scraping of any form of biometric data, as well as the nonconsensual collection and aggregation of biometric data using AR devices should be banned by legislation.

3. The GDPR should be comprehensively analyzed to determine if the data processor/controller distinction is still fit for purpose (Martin 2022). If specific IXR legislation is adopted, it should clarify the allocation of data protection responsibilities between platforms, hardware providers, and advertisers. In the case of joint controllership, legal arrangements explaining responsibility allocation should be made mandatory (cf. Article 26 GDPR). Upon user request, IXR platforms should display a point of contact to exercise data protection rights.
4. Competent authorities under EU data protection law should require IXR platforms that allow users to record to ensure that avatars whose users did not explicitly consent to being recorded are blurred or otherwise anonymized when the video is exported. A clear indication should be displayed when a user is recording in VR, and on AR devices in the physical world.
5. Competent authorities under EU data protection law should require device providers to inform users about exactly what biometric data their IXR devices can collect in an understandable format on first use or upon terms' modification and reminded at least annually. IXR platforms and experience providers should provide users similar information about what data the specific IXR experience collects.

7.5. Decisional Privacy

1. What dark patterns look like in IXR should be clarified by the EDPB, and a mechanism for reporting them should be established. The European Centre for Algorithmic Transparency (ECAT), through their research into the impact of algorithmic systems, may be able to aid in this.

7.6. Local Privacy

1. Gathering bystander data and creating "shadow profiles" containing data about individuals in the vicinity of IXR users should be prohibited by primary law or judicial interpretation.
2. VR users should always have access to a private space, whether a home-like environment or a "lobby," where they can turn off recording by individuals and the platform, but platforms should

develop alternative behavior reporting mechanisms that do not rely on video evidence to protect these spaces. Legislation should clarify the distinction between public and private spaces, and IXR providers should remind users where their actions are subject to monitoring, recording, and/or analysis.

3. Clauses of the AI Act that deal with AI in physical spaces should be expanded to include virtual spaces.

7.7. Freedom of Assembly

1. The AI Act's prohibition on real-time biometric identification by law enforcement in publicly accessible *physical* spaces (Art. 5) should be explicitly extended to cover publicly accessible *virtual* spaces to prevent chilling effects on virtual protests.
2. The GDPR and ePrivacy Directive, specifically Articles 12-13 of the GDPR and Article 5(3) of the ePrivacy Directive, should be interpreted to require platforms to provide clear, upfront notice to users when an assembly (virtual or physical) is being monitored or recorded by the platform or state authorities. This ensures participants can be informed as to the information privacy dynamics of their participation.
3. Clarify under the DSA that "content moderation" includes spatial/embodied enforcement (e.g., geoblocking 3D areas, occluding avatars, dynamic crowd limits, and line-of-sight demotion). Platforms must log these decisions and disclose them in user-facing notices to make removals reviewable rather than opaque.
4. Create XR-specific assembly due-process rules: when platforms restrict an XR gathering (e.g., close a world, cap crowd size, block a virtual route, or throttle discovery), they must issue a contemporaneous, plain-language statement of reasons, specify whether automation was used, and provide rapid remedies (likely including internal complaint and certified out-of-court mediation or dispute resolution). Apply these duties to all significant IXR platforms, not only VLOPs. These build on content moderation disclosure and appeal requirements in the DSA.

5. Require time, place, and manner (TPM) standards for virtual public forums: restrictions on marches, rallies, vigils, or pickets in XR must be necessary, proportionate, and content-neutral, with routes and capacity rules published in advance. This translates the DSA's "diligent, objective and proportionate" enforcement to embodied, spatial moderation where blocking a path can suppress assembly.

7.8. Freedom of Expression

1. It should be clarified that image and likeness rights extend to avatars and spatial renderings to curb deceptive clones or near-clones and deepfake performances that chill real speakers and can be used to abuse others. This should be coupled with provenance and watermarking measures while preserving latitude for parody.
2. EU Member States and competent authorities should promote the development of interoperability standards for avatars and user-created assets, as enabled by the DMA and GDPR's data portability requirements. This would allow users to move their expressive identities and creations between platforms, reducing platform lock-in and censorship power.
3. The DSA should be amended to require that all IXR platforms, regardless of size, provide users with a wide and evolving range of options for self-representation (avatars). This should include diverse races, body types, genders, and functional representations of disabilities (e.g., virtual wheelchairs, not just stickers), directly countering the creation of a "tiered reality" where only some identities can be authentically expressed.
4. Transparency for algorithmic occlusion of expression should be required. When visibility is reduced via spatial tricks (moving user spawns, altering lighting/line-of-sight, "ghosting" avatars/worlds), statements of reasons must specify the rule violated and the mechanism used, preserving the DSA's due-process core in immersive contexts.
5. The European Commission, through DG CNECT and the ECAT—already responsible for DSA enforcement (Jahangir 2025)—should issue guidance on AR overlays in public spaces

requiring clear labeling and user controls for political overlays and ensuring that counter-speech layers can co-exist rather than being suppressed by default platform skins, reflecting heightened platform responsibilities as XR makes online experiences akin to offline ones.

These policy recommendations are isolated recommendations to address specific issues with the technology. While that is a necessary step, it is insufficient to sporadically address individual risks. Instead, we need a comprehensive operationalizing framework to guide us in determining what regulations are needed and how to make them, one that fits into the EU's fundamental-rights-based regulation regime. This harkens back to the acknowledgement that, although businesses have responsibilities to uphold fundamental rights under the Ruggie Principles, there is little guidance for *how* to do so. The next chapter—the Conclusion—will outline an approach to thinking about fundamental rights responsibilities in the digital sphere, arguing that the more embodied a digital experience is, the more responsibility a business has to uphold fundamental rights.

Chapter 8: A New Framework and Conclusion

8.1. Introduction

This dissertation began with a fundamental question, one that resonates with increasing urgency in our hyperconnected era: *How does the rise of immersive extended reality (IXR) technology affect our conceptualization of fundamental rights in digital spaces?* This inquiry is not merely technical or legal, but mirrors back to us a more profound shift in our "onlife" condition. More than two decades ago, Lawrence Lessig presciently asked how we might protect liberty, privacy, and self-determination when the "architectures of control are managed as much by the government as by the private sector" (Lessig 1999, x–xi). Today, with the rise of IXR, we must confront a world where these architectures are managed *far more* by the private sector, and where their control extends not just to information, but to the very fabric of perceived reality.

This concluding chapter does several things. First, it provides a brief synopsis of the argument, recapitulating the thesis's theoretical, legal, and normative contributions and how they answer the thesis's research questions. Then, it advances the dissertation's central argument: that the unique nature of IXR—as a privately controlled, constitutive infrastructure enabling profoundly embodied experiences—necessitates a recalibration of how we protect fundamental rights. Finally, it proposes a preliminary framework for how to think about fundamental rights in digital settings based on embodiment, the public function doctrine, and the idea of fair procedure. The shift from the physical world to a mediated reality cannot be a moment of rights abnegation. Instead, it demands a corresponding evolution in our understanding of responsibility. As reality becomes increasingly mediated, the duties of the mediators must increase, moving beyond a baseline "do no harm" principle toward a more positive obligation to structure these new realities in a manner that actively preserves and enables the exercise of fundamental rights. This is the normative core of this work—an argument not for the rejection of technology, but for its deliberate and just governance. The principle articulated by the Human Rights Council, that "the same rights that people have offline must also be protected online" (Human Rights Council 2012), serves as our starting point, but IXR forces us to ask what "protection" truly means when the line between online and offline blurs.

8.2. Synopsis

In the introduction, this thesis posed one overarching research question (ORQ) and three primary sub-questions (RQ1–RQ3, plus a follow-up RQ3.5). Here, I restate the RQs and summarize how the dissertation answered them, addressing the theoretical, legal, and normative components. Later, this Conclusion will address the ORQ: *How does the rise of IXR technology affect our conceptualization of fundamental rights in digital spaces?*

RQ1: What does the structure of IXR services mean for individual user experiences?

RQ1 was the primary theoretical component of the thesis, probing how the architecture of IXR platforms shapes user experience. The dissertation answered RQ1 by demonstrating that the structure of IXR services—including hardware constraints, software design, platform governance, and content ecosystems—determines what users can and cannot do, and thus how they experience "reality" in XR. If only a few corporations provide the dominant XR platforms, for example, this centralization of infrastructure directly impacts users' agency, equality, and safety in those environments. Chapter 3 showed that IXR services function as layered infrastructures with embedded values: design choices like whether a platform is open or closed, interoperable or walled-off, advertising-driven or subscription-based, etc., can translate into constraints or affordances for users, affecting their freedom of expression (e.g., what content or avatars are permitted), their inclusion or exclusion from communities, and even their physical wellbeing (through safety tools or lack thereof). In practical terms, RQ1's answer is that the structure of IXR services means user experiences are fundamentally mediated by platform design. XR systems do not just deliver content; they constitute environments. Thus, features like immersive graphics, haptic feedback, community standards, privacy settings, and avatar designs all coalesce to define how a user experiences presence and interaction. This thesis highlighted that such mediation can lead to unequal experiences—for instance, high-end devices offer more vivid experiences than cheaper ones, and platform policies could privilege certain speech or behavior over others. The implication is that understanding XR's impact on rights starts with recognizing these services as reality-defining infrastructures: the architecture of IXR carries normative weight, conditioning experiences in ways that traditional internet services do not. By addressing RQ1, the thesis set the stage for linking XR's technical structure to its rights implications, illustrating how a seemingly technical question (how XR is built) has deep human rights significance.

RQ2: What are the positive and negative impacts of IXR on fundamental rights?

RQ2 was the core rights analysis, and the dissertation answered it by examining four specific rights—notably the right to personal safety (and related security of person), the right to privacy, and the freedoms of expression and assembly—across two categories to evaluate how IXR's immersive features both amplify familiar issues and create new ones. On the positive side, the research found that IXR can enhance certain fundamental rights or interests. For example, XR can support freedom of expression and assembly by allowing people to gather and speak in virtual spaces beyond physical limitations. Real-world illustrations are already emerging; virtual reality concerts and protests allow assembly across vast distances. As AR devices make inroads, they may empower political expression (such as overlaying digital protest art onto real-world spaces). XR can also promote equality and inclusion in some cases—for instance, by enabling virtual participation for people with disabilities, or allowing marginalized individuals to express their identity more freely through avatars. These are ways IXR might further the enjoyment of rights by overcoming physical-world barriers.

However, IXR also introduces or heightens a host of negative impacts on rights. The dissertation's analysis (in Chapters 5 and 6) demonstrated several key risk areas. First, user safety and bodily integrity face new threats: immersive harassment (like virtual groping or stalking) and psychological harms can occur in XR with an intensity approaching physical reality. A virtual assault may not leave physical bruises, but it can trigger fear, trauma, or exclusion just as a real-world assault might—especially given the sense of presence and embodiment in VR. IXR platforms thus see familiar problems like harassment take on an embodied dimension, potentially requiring rethinking of concepts like assault or consent in virtual settings.

Second, privacy and data protection are deeply challenged by XR. These systems rely on extensive data collection (from eye movements and body motion to one's physical surroundings in AR) to function. As a result, XR can generate sensitive personal data, including biometric identifiers and inferences about emotional or mental states, far beyond what traditional web platforms collect. This raises the risk of unprecedented surveillance and profiling, threatening the right to privacy and even the right to mental integrity or thought when manipulative techniques are used.

Third, freedom of expression and freedom of assembly face a double-edged sword in XR. While IXR can facilitate these rights (as noted), it can also endanger them. Platforms might impose new forms of censorship or control: for example, by algorithmically down-ranking certain virtual gatherings or by deleting user-created environments deemed "offensive." Moreover, because XR interactions feel real, any restriction on speech or assembly in these spaces can have a more profound chilling effect on users than a similar moderation on a 2D website. The thesis identified novel forms of potential infringement—e.g., using code-based affordances to disperse a virtual crowd or to silence an avatar's speech by altering the environment—which have no direct parallel in traditional social media. These actions could be akin to using state force to break up a physical meeting, illustrating how immersiveness intensifies the impact of rights restrictions. Additionally, while AR devices may empower physical political participation, they can equally chill it in places with a dearth of protections against facial recognition by law enforcement.

In summary, IXR affects fundamental rights in both empowering and threatening ways. It can enhance participation, expression, and accessibility (a boon for rights), even as it amplifies risks like harassment, discrimination, surveillance, and manipulation (a hazard for rights). A crucial finding of this work is that the immersive, embodied nature of XR means that harms in virtual environments can elicit real harm—emotional or physiological—blurring the dichotomy of "virtual" versus "real" injury. Consequently, the cost of ignoring rights in IXR is high. The analysis under RQ2 also emphasized that these impacts are not evenly distributed: vulnerable and marginalized groups often bear the brunt of XR's risks (just as they do offline). For instance, women and minorities are more frequently targets of virtual harassment, and persons with disabilities may find themselves excluded by non-accessible XR design. These insights underscore why a proactive, inclusive approach to XR governance is necessary to maximize the technology's benefits while mitigating its dangers.

RQ3: How does the extant EU legal regime address the fundamental rights impacts of IXR?

To answer RQ3, the dissertation conducted a survey and analysis of the existing EU digital governance framework to see how well current laws and regulations might apply to XR scenarios. The findings revealed a patchwork of partial coverage and significant gaps. On one hand, several EU legal instruments do extend to IXR contexts: for example, the General Data Protection Regulation (GDPR) applies to personal data collected via XR devices, meaning there are baseline rules for data privacy and consent in XR. Likewise, the Digital Services Act (DSA) covers online platforms broadly and would impose certain duties on XR platform operators regarding illegal content or systemic risks (although its requirements for the largest platforms do not cover any IXR platforms as of yet), and product safety laws (like the General Product Safety Regulation and product liability rules) apply to XR hardware and software. In these ways, the EU's horizontal regulations do provide some protection—e.g., XR users have data rights under the GDPR, and dangerous XR products could be subject to safety recalls or liability.

However, the analysis also identified important mismatches and areas where EU law falls short for XR. The laws were not necessarily written with immersive, embodied technologies in mind, leading to ambiguity in application. For instance, EU rules against online harassment or hate speech are largely indirect (relying on platforms' terms of service and the DSA's processes), and they may not clearly encompass new XR-specific harms like simulated physical harassment. Biometric and emotional data collected by XR systems present questions that current privacy laws only partially answer—the GDPR regulates processing of biometric data, but subtle inferences about a user's emotions or attention (gleaned from eye-tracking, for example) might slip through the cracks of existing definitions unless appropriately interpreted. Similarly, the intensity of manipulation possible in XR (through immersive dark patterns or subliminal cues) could demand stricter safeguards than currently exist in consumer protection law, particularly since what "dark patterns" look like in IXR is unclear. Additionally, the EU's emerging AI Act, while banning subliminal manipulation by AI, may not fully encompass manipulative design in an XR context that is not strictly "AI." Another gap lies in the freedom of expression and assembly domain: the EU Charter of Fundamental Rights binds Member States, not private companies, so users on an XR platform cannot invoke the Charter directly against the platform. The public law nature of fundamental rights leaves a void when private XR companies govern large social spaces and impact the exercise of rights in both virtual and physical spaces.

In essence, if IXR were to become mainstream tomorrow, the current EU legal tools would provide only partial protection for users' fundamental rights. Some important pieces are in place (data protection, basic platform accountability for illegal content, etc.), but key aspects—like protection from bodily harms in virtual space, robust safeguarding of mental integrity, and ensuring fair content moderation procedures—are not comprehensively addressed. The analysis for RQ3 thus highlighted a need for legal adaptation: Europe's framework, while comprehensive in traditional digital realms and commendably adaptable, has significant gaps vis-à-vis IXR's distinctive challenges. This conclusion set the stage for RQ3.5, which solicited recommendations on how the legal regime should adapt.

RQ3.5: How should the legal regime adapt to better protect fundamental rights in XR?

RQ3.5 invited a forward-looking, normative inquiry, bridging the gap between analysis and prescription. The dissertation responded by proposing a range of governance responses and regulatory adaptations (detailed in Chapter 7) to address the gaps identified. These recommendations span both targeted interventions and broad frameworks. On the targeted side, the thesis put forward concrete measures for EU policymakers and regulators: for example, updating safety regulations to require in-world safety features (like personal "safe zones," avatar muting, and personal space buffers to prevent virtual harassment) as standard on XR platforms, clarifying that existing criminal laws (e.g., around assault and stalking) and civil protections apply to serious misconduct in virtual environments, strengthening privacy rules to explicitly cover XR-specific data (like banning certain uses of biometric tracking data or mandating transparency for behavioral manipulation techniques), and raising standards for age verification and child safety in XR given the heightened risks to minors in immersive settings. The recommendations also extended to protecting freedoms of expression and assembly: for instance, ensuring that content moderation in XR is transparent and fair, by treating spatial or embodied moderation (like geo-blocking virtual locations or removing avatars) as "content moderation" under laws like the DSA—thereby requiring notice and appeals for affected users. In short, a spectrum of policy actions was outlined, from hard law to soft law and industry self-regulation. These proposed adaptations aim to fill the current gaps so that existing fundamental rights are more effectively upheld in XR contexts.

Importantly, Chapter 7 acknowledged that piecemeal solutions to individual risks, while necessary, are not sufficient. Thus, beyond specific fixes, I argue below for a comprehensive operational framework to guide XR governance. This is where the research segues into the dissertation's final prescriptive contribution: a normative framework (developed in this Conclusion) that ties together the insights on infrastructure, embodiment, and rights into an overarching approach. In essence, RQ3.5 is answered by the call for embedding fundamental rights considerations into the very design and governance of XR platforms. This includes urging companies to anticipate and mitigate human rights risks (in line with the UN Guiding Principles on Business and Human Rights) and urging regulators to treat immersive platforms not merely as products or services but as spaces requiring oversight akin to public spaces. A key thesis argument—which I elaborate below—is that as immersion and embodiment in digital platforms increase, so too should the responsibilities and legal obligations of platform operators to respect, protect, and enable fundamental rights. In summary, the legal regime should adapt by: (a) updating and extending laws to cover XR-specific harms and realities; and (b) adopting a new governance mindset that recognizes immersive platforms as holding a duty of care akin to public authorities in certain respects. With RQ3.5 thus addressed, the stage is set to discuss why IXR platform operators bear heightened responsibilities and how we can enforce accountability through existing and novel frameworks.

8.3. How IXR Recalibrates Conceptions of Fundamental Rights

The cumulative evidence and analysis presented throughout this dissertation provide a clear and multi-faceted answer to the overarching research question. The rise of IXR technology affects our conceptualization of fundamental rights in digital spaces by fundamentally altering the nature of harm, the scope of privacy, the locus of public discourse, and the vectors of manipulation and discrimination. It forces a move from abstract principles to embodied realities, demanding that our legal and ethical frameworks catch up to a world where the virtual and the physical are increasingly intertwined.

First, IXR collapses the distinction between online and offline harm. The core affordances of presence and embodiment mean that a virtual assault is not merely an exchange of pixels or text; it can trigger genuine psychological and physiological trauma, akin to a physical-world encounter. This experiential reality forces a reconceptualization of the right to safety and security of person (UDHR Art. 3). It compels a move beyond purely physical protection to include psychological integrity and dignitary harm as first-order concerns. This shift is already being tentatively recognized in law, as evidenced by the EU's updated Product Liability Directive,[129] which now includes "medically recognised damage to psychological health" as a compensable form of harm (Art. 6). In IXR, what was once considered "virtual" harm must be conceptualized as real harm, requiring equivalent standards of prevention and remedy.

Second, IXR forces us to expand our definition of digital privacy to one more in line with privacy in the physical world, shifting its focus from a primarily informational concern (data protection) to a

[129] (Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on Liability for Defective Products and Repealing Council Directive 85/374/EEC (Text with EEA Relevance) 2024)

more profound concept of embodied privacy. The sensor-rich nature of IXR devices—potentially capturing everything from eye movements and facial expressions to the layout of a user's home—creates unprecedented privacy risks that extend beyond traditional data breaches. This recalibration occurs across three dimensions, as conceptualized by Roessler (Roessler 2005):

- Informational Privacy: Data privacy is a paramount issue in IXR. Biometric data is not just limited to discrete fingerprints or retina scans. Identity can be inferred from the aggregation of XR motion data, creating "kinematic fingerprints" that threaten individual privacy.
- Local Privacy: The sanctity of one's private spaces, like a home or office, is compromised when cameras and sensors map and transmit data about one's physical surroundings, potentially without the consent of the user or bystanders.
- Decisional Privacy: The right to autonomy is threatened by the potential for "biometric psychography"—the use of physiological data to infer emotional states and nudge behavior in real-time, creating a powerful new tool of manipulation that operates below the threshold of conscious awareness.

The GDPR provides a crucial starting point, but its framework, built for an era of screen-based interactions, is stretched by the intimate, pervasive, and embodied nature of IXR data collection.

Third, IXR privatizes the public square, transforming what was once a metaphor for online discourse into a literal, albeit virtual, space. Social VR platforms and augmented public spaces become new arenas for assembly and expression. However, unlike a physical park or plaza, these spaces are built on privately owned, constitutive infrastructure. This concentrates immense control over fundamental civic rights in the hands of platform operators. They can regulate not just the content of speech but the very conditions of presence, location, and perception through the architecture of code. The ability to disperse a virtual protest by altering the spatial code or to render certain speakers invisible to others represents a form of power far more absolute than traditional content moderation, blurring the line between private platform governance and state-like control over civic life.

Finally, IXR infrastructuralizes manipulation and discrimination. It creates new vectors for societal harm that operate at the level of perception itself. As argued in Chapter 3, disparities in hardware quality and network access can create a "tiered reality," where the fidelity and richness of one's experience are dictated by economic status. This goes beyond the traditional digital divide; it risks embedding inequality into the very fabric of perception. Furthermore, the potential for personalized "Reality Distortion Filters," where algorithms curate not just a news feed but the entire sensory environment, challenges the shared experiential baseline necessary for democratic discourse and social cohesion. When two people standing in the same virtual space can be shown fundamentally different realities without their knowledge, the potential for polarization and manipulation becomes systemic and infrastructural. This forces us to conceptualize rights like non-discrimination and the right to receive information not just as protections against overt bias, but as guarantees of access to a minimally shared and authentic reality.

Given this profound recalibration of fundamental rights, the existing framework for corporate responsibility is no longer sufficient. The baseline "responsibility to respect" human rights, as articulated in the UNGPs (United Nations Human Rights Office of the High Commissioner 2011a) and discussed in Chapter 2, is a crucial but inadequate standard for the age of IXR. This standard, which calls on companies to "avoid infringing on the rights of others and address adverse impacts," frames corporate duty primarily in negative terms—a duty of non-interference (United Nations Human Rights Office of the High Commissioner 2011a). While essential, this fails to capture the unique power and position of IXR platform operators.

Essentially, this dissertation argues for a conceptual shift from a duty of *respect* to a duty of *stewardship*. This heightened responsibility stems directly from the theoretical foundations established in Part II. Because IXR platforms are built on a constitutive infrastructure that does not merely regulate behavior but creates the environment of experience, their operators are not simply service providers; they are architects of reality. Their power is not just regulative but, in Floridi's terms, poietic—it is world-making (Floridi 2020b). This poietic power comes with a correspondingly heightened duty of care.

Furthermore, because interactions within these platforms are deeply embodied, the potential for profound psychological and social impact is magnified. An architectural choice, a moderation policy, or a design flaw on a non-immersive website might cause frustration or offense; in a high-immersion IXR environment, the same type of decision can lead to genuine trauma, social exclusion, or the erosion of personal autonomy. In this context, inaction, negligence, or a purely reactive stance to harm carries far greater moral weight. The operators of these platforms are stewards of a new kind of human environment, and their responsibilities must be commensurate with their power to shape it. This argument reframes the BHR conversation for emerging technologies, moving it from a focus on mitigating negative externalities to one of proactively designing for the positive realization of fundamental rights.

8.4. A Governance Framework for a Just IXR

The challenge of governing IXR cannot be met solely by applying existing laws, however robust. The unique nature of immersive technologies requires a new conceptual framework for understanding the responsibilities of the private actors who build and control them. This dissertation proposes such a framework, one that adapts principles from public law to the realities of platform power, providing a principled basis for assigning heightened duties to digital platform operators, from embodied IXR platforms to traditional digital platforms. This framework rests on three pillars: the degree of platform embodiment, the concept of a public function, and the duty of fair procedure.

8.4.1. Adopting State Doctrines for Platform Governance

The framework's conceptual origins lie in the public function doctrine, a strand of US constitutional law. The public function doctrine is a subset of state action doctrine that holds that private actors are responsible for upholding constitutional rights if they play the role of a state actor. It was initially articulated in *Marsh v. Alabama* (*Marsh v. Alabama* 114 AD; Diamond 1979), a case decided by the US

Supreme Court that held that a privately owned company town had to uphold free speech rights because the company took on the functions of a state and thus had a corresponding responsibility to uphold constitutional rights, as the government would if the town was not privately owned.[130] While the public function doctrine has had a mixed record in its application to the Internet in the US (with the court in *Cyber Promotions v. America Online* (*Cyber Promotions, Inc. v. American Online, Inc.* 1996) ruling that AOL's operation of email servers did not count as a public function), I am not arguing about the law in any particular jurisdiction.[131] Rather, I am arguing that the ideas behind this doctrine can inform how we think about fundamental rights in digital settings. Thus, although the idea originates in US case law, our conceptual discussion is independent of any specific judicial ruling in any particular jurisdiction.

Lawmakers have been hesitant to classify traditional social media platforms as public utilities (Andrejevic 2013). My argument does not rely on a formal reclassification of IXR platforms or other digital services as public utilities; the public function doctrine relies on the assertion that private companies can play a role equivalent to that of public bodies. When it comes to digital platforms, this argument is based on the metaphor that digital experiences—particularly immersive ones—can compare to physical experiences and that platform operators therefore are playing a function akin to government when they manage, moderate, and mediate them.

The platform companies are the key operators here; their nature and that of their services impact rights and remedies. While it is often claimed that social media itself is the "new town square," it has not been legally recognized as such. Still, social media, while an important method of communication in the modern era, is not embodied. While a full ban from all social media by the state may violate one's right to freedom of expression in various jurisdictions (as found by the US Supreme Court (*Packingham v. North Carolina* 2017)) it is generally accepted that individual platforms have the right to moderate their platforms

---

[130] There is a second possible reading of *Marsh:* that the application of a facially neutral law in a way that cuts off one's access to a private town is state action, but it has more often been interpreted to be about private actors taking on state functions, which I adopt here (see Shaffer Van Houweling (2000) for a fuller discussion).

[131] Even within the US, the doctrine has been applied differently by different states; in California, the owners of shopping malls cannot restrict expression like soliciting petition signatures (Shaffer Van Houweling 2000; *PruneYard Shopping Center v. Robins* 1980).

as they see fit, including banning users that misuse the platform, but also an obligation to remove and report illegal content. However, IXR constitutes a set of immersive media, and thus the metaphor of the "town square" is much more apt in that it can be an immersive space where a person can declaim to a group of others and express themselves in more and different ways than in non-immersive virtual spaces.[132] If IXR platforms begin suppressing specific forms of assembly or expression, that would be a more severe restriction on those rights than banning a social media group or removing a post. Taken to their logical conclusion, moderation methods like using the affordances of code to disperse an assembly to silence a speaker would be equivalent to using state force to control those rights. In IXR, these actions could be much more embodied, causing emotional harm in addition to having the intended effects of halting assembly or expression. Thus, because of the power of expressing those rights in IXR and the harm done by restricting them, these platforms should have an increased responsibility to ensure that rights are not unduly restricted.

Note that this builds on the argument that virtual experiences are real experiences with non-trivial impacts similar to those in the physical world. Though they are not exactly the same as experiences in the physical world—otherwise we would be demanding government oversight—they are significant enough that platform responsibility is significantly heightened.

8.4.2. The Scalar Framework of Embodiment

The core argument of this framework is that platform responsibility is not a binary, all-or-nothing proposition. Instead, it is scalar: the degree of responsibility an operator bears correlates directly with the degree of platform-enabled embodiment, as Milgram and Kishino intuited in their famous reality-virtuality continuum (Milgram and Kishino 1994). Embodiment relative to the virtual medium, as

[132] The metaphor is not exact, as IXR is not ubiquitously accessible, nor is there a single dominating platform, but the analogy to the physical world remains apt.

analyzed in Chapter 4, is the key variable that determines the intensity and impact of a virtual experience. We can therefore map platforms onto a spectrum of responsibility:

- **Low Embodiment:** A text-based forum like an early bulletin board system or a modern platform like Reddit has a low degree of embodiment. Interactions are mediated through text, and the sense of physical presence is minimal. Here, traditional content moderation rules and a baseline "responsibility to respect" are appropriate.
- **Moderate Embodiment:** A social media platform like Facebook or Instagram, which uses profile pictures, videos, and real names, has a moderate degree of embodiment. The user's identity is more closely tied to their physical self, and harms like harassment can feel more personal. Responsibilities here are greater, as reflected in the extensive (if often controversial) community standards these platforms enforce.
- **Medium-High Embodiment**: Video-based traditional platforms and immersive AR experiences—many of which are still developing—will likely possess medium-high embodiment. Experiences like virtual overlays are more immersive than traditional two-dimensional platforms, and can be psychologically impactful, but are embodied to a lesser degree than full VR.
- **High Embodiment:** An immersive VR platform like *Horizon Worlds* or *VRChat* represents the highest degree of embodiment. Through avatars, spatial audio, and motion tracking, these platforms generate powerful feelings of presence, co-presence, and body ownership. Interactions are experienced viscerally, and the platform itself might function as a navigable, three-dimensional social space.

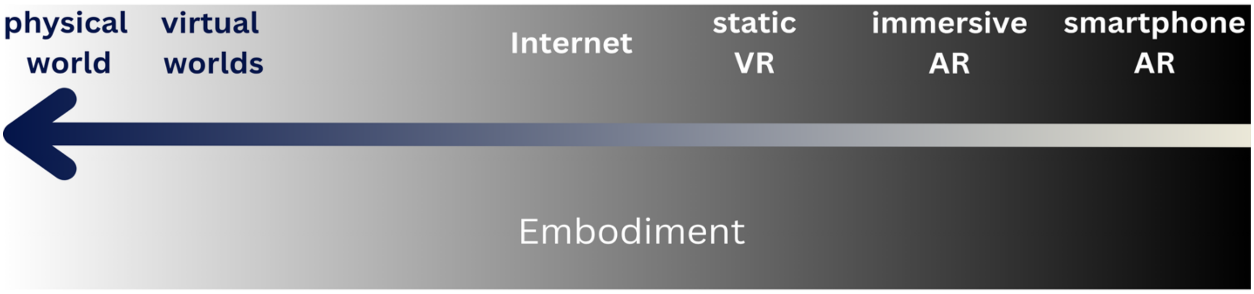

Figure 1: The Embodiment Spectrum

As a platform's capacity to mediate an embodied experience increases, its function shifts from that of a simple content host to that of a governor of a socio-technical environment. At high levels of embodiment, the platform's function becomes nearly analogous to the company town in *Marsh*. It is the constitutive "space" where social life happens, where assemblies gather, and where expression is performed. It is at this point that its responsibilities must escalate. For instance, removing an AR filter may restrict assembly—especially if part of an app used by protestors to guide participants—but would not be an insurmountable obstacle. However, preventing people from gathering at all in VR would create an impassable barrier to gathering (a prior restraint in some jurisdictions) and should be treated with more scrutiny.[133]

8.4.3. *A Heightened Duty of Fair Procedure*

This scalar public function argument leads directly to a specific, actionable consequence: a heightened duty of fair procedure. The doctrine of fair procedure (also called "natural justice" in some jurisdictions ("Procedural Fairness" 2022)) requires some private actors to provide rudimentary due process when taking significant actions (Diaz and Ty 2000; *Potvin v. Metropolitan Life Ins. Co.* 2000). This thus provides

[133] In both scenarios, individuals are (also) still fully embodied in the physical world, and the state still has a responsibility to uphold their human rights, so in the case of the AR-enabled protest, if people still manage to gather despite the lack of AR guidance, the state should not arbitrarily disperse them.

individuals with a layer of private protection—the company must provide a fair process before taking drastic action and allow for appeal and redress (a principle supported by the Santa Clara Principles on Transparency and Accountability in Content Moderation (Santa Clara Principles 2021))—but also public protection, as the state can compel the private actor to act when it does not adhere to the procedure.

When a high-embodiment IXR platform takes an action that infringes on fundamental rights—such as algorithmically dispersing a virtual assembly, silencing an avatar's speech, or banishing a user from the environment—the impact is qualitatively different from a simple content takedown on a website. It is an act of governance within a quasi-public, albeit virtual, space. Therefore, such platforms have a heightened responsibility to provide robust fair procedure. This includes clear and content-neutral rules; the "laws" of the virtual world, governing time, place, and manner of assembly and expression should be published in advance and applied neutrally. Additionally, enforcement must be transparent. Users whose rights are restricted must be given a clear statement of reasons, specifying the rule violated and whether the decision was automated, as outlined in the DSA[134] (Art. 17). Finally, users—and impacted non-users—must have access to meaningful avenues for appeal and redress. This must include accessible internal complaint mechanisms and options for independent, out-of-court dispute resolution, allowing for human review of consequential decisions.

This framework provides a principled middle ground in the often-polarized debate over platform governance. It avoids the legally and conceptually fraught claim that "platforms are states" and the methodologically fraught effort of trying to outline every possible scenario and outcome. Instead, it offers a nuanced criterion—the degree of embodiment—for determining when and to what extent a platform's responsibilities should approach those of a public authority with respect to procedural fairness. This heuristic is both flexible and future-proofed. It justifies imposing stricter procedural obligations on immersive virtual worlds than on a simple blog hosting service, without needing to create entirely new

134 (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) 2022)

legal categories for every new technology. It directly links the unique technological affordances of IXR, analyzed throughout this dissertation, to a specific and heightened governance obligation.

8.4.4. The Limitations of Existing Models

While IXR platforms will still face difficult jurisdictional questions as long as different countries have different standards for freedom of speech, my proposed model provides a guide for how to approach content moderation, user protection, and other issues that impact human rights in virtual contexts. It allows for platforms to moderate conduct and content to keep their platforms safe for a diverse userbase, while recognizing the importance of these platforms to modern life and communication and the impact that embodied virtual experiences have on our well-being. This is a novel approach with philosophical implications for embodiment and human rights that will be explored in a subsequent paper. Other IXR governance solutions have been proposed, so here I discuss two and their inadequacies.

One alternative proposed solution for the problem of legitimacy of rights governance in IXR is publicly owned virtual worlds (or "metaverses') administered by governments, from the city to the national level ("Finland Metaverse Strategy," n.d.; Thomson 2023). This would obligate the jurisdiction to uphold rights according to its laws and interpretations. Because of different interpretations of rights across countries, this could lead to a network of IXR platforms with different standards for assembly and expression. This would be particularly noticeable in VR, where national metaverses would result in assembly and expression standards changing rapidly as users travel between platforms. While national governments could make the same arbitrary restrictive decisions that this thesis has discussed in the context of platform companies, they ostensibly should have more accountability through national and international judiciaries and thus could be a more legitimate form of IXR governance.

Another proposal is to regulate IXR (and the infosphere more broadly) like a commons (Floridi 2021). Condominiums and gated communities are owned and governed by their residents, who have a say in the community governance and rules (Treffers and Lippert 2020; Le Goix and Webster 2008). This is the model adopted by so-called "decentralized metaverses," which are VR worlds owned and governed by a community (Alsamhi et al. 2023). Though often intertwined with cryptocurrency and other "Web3.0" topics *du jour*, the seed of the idea—descended from the community governance of Reddit and other social media platforms—could be a model for ground-up community ownership and governance in a way that could be on par with the state governed model in terms of democratic participation. In practice, though, large corporations are the entities with the resources to develop IXR technologies and platforms, meaning they will likely play a primary role in IXR governance, so determining how they can do so while respecting rights is of paramount importance. Additionally, the public and cooperatively owned models primarily deal with VR and "metaverse" environments, but IXR governance must go beyond this. The embodiment and public function approach accounts for the spectrum of IXR applications, implying that the more embodied a user is on a platform, the closer those rights are to their physical equivalents, and the more responsibility a company has to uphold human rights and ensure that fair procedure is followed when restricting them.

This can apply beyond just assembly and expression to other human rights, and beyond IXR to less immersive platforms. While there is extensive debate over traditional social media content moderation, considering it from a perspective of embodiment offers an alternative way to think about the level of responsibility that platforms have. Even traditional social media, while not immersive, is still embodied to some degree; we create online personas through profile pictures and the content we post (Hine 2024b). Thus, social media platforms have an obligation to uphold basic levels of free assembly and speech. While this should not infringe on their ability to moderate their platforms to ensure safe and pleasant experiences for their users, it should restrict them from, for example, arbitrary news censorship (Morrow 2024; Davies 2022). While it is accepted that traditional social media platforms can be governed in a top-down fashion, reliance on the state will lead to inevitable jurisdictional clashes in IXR environments, so a combination of this model plus aspects of community governance may be a more desirable blend of legitimacy and consistency in immersive environments.

8.5. Limitations and Avenues for Future Research

This dissertation is subject to several limitations. First, having just proposed a guiding framework for XR governance, I must note that the implementation of this framework—including legal and platform mechanisms for enforcement and formalizing the shift from a duty of respect to one of stewardship—would likely require another dissertation to explore; implementation will vary based on what kind of XR is in play, how specific jurisdictions protect specific rights, the structure of a platform and government, and whether a jurisdiction relies on common law or civil law, so I leave it to future work.

The dissertation's approach does carry methodological limitations. The analysis presented here is primarily theoretical and legal-doctrinal, supplemented by a GELSI-informed approach. It relies on synthesizing existing literature from computer science, psychology, law, and philosophy to build its arguments about harm and user experience. It does not include new primary empirical data. While the conclusions are grounded in a robust review of existing evidence, they remain, in part, predictive and conceptual.

This work also has a clear jurisdictional focus on the European Union. This focus was justified by the EU's proactive regulatory posture and the global impact of the "Brussels Effect." However, this means that the specific legal conclusions and policy recommendations, which are tied to instruments like the GDPR, DSA, and CSDDD, may not be directly transferable to other major legal systems. The approach to platform regulation in the United States, for example, differs significantly—with the First Amendment limiting government regulation of private platform moderation, and a lighter-touch regulatory philosophy historically. Other regions, like East Asia or Latin America, may bring different values and approaches to XR governance. Comparative legal analysis of how different jurisdictions' laws apply to XR (and where they clash or converge) is a ripe area for future work.

The scope of rights analyzed was deliberately narrowed to a core set of civil and political rights: safety, privacy, and the freedoms of assembly and expression. This was necessary to allow for a deep and tractable analysis. However, IXR will have profound implications for a much wider range of fundamental rights that this dissertation did not deeply investigate, including labor rights in virtual workplaces, the right to education in immersive learning environments, economic and property rights in virtual economies, and the right to health in clinical VR applications.

Additionally, the subject matter is characterized by technological fluidity. This research is based on the current and near-future trajectory of IXR technology—head-mounted displays, AR glasses, and their associated software platforms. As the technology evolves, particularly with the advent of new mass-market AR devices and the potential integration of more advanced haptics, brain-computer interfaces, and AI-driven generative worlds, the specific risk landscape will undoubtedly change. The proposed governance framework is designed to be flexible, but its application will require continuous re-evaluation in light of technological advancements.

This work traversed law, philosophy, and technology studies, but there remain interdisciplinary gaps to explore. One such gap is between legal/policy analysis and the technical design realm. Ensuring fundamental rights in XR is not only about writing laws or policies but also about engineering platforms in a certain way. Future research into "rights by design" at the intersection of computer science, HCI, and ethics could delve deeper into technical frameworks or tools that embed rights protections. Collaboration between technologists and legal scholars will be valuable to translate normative goals into practical features.

Part of this effort may involve the consideration of new human rights, which could go as far as to consider the expansion of personality rights to avatars and the right to "mental self-determination" (Madary and Metzinger 2016); the rights to experiential authenticity, emotional privacy, and behavioral privacy (Rosenberg 2022b); "neurorights" to physical and mental integrity and the protection of brain activity and related data, as enshrined in Chile's new constitution (McCay 2022). The feasibility and necessity of some of these proposals have been questioned (Bublitz 2022), with some instead suggesting an expansive conception of human rights to challenge the datafication of our physical and virtual worlds (Renieris 2023) or a broader interpretation of the right to freedom of thought (Hertz 2022) to protect mental self-determination. This work, by centering our existing fundamental rights regime, takes the stance that what we need are not necessarily new rights, but appropriate interpretations of our existing rights. Still, some of these ideas could be a fruitful avenue to further explore how emerging technologies impact our understanding of fundamental rights.

8.6. Concluding Remarks

This dissertation opened by invoking two foundational statements: the Human Rights Council's affirmation that offline rights must be protected online, and Lawrence Lessig's warning about privately managed architectures of control. The journey through the technological, philosophical, and legal landscape of immersive extended reality has demonstrated that this principle and this warning are both more urgent and more complex than ever before. In the age of IXR, the "online" world is no longer a separate space one visits through a screen; it is an immersive layer of experience that is increasingly woven into the fabric of our "onlife" (Floridi 2015).

Ensuring that our transition from the physical world to a mediated reality does not result in a diminution of fundamental rights is one of the paramount challenges of our time. It requires a deliberate, proactive, and principled approach to governance—one that recognizes the unique power of those who build these new worlds and holds them to a standard of responsibility commensurate with that power. We do not abandon our fundamental rights at the virtual door. The architectures of control of these new spaces may be privately built, but they can be built not just on hardware and software, but also respect for our fundamental rights. This dissertation has sought to provide a robust conceptual and normative framework for beginning that essential work. And it is essential, for our future extended reality depends on it.

Works Cited

Abraham, Melvin, Pejman Saeghe, Mark Mcgill, and Mohamed Khamis. 2022. "Implications of XR on Privacy, Security and Behaviour: Insights from Experts." *Nordic Human-Computer Interaction Conference* (New York, NY, USA), NordiCHI '22, October 8, 1–12. https://doi.org/10.1145/3546155.3546691.

Access Now. n.d. "Access Now." Accessed September 16, 2025. https://www.accessnow.org/.

Adhanom, Isayas Berhe, Paul MacNeilage, and Eelke Folmer. 2023. "Eye Tracking in Virtual Reality: A Broad Review of Applications and Challenges." *Virtual Reality* 27 (2): 1481–505. https://doi.org/10.1007/s10055-022-00738-z.

Aghajan, Zahra M., Lavanya Acharya, Jason J. Moore, Jesse D. Cushman, Cliff Vuong, and Mayank R. Mehta. 2015. "Impaired Spatial Selectivity and Intact Phase Precession in Two-Dimensional Virtual Reality." *Nature Neuroscience* 18 (1): 121–28. https://doi.org/10.1038/nn.3884.

Aguiar, Luis, Christian Peukert, Maximilian Schäfer, and Hannes Ullrich. 2022. "Facebook Shadow Profiles." arXiv:2202.04131. Preprint, arXiv, July 19. https://doi.org/10.48550/arXiv.2202.04131.

Ajana, Btihaj. 2005. *Disembodiment and Cyberspace: A Phenomenological Approach.*

Alien's Action for Tort, 28 U.S. Code § 1350 (1948). https://www.law.cornell.edu/uscode/text/28/1350.

Alriksson, Fredrik, Du Ho Kang, Chris Phillips, Jose Luis Pradas, and Ali Zaidi. 2021. "XR and 5G: Extended Reality at Scale with 5G Networks." Ericcson Technology Review, August 24. https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/xr-and-5g-extended-reality-at-scale-with-time-critical-communication.

Alsamhi, Saeed Hamood, Ammar Hawbani, Santosh Kumar, Lukasz Porwol, and Edward Curry. 2023. "Decentralized Metaverse: Towards a Secure, Autonomous, and Inclusive Virtual World." *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, November, 1–7. https://doi.org/10.1109/ICECET58911.2023.10389478.

Alsop, Thomas. 2022. "Topic: XR: AR, VR, and the Metaverse." Statista, October 20. https://www.statista.com/topics/6072/extended-reality-xr/.

Amnesty International. 2022. "Myanmar: The Social Atrocity: Meta and the Right to Remedy for the Rohingya." *Amnesty International*, September 29. https://www.amnesty.org/en/documents/asa16/5933/2022/en/.

Anderson, Janna, and Lee Rainie. 2022. "The Metaverse in 2040." June 30. https://eloncdn.blob.core.windows.net/eu3/sites/964/2022/06/Metaverse-in-2040-Elon-Univ-Pew-Research-06-30-22.pdf.

Andrejevic, Mark. 2013. "Public Service Media Utilities: Rethinking Search Engines and Social Networking as Public Goods." *Media International Australia* 146 (1): 123–32. https://doi.org/10.1177/1329878X1314600116.

Ang, Samuel, and John Quarles. 2023. "Reduction of Cybersickness in Head Mounted Displays Use: A Systematic Review and Taxonomy of Current Strategies." *Frontiers in Virtual Reality* 4. https://www.frontiersin.org/articles/10.3389/frvir.2023.1027552.

ANSES. 2014. "3D Technologies and Eyesight: Use Not Recommended for Children under the Age of Six, Use in Moderation for Those under the Age of 13." Anses - Agence Nationale de Sécurité Sanitaire de l'alimentation, de l'environnement et Du Travail, November 6. https://www.anses.fr/en/content/3d-technologies-and-eyesight-use-not-recommended-children-under-age-six-use-moderation-0.

Apple, dir. 2023. *Introducing Apple Vision Pro*. 9:11. https://www.youtube.com/watch?v=TX9qSaGXFyg.

Apple. 2024. "If You Need Help with Eye Setup on Apple Vision Pro." Apple Support, November 14. https://support.apple.com/en-us/118513.

Apple. 2025a. "Get Started with Accessibility Features on Apple Vision Pro." Apple Support, July. https://support.apple.com/guide/apple-vision-pro/get-started-with-accessibility-features-tan426c48bdc/visionos.

Apple. 2025b. "Use Gestures with Apple Vision Pro." Apple Support, March 8. https://support.apple.com/en-us/117741.

Apple. n.d.-a. "Apple Vision Pro." Accessed October 6, 2025. https://www.apple.com/apple-vision-pro/.

Apple. n.d.-b. "Learn Basic Gestures and Controls on Apple Vision Pro." Apple Support. Accessed October 6, 2025. https://support.apple.com/guide/apple-vision-pro/basic-gestures-and-controls-tan1e2a29e00/visionos.

Apple. n.d.-c. "Use Voice Control to Interact with Apple Vision Pro." Apple Support. Accessed October 6, 2025. https://support.apple.com/guide/apple-vision-pro/perform-actions-with-your-voice-tan14d179ad1/visionos.

Apple Legal. n.d. "Face ID & Privacy." Accessed February 13, 2023. https://www.apple.com/legal/privacy/data/en/face-id/.

Aquino, Steven. 2016. "The iPad Pro Is the Most Accessible Computer Apple Has Ever Built." TechCrunch, April 10. https://techcrunch.com/2016/04/10/the-ipad-pro-is-the-most-accessible-computer-apple-has-ever-built/.

Artaud, Antonin. 1938. *Le Théâtre et Son Double*. Gallimard. https://gallica.bnf.fr/ark:/12148/bpt6k856920z.

Artzt, Matthias. 2022. *Metaverse and Privacy*. August 23. https://iapp.org/news/a/metaverse-and-privacy-2/.

Aubrey, Elizabeth. 2024. "Graphic Taylor Swift Deepfake AI Images Linked to 4chan Challenge." *NME*, February 5. https://www.nme.com/news/music/graphic-taylor-swift-deepfake-imahes-linked-to-4chan-challenge-3582813.

Awan, Imran. 2017. "Cyber-Extremism: Isis and the Power of Social Media." *Society* 54 (2): 138–49. https://doi.org/10.1007/s12115-017-0114-0.

Axelsson, Ann-Sofie. 2002. "The Digital Divide: Status Differences in Virtual Environments." In *The Social Life of Avatars*, edited by Ralph Schroeder. Computer Supported Cooperative Work, edited by Dan Diaper and Colston Sanger. Springer London. https://doi.org/10.1007/978-1-4471-0277-9_11.

Ayoubi, Ayda. 2017. "IKEA Launches Augmented Reality Application." Architect, September 21. https://www.architectmagazine.com/technology/ikea-launches-augmented-reality-application.

Bagheri, Roya. 2016. "Virtual Reality: The Real Life Consequences." *UC Davis Business Law Journal* 17 (1): 101–20.

Bagheri, Roya. 2017. "Virtual Reality: The Real Life Consequences." *UC Davis Business Law Journal* 17 (March): 102–20.

Bailey, Jakki O., Jeremy N. Bailenson, Jelena Obradović, and Naomi R. Aguiar. 2019. "Virtual Reality's Effect on Children's Inhibitory Control, Social Compliance, and Sharing." *Journal of Applied Developmental Psychology* 64 (July): 101052. https://doi.org/10.1016/j.appdev.2019.101052.

Baker, Gordon, Katherine Morris, and Baker Gordon. 1995. *Descartes' Dualism*. Taylor & Francis Group. http://ebookcentral.proquest.com/lib/unibo/detail.action?docID=241820.

Baker, Stephen, and Dylan Cutifani. 2025. "The Parent Trap: When UK Companies Face Liability for Overseas Harm." *Herrington Carmichael*, June 19. https://www.herrington-carmichael.com/the-parent-trap-when-uk-companies-face-liability-for-overseas-harm/.

Baker-White, Emily. 2022. "Meta Wouldn't Tell Us How It Enforces Its Rules In VR, So We Ran A Test To Find Out." *Buzzfeed News*, February 11. https://www.buzzfeednews.com/article/emilybakerwhite/meta-facebook-horizon-vr-content-rules-test.

Balcerak Jackson, Magdalena, and Brendan Balcerak Jackson. 2024. "Immersive Experience and Virtual Reality." *Philosophy & Technology* 37 (1): 19. https://doi.org/10.1007/s13347-024-00707-1.

Balkin, Jack M. 2014. "Old School/New School Speech Regulation." *Harvard Law Review* 127 (8): 2296–342.

Ball, James. 2025. "Free Expression Concerns over Online Safety Act's Age Verification Requirements." *Index on Censorship*, July 30. https://www.indexoncensorship.org/2025/07/free-expression-concerns-over-online-safety-acts-age-verification-requirements/.

Ball, Matthew. 2022. *The Metaverse: And How It Will Revolutionize Everything*. Liveright Publishing.

Balsamo, Anne. 1996. "The Virtual Body in Cyberspace." In *Technologies of the Gendered Body: Reading Cyborg Women*. Duke University Press.

Banakou, Domna, Raphaela Groten, and Mel Slater. 2013. "Illusory Ownership of a Virtual Child Body Causes Overestimation of Object Sizes and Implicit Attitude Changes." *Proceedings of the National Academy of Sciences* 110 (31): 12846–51. https://doi.org/10.1073/pnas.1306779110.

Banakou, Domna, Parasuram D. Hanumanthu, and Mel Slater. 2016. "Virtual Embodiment of White People in a Black Virtual Body Leads to a Sustained Reduction in Their Implicit Racial Bias." *Frontiers in Human Neuroscience* 10 (November). https://doi.org/10.3389/fnhum.2016.00601.

Banakou, Domna, Sameer Kishore, and Mel Slater. 2018. "Virtually Being Einstein Results in an Improvement in Cognitive Task Performance and a Decrease in Age Bias." *Frontiers in Psychology* 9 (June). https://doi.org/10.3389/fpsyg.2018.00917.

Bardhan, Ashley. 2022. "Men Are Creating AI Girlfriends and Then Verbally Abusing Them." Futurism, January 18. https://futurism.com/chatbot-abuse.

Barendt, Eric. 2007. *Freedom of Speech*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199225811.001.0001.

Barlow, John Perry. 1990a. "Being in Nothingness Virtual Reality and the Pioneers of Cyberspace." *Mondo 2000*.

Barlow, John Perry. 1990b. "Scratching Your Eyes Back In: John Barlow Interviews Jaron Lanier." *Mondo 2000*.

Barreda-Ángeles, Miguel, and Tilo Hartmann. 2022. "Hooked on the Metaverse? Exploring the Prevalence of Addiction to Virtual Reality Applications." *Frontiers in Virtual Reality* 3. https://www.frontiersin.org/articles/10.3389/frvir.2022.1031697.

Basu, Tanya. 2021. "The Metaverse Has a Groping Problem Already." MIT Technology Review, December 21. https://www.technologyreview.com/2021/12/16/1042516/the-metaverse-has-a-groping-problem/.

Bavana, K. 2021. "Privacy in the Metaverse." *Jus Corpus Law Journal* 2 (3): 1–11.

Beck, Canary. 2015. "Survey: Women in Second Life Less Private About Their RL Than Men - and Harassed Much More." New World Notes, September 3. https://nwn.blogs.com/nwn/2015/09/online-second-life-mmo-harassment.html.

Beck, Julia, Mattia Rainoldi, and Roman Egger. 2019. "Virtual Reality in Tourism: A State-of-the-Art Review." *Tourism Review* 74 (3): 586–612. https://doi.org/10.1108/TR-03-2017-0049.

"Behind the Scenes of 'IN PROTEST' with Alton Glass and Adam Davis-McGee." n.d. Accessed April 19, 2024. https://www.oculus.com/blog/behind-the-scenes-of-in-protest-with-alton-glass-and-adam-davis-mcgee/.

Belamire, Jordan. 2016. "My First Virtual Reality Groping." *Athena Talks*, October 22. https://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee.

Belic, Jelena, Matthew Canfield, Rachel Griffin, Henning Lahmann, and Barrie Sander. 2024. "The Promise and Perils of Human Rights for Governing Digital Platforms: Symposium Introduction." Tech Policy Press, June 18. https://techpolicy.press/the-promise-and-perils-of-human-rights-for-governing-digital-platforms-symposium-introduction.

Berardo, Jackie. 2024. "Gucci, Louis Vuitton, And Dior Bring 'Quiet Luxury' To Crypto In 2024." Forbes, March 1. https://www.forbes.com/sites/digital-assets/2024/03/01/gucci-louis-vuitton-and-dior-bring-quiet-luxury-to-crypto-in-2024/.

Beres, Nicole A, Julian Frommel, Elizabeth Reid, Regan L Mandryk, and Madison Klarkowski. 2021. "Don't You Know That You're Toxic: Normalization of Toxicity in Online Gaming." *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA), CHI '21, May 7, 1–15. https://doi.org/10.1145/3411764.3445157.

Berg, Leif P., and Judy M. Vance. 2017. "Industry Use of Virtual Reality in Product Design and Manufacturing: A Survey." *Virtual Reality* 21 (1): 1–17. https://doi.org/10.1007/s10055-016-0293-9.

Bertuzzi, Luca. 2022. "Leading Lawmakers Pitch Extending Scope of AI Rulebook to the Metaverse." Www.Euractiv.Com, September 29. https://www.euractiv.com/section/digital/news/leading-lawmakers-pitch-extending-scope-of-ai-rulebook-to-the-metaverse/.

Bevir, Mark. 2012. *Governance: A Very Short Introduction*. OUP Oxford.

Beyene, Luel Hagos, Vivek Verma, Min Ma, et al. 2025. "mSTEB: Massively Multilingual Evaluation of LLMs on Speech and Text Tasks." arXiv:2506.08400. Preprint, arXiv, June 25. https://doi.org/10.48550/arXiv.2506.08400.

Bhat, P. Ishwara. 2020. "Doctrinal Legal Research as a Means of Synthesizing Facts, Thoughts, and Legal Principles." In *Idea and Methods of Legal Research*, edited by P. Ishwara Bhat. Oxford University Press. https://doi.org/10.1093/oso/9780199493098.003.0005.

Big Brother Watch and Others v. the United Kingdom, 58170/13, 62322/14, 24960/15 (ECtHR [GC] May 25, 2021). https://hudoc.echr.coe.int/eng?i=001-210077.

"Binding Decision 3/2022 on the Dispute Submitted by the Irish SA on Meta Platforms Ireland Limited and Its Facebook Service (Art. 65 GDPR)." 2022. December 5. https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-32022-dispute-submitted_en.

Black, Julia. 2020. "Critical Reflections on Regulation." *Australasian Journal of Legal Philosophy* 27 (2002): 1–46. https://doi.org/10.3316/ielapa.200206927.

Blackwell, Lindsay, Nicole Ellison, Natasha Elliott-Deflo, and Raz Schwartz. 2019. "Harassment in Social Virtual Reality: Challenges for Platform Governance." *Proceedings of the ACM on Human-Computer Interaction* 3 (CSCW): 1–25. https://doi.org/10.1145/3359202.

Blanchard, Chuck, Scott Burgess, Young Harvill, et al. 1990. "Reality Built for Two: A Virtual Reality Tool." *ACM SIGGRAPH Computer Graphics* 24 (2): 35–36. https://doi.org/10.1145/91394.91409.

Blum, Paul Richard. 2019. *Substance Dualism in Descartes*. September 10. https://press.rebus.community/intro-to-phil-of-mind/chapter/substance-dualism-in-descartes-2/.

Bogost, Ian, and Nick Montfort. 2009. *Platform Studies: Frequently Questioned Answers*. December 12. https://escholarship.org/uc/item/01r0k9br.

Bohn, Dieter. 2014. "Google Glass Just Got a Lot Less Geeky." The Verge, January 28. https://www.theverge.com/2014/1/28/5352592/google-glass-prescription-lenses-frames-titanium-collection.

Boine, Claire. 2025. "The AI Act Manipulation Gap." *Emory International Law Review* 39 (2): 417.

Boler, Megan. 2007. "Hypes, Hopes and Actualities: New Digital Cartesianism and Bodies in Cyberspace." *New Media & Society* 9 (1): 139–68. https://doi.org/10.1177/1461444807067586.

Botvinick, Matthew, and Jonathan Cohen. 1998. "Rubber Hands 'Feel' Touch That Eyes See." *Nature* 391 (6669): 756–756. https://doi.org/10.1038/35784.

Boyer, Steven. 2009. "Virtual Failure." *The Velvet Light Trap*, no. 64: 23–35.

Bradford, Anu. 2020. *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

Bradford, Anu. 2024. "The False Choice Between Digital Regulation and Innovation." *Nw. U. L. Rev.* 19 (October): 377.

Brandeis, Louis D. 1890. *The Right to Privacy*. With JSTOR. Harvard Law Review. http://archive.org/details/jstor-1321160.

Bridges, R (On the Application Of) v South Wales Police [2020] EWCA Civ 1058 (EWCA (Civ) August 11, 2020). https://www.bailii.org/ew/cases/EWCA/Civ/2020/1058.html.

Britt, Aaron. 2008. "Avatar." Magazine. *The New York Times*, August 8. https://www.nytimes.com/2008/08/10/magazine/10wwln-guest-t.html.

Bruckman, Amy. 1996. "Gender Swapping on the Internet." In *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*, by Peter Ludlow.

Bryant, Jennifer. 2023. *Irish DPC, EDPB Meta Decisions Raise Complex, Fundamental Questions*. January 13. https://iapp.org/news/a/irelands-meta-decisions-raise-complex-fundamental-questions/.

Bublitz, Jan Christoph. 2022. "Novel Neurorights: From Nonsense to Substance." *Neuroethics* 15 (1): 7. https://doi.org/10.1007/s12152-022-09481-3.

Bugeja, Michael J. 2008. "Second Thoughts About Second Life." *Education Digest* 73 (5): 18–22.

Bujić, Mila, Mikko Salminen, Joseph Macey, and Juho Hamari. 2020. "'Empathy Machine': How Virtual Reality Affects Human Rights Attitudes." *Internet Research* 30 (5): 1407–25. https://doi.org/10.1108/INTR-07-2019-0306.

Buolamwini, Joy, and Timnit Gebru. 2018. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, January 21, 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html.

Bureau of Labor Statistics. n.d. "CPI Inflation Calculator." Accessed September 18, 2025. https://www.bls.gov/data/inflation_calculator.htm.

Burrows, Emma, Dasha Litvinova, and Jim Heintz. 2024. "Putin Extends Rule in Preordained Russian Election after Harshest Crackdown since Soviet Era." Los Angeles Times, March 18. https://www.latimes.com/world-nation/story/2024-03-18/putin-extends-rule-in-preordained-russian-election-after-harshest-crackdown-since-soviet-era.

Business Help Center. n.d. "Sponsored Lenses Overview." Accessed April 16, 2024. https://businesshelp.snapchat.com/s/article/lenses?language=en_US.

Bylieva, Daria, Zafer Bekirogullari, Victoria Lobatyuk, and Tatiana Nam. 2021. "How Virtual Personal Assistants Influence Children's Communication." In *Knowledge in the Information Society*, edited by Daria Bylieva, Alfred Nordmann, Olga Shipunova, and Violetta Volkova. Lecture Notes in Networks and Systems. Springer International Publishing. https://doi.org/10.1007/978-3-030-65857-1_12.

Campoamor, Danielle. 2022. “New Report Reveals the Dangers of Virtual Reality for Young Children.” TODAY.Com, March 24. https://www.today.com/parents/parents/dangers-virtual-reality-young-children-rcna21278.

Canales, Katie. 2022. “Silicon Valley Says Kids over the Age of 13 Can Handle the Big, Bad World of Social Media. Experts Say That’s the Result of a ‘problematic’ 1990s Internet Law.” Business Insider, January 14. https://www.businessinsider.com/why-you-must-be-13-facebook-instagram-problematic-law-coppa-2022-1.

Canbay, Yavuz, Anil Utku, and Pelin Canbay. 2022. “Privacy Concerns and Measures in Metaverse: A Review.” *2022 15th International Conference on Information Security and Cryptography (ISCTURKEY)*, October, 80–85. https://doi.org/10.1109/ISCTURKEY56345.2022.9931866.

Cao, Jiaxun, Abhinaya S. B, Anupam Das, and Pardis Emami-Naeini. 2024. “Understanding Parents’ Perceptions and Practices Toward Children’s Security and Privacy in Virtual Reality.” *2024 IEEE Symposium on Security and Privacy (SP)*, May 19, 1554–72. https://doi.org/10.1109/SP54263.2024.00222.

Carman, Taylor. 1999. “The Body in Husserl and Merleau-Ponty.” *Philosophical Topics* 27 (2): 205–26.

Carpenter, Nicole. 2018. “On ‘The Palace,’ You Can Be Anyone You Want to Be.” The Outline, May 29. https://theoutline.com/post/3964/the-palace-game-history.

Carpenter v. United States, No. 16-402 (US Supreme Court June 22, 2018). https://www.oyez.org/cases/2017/16-402.

Carter, Rebekah. 2024. “The Top AR Smart Glasses Vendors for 2024.” *XR Today*, April 1. https://www.xrtoday.com/mixed-reality/the-top-ar-smart-glasses-vendors-for-2024/.

Center for Countering Digital Hate. 2023. *Horizon Worlds Exposed*. Center for Countering Digital Hate. https://counterhate.com/research/horizon-worlds-exposed/.

Chalmers, David J. 2022. *Reality+: Virtual Worlds and the Problems of Philosophy*. W. W. Norton & Company.

Chambers, Rachel, and Anil Yilmaz Vastardis. 2021. “Human Rights Disclosure and Due Diligence Laws: The Role of Regulatory Oversight in Ensuring Corporate Accountability.” *Chicago Journal of International Law* 21 (2). https://cjil.uchicago.edu/print-archive/human-rights-disclosure-and-due-diligence-laws-role-regulatory-oversight-ensuring.

Chan, Jason, Anindya Ghose, and Robert Seamans. 2016. “The Internet and Racial Hate Crime: Offline Spillovers from Online Access.” *MIS Quarterly* 40 (2).

Chang, Patricia. 2018. “U.S. Navy Enlists Virtual And Augmented Reality For Cutting-Edge Training And Recruitment.” October 12. https://arpost.co/2018/10/12/us-navy-virtual-augmented-reality-cutting-edge-training-recruitment/.

Charr, Manuel. 2024. “How Museums Are Using Augmented Reality.” MuseumNext, February 1. https://www.museumnext.com/article/how-museums-are-using-augmented-reality/.

Charter of Fundamental Rights of the European Union, 326 OJ C 391 (2012). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT.

Chemaly, Soraya. 2014. "When It Comes to Harassment and Stalking, the Virtual World IS Real." HuffPost, January 10. https://www.huffpost.com/entry/when-it-comes-to-harassme_b_4577719.

Chemero, Anthony. 2003. "An Outline of a Theory of Affordances." *Ecological Psychology* 15 (2): 181–95. https://doi.org/10.1207/S15326969ECO1502_5.

Chen, Zefeng, Jiayang Wu, Wensheng Gan, and Zhenlian Qi. 2022. *Metaverse Security and Privacy: An Overview*. November 27. https://doi.org/10.48550/arXiv.2211.14948.

Cherny, Lynn. 1994. "Gender Differences in Text-Based Virtual Reality." Paper presented at Berkeley Conference on Women and Language. *Proceedings of the Berkeley Conference on Women and Language*, April.

Chon, Margaret. 2000. "Erasing Race? A Critical Race Feminist View of Internet Identity Shifting." *The Journal of Gender, Race & Justice*, no. 3.

Cicero. 2007. *Tusculan Disputations*. Translated by John Edward King. Harvard University Press.

Clark, Mitchell. 2023. "Google Glass Enterprise Edition Is No More." The Verge, March 15. https://www.theverge.com/2023/3/15/23641872/google-glass-enterprise-edition-discontinued-support.

Clover, Juli. 2025. "Apple Smart Glasses: Everything We Know About Apple's Answer to Meta Ray-Bans." MacRumors, July 11. https://www.macrumors.com/guide/apple-smart-glasses/.

Clubhouse Blog. 2020. "On Community Moderation." October 2. https://blog.clubhouse.com/on-community-moderation/.

Cole, Alex. 2025. "Save the Date! Samsung XR Headset Project Moohan Could Launch on September 29 – At a Much Cheaper Price Than the Apple Vision Pro." *XR Today*, August 28. https://www.xrtoday.com/virtual-reality/save-the-date-samsung-xr-headset-project-moohan-could-launch-on-september-29-at-a-much-cheaper-price-than-the-apple-vision-pro/.

Collins, Jazmin, Crescentia Jung, Yeonju Jang, Danielle Montour, Andrea Stevenson Won, and Shiri Azenkot. 2023. "'The Guide Has Your Back': Exploring How Sighted Guides Can Enhance Accessibility in Social Virtual Reality for Blind and Low Vision People." *Proceedings of the 25th International ACM SIGACCESS Conference on Computers and Accessibility* (New York, NY, USA), ASSETS '23, October 22, 1–14. https://doi.org/10.1145/3597638.3608386.

Commission Directive 2008/63/EC of 20 June 2008 on Competition in the Markets in Telecommunications Terminal Equipment (Codified Version) (Text with EEA Relevance), COM, 162 OJ L (2008). http://data.europa.eu/eli/dir/2008/63/oj/eng.

Commission Notice – Guidance on the Interpretation and Application of Directive 2005/29/EC of the European Parliament and of the Council Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market (Text with EEA Relevance) (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2021_526_R_0001.

Committee of Ministers. 2019. "Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes." Council of Europe, February 13. https://search.coe.int/cm#{%22CoEIdentifier%22:[%22090000168092dd4b%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}.

Committee of Ministers. 2022. "Recommendation of the Committee of Ministers to Member States on the Impacts of Digital Technologies on Freedom of Expression." Council of Europe, April 6. https://search.coe.int/cm?i=0900001680a61729.

Committee on the Internal Market and Consumer Protection. 2023. "Draft Report: Virtual Worlds - Opportunities, Risks and Policy Implications for the Single Market." European Parliament, August 4. https://www.europarl.europa.eu/doceo/document/IMCO-PR-751902_EN.pdf?utm_source=substack&utm_medium=email.

Communications Decency Act of 1995, S.314 (1995). https://www.congress.gov/bill/104th-congress/senate-bill/314.

Consolidated Version of the Treaty on the Functioning of the European Union, 202 OJ C (2016). http://data.europa.eu/eli/treaty/tfeu_2016/art_288/oj/eng.

Costello, P. 1997. "Health and Safety Issues Associated with Virtual Reality-A Review of Current Literature." Advanced VR Research Centre, Loughborough University. https://www.semanticscholar.org/paper/Health-and-Safety-Issues-associated-with-Virtual-of-Costello/21715ff64d02273574f2ded35d7a1525ca529aa0.

Council Directive 85/374/EEC of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products, 210 OB L 29 (1999). http://data.europa.eu/eli/dir/1985/374/1999-06-04/eng.

Council of Europe. 2024. "The Framework Convention on Artificial Intelligence." September 5. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence.

Cowls, Josh. 2023. "The Responsible Governance of Hate Speech in App Stores: The Case of Parler." University of Oxford.

Crawford, Angus, and Tony Smith. 2022. "Metaverse App Allows Kids into Virtual Strip Clubs." Technology. *BBC News*, February 23. https://www.bbc.com/news/technology-60415317.

Creed, Chris, Maadh Al-Kalbani, Arthur Theil, Sayan Sarcar, and Ian Williams. 2024a. "Inclusive AR/VR: Accessibility Barriers for Immersive Technologies." *Universal Access in the Information Society* 23 (1): 59–73. https://doi.org/10.1007/s10209-023-00969-0.

Creed, Chris, Maadh Al-Kalbani, Arthur Theil, Sayan Sarcar, and Ian Williams. 2024b. "Inclusive Augmented and Virtual Reality: A Research Agenda." *International Journal of Human–Computer Interaction* 40 (20): 6200–6219. https://doi.org/10.1080/10447318.2023.2247614.

Cross, Katherine Angel. 2014. "Ethics for Cyborgs: On Real Harassment in an 'Unreal' Place." *Loading... The Journal of the Canadian Game Studies Association* 8 (13): 13. https://journals.sfu.ca/loading/index.php/loading/article/view/140.

Cyber Promotions, Inc. v. American Online, Inc., 948 F. Supp. 436 (Dist. Court, E.D. Pennsylvania 1996).

Darcy, Oliver. 2019. "Louis Farrakhan, Alex Jones and Other 'Dangerous' Voices Banned by Facebook and Instagram." CNN Business, May 2. https://www.cnn.com/2019/05/02/tech/facebook-ban-louis-farrakhan-infowars-alex-jones-milo-laura-loomer/index.html.

Davies, Alys. 2022. *Twitter Reinstates Banned Journalists' Accounts*. December 17. https://www.bbc.com/news/business-64010202.

Davis, Rachel. 2012. "The UN Guiding Principles on Business and Human Rights and Conflict-Affected Areas: State Obligations and Business Responsibilities." *International Review of the Red Cross* 94 (887): 961–79. https://doi.org/10.1017/S1816383113000350.

Davis, Wes. 2023. "Meta's AI for Ray-Ban Smart Glasses Can Identify Objects and Translate Languages." The Verge, December 12. https://www.theverge.com/2023/12/12/23998780/ray-ban-smart-glasses-hey-meta-multimodal-ai-features.

De Gregorio, Giovanni, and Nicole Stremlau. 2023. "Inequalities and Content Moderation." *Global Policy* 14 (5): 870–79. https://doi.org/10.1111/1758-5899.13243.

De Luca, Stefano. 2023. "New Product Liability Directive." European Parliamentary Research Service, February. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739341/EPRS_BRI(2023)739341_EN.pdf.

De Minico, Giovanna. 2015. "Towards an Internet Bill of Rights." *SSRN Electronic Journal*, ahead of print. https://doi.org/10.2139/ssrn.2681186.

De Pasquale, Concetta, Carmela Dinaro, and Federica Sciacca. 2018. "Relationship of Internet Gaming Disorder with Dissociative Experience in Italian University Students." *Annals of General Psychiatry* 17 (1): 28. https://doi.org/10.1186/s12991-018-0198-y.

Del Vicario, Michela, Gianna Vivaldo, Alessandro Bessi, et al. 2016. "Echo Chambers: Emotional Contagion and Group Polarization on Facebook." *Scientific Reports* 6 (1): 1. https://doi.org/10.1038/srep37825.

"Deliberação/2021/622." 2021. Comissão Nacional de Proteção de Dados, May 28. https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121887.

Desai, Nilam. 2018. "Recreation of History Using Augmented Reality." *ACCENTS Transactions on Image Processing and Computer Vision* 4 (February): 1–5. https://doi.org/10.19101/TIPCV.2017.39019.

Desmarais, Anna. 2025. "Denmark Fights Back against Deepfakes with Copyright Protection. What Other Laws Exist in Europe?" Euronews, June 30. https://www.euronews.com/next/2025/06/30/denmark-fights-back-against-deepfakes-with-copyright-protection-what-other-laws-exist-in-e.

DeVon, Cheyenne. 2024. "Apple Calls Its Vision Pro a 'Spatial Computer'—Here's What That Means." CNBC, February 8. https://www.cnbc.com/2024/02/08/apple-calls-its-vision-pro-a-spatial-computer-what-that-means.html.

Dhimolea, Tetyana Kucher, Regina Kaplan-Rakowski, and Lin Lin. 2022. "A Systematic Review of Research on High-Immersion Virtual Reality for Language Learning." *TechTrends* 66 (5): 810–24. https://doi.org/10.1007/s11528-022-00717-w.

Diamond, William A. 1979. "State Action and the Public Function Doctrine: Are There Really Public Functions?" *University of Richmond Law Review* 13 (3).

Diaz, D. S., and M. Y. Ty. 2000. "Termination of a Physician Contract: Fair Procedure under Potvin v. Metropolitan Life." *Managed Care Interface* 13 (11): 77–79.

Dibbell, Julian. 1994. "A Rape in Cyberspace or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society Symposium: Fundamental Rights on the Information Superhighway: Appendix." *Annual Survey of American Law* 1994 (3): 471–90.

Digital, Culture, Media and Sport Committee. 2019. "Psychosocial Harms of Immersive Technologies." UK Parliament, September 12. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1846/184605.htm.

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, C-293/12 (High Court of Ireland December 12, 2013). https://curia.europa.eu/juris/liste.jsf?num=C-293/12.

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on General Product Safety, EP, CONSIL, 011 OJ L (2001). http://data.europa.eu/eli/dir/2001/95/oj/eng.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), EP, CONSIL, 201 OJ L 201 37 (2002). http://data.europa.eu/eli/dir/2002/58/oj/eng.

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market and Amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA Relevance), CONSIL, EP, 149 OJ L (2005). http://data.europa.eu/eli/dir/2005/29/oj/eng.

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws (Text with EEA Relevance)Text with EEA Relevance (2020). http://data.europa.eu/eli/dir/2009/136/2020-12-21/eng.

Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the Coordination of Certain Provisions Laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive), CONSIL, EP, 095 OJ L (2010). http://data.europa.eu/eli/dir/2010/13/oj/eng.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA, EP, CONSIL, 218 OJ L (2013). http://data.europa.eu/eli/dir/2013/40/oj/eng.

Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the Accessibility of the Websites and Mobile Applications of Public Sector Bodies, L 327/1 (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32016L2102.

Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 Amending Directive 2010/13/EU on the Coordination of Certain Provisions Laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) in View of Changing Market Realities, OJ L 303 (2018). https://eur-lex.europa.eu/eli/dir/2018/1808/oj/eng.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive), Pub. L. No. 2022/2555, OJ L 333 80 (2022). https://eur-lex.europa.eu/eli/dir/2022/2555.

Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on Combating Violence against Women and Domestic Violence, PE/33/2024/REV/1 (2024). https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng.

Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on Corporate Sustainability Due Diligence and Amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859 (Text with EEA Relevance) (2025). http://data.europa.eu/eli/dir/2024/1760/2025-04-17/eng.

Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on Liability for Defective Products and Repealing Council Directive 85/374/EEC (Text with EEA Relevance), CONSIL, EP (2024). http://data.europa.eu/eli/dir/2024/2853/oj/eng.

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 Establishing the European Electronic Communications Code (Recast) (Text with EEA Relevance) (2024). http://data.europa.eu/eli/dir/2018/1972/2024-10-18/eng.

"DMA Designated Gatekeepers." n.d. Accessed November 25, 2024. https://digital-markets-act.ec.europa.eu/gatekeepers_en.

Doctor, Austin C., Joel S. Elson, and Sam Hunter. 2022. "The Metaverse Offers a Future Full of Potential – for Terrorists and Extremists, Too." The Conversation, January 7. http://theconversation.com/the-metaverse-offers-a-future-full-of-potential-for-terrorists-and-extremists-too-173622.

Dodge, William S. 2020. "Supreme Court of Canada Recognizes Corporate Liability for Human Rights Violations." UC Davis School of Law, March 26. https://law.ucdavis.edu/faculty-blog/supreme-court-canada-recognizes-corporate-liability-human-rights-violations.

D'Onfro, Jillian. 2016. "Facebook Gives Its Oculus Employees a Dystopian Sci-Fi Book to Get Them Excited about Building the Future." Business Insider, July 27. https://www.businessinsider.com/oculus-gives-all-its-employees-ready-player-one-2016-7.

Döring, Nicola. 2000. "Feminist Views of Cybersex: Victimization, Liberation, and Empowerment." *CyberPsychology and Behavior* 3 (October): 863–84. https://doi.org/10.1089/10949310050191845.

Douglas-Scott, Sionaidh. 1998. "The Hatefulness of Protected Speech: A Comparison of the American and European Approaches." *William & Mary Bill of Rights Journal* 7 (2): 305–46.

Dove, Edward S, and Jiahong Chen. 2021. "What Does It Mean for a Data Subject to Make Their Personal Data 'Manifestly Public'? An Analysis of GDPR Article 9(2)(e)." *International Data Privacy Law* 11 (2): 107–24. https://doi.org/10.1093/idpl/ipab005.

Down, Lee. 2023. "Virtual Reality and the Future of Art Exhibitions." General. *AAA*, May 13. https://artsartistsartwork.com/virtual-reality-and-the-future-of-art-exhibitions/.

Driscoll, Kevin. 2020. "Demography and Decentralization: Measuring the Bulletin Board Systems of North America." *WiderScreen*, no. 23: 2–3.

Driscoll, Kevin. 2022. *The Modem World: A Prehistory of Social Media*. Yale University Press.

Drummond, Katie, Ellis Hamburger, Thomas Houston, et al. 2014. "The Rise and Fall and Rise of Virtual Reality." The Verge, August 25. http://www.theverge.com/a/virtual-reality.

Ducheneaut, Nicolas, Ming-Hui Wen, Nicholas Yee, and Greg Wadley. 2009. "Body and Mind: A Study of Avatar Personalization in Three Virtual Worlds." *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, April 4, 1151–60. https://doi.org/10.1145/1518701.1518877.

Eckhoff, Daniel, Alvaro Cassinelli, Tuo Liu, and Christian Sandor. 2020. "Psychophysical Effects of Experiencing Burning Hands in Augmented Reality." In *Virtual Reality and Augmented Reality*, edited by Patrick Bourdot, Victoria Interrante, Regis Kopper, Anne-Hélène Olivier, Hideo Saito, and Gabriel Zachmann. Springer International Publishing. https://doi.org/10.1007/978-3-030-62655-6_5.

Edelson, Laura. 2024. "Content Moderation in Practice." In *Media and Society After Technological Disruption*, 1st ed., edited by Kyle Langvardt and Justin (Gus) Hurwitz. Cambridge University Press. https://doi.org/10.1017/9781009174411.017.

Edwards, Benj. 2016. "The Lost Civilization of Dial-Up Bulletin Board Systems." The Atlantic, November 4. https://www.theatlantic.com/technology/archive/2016/11/the-lost-civilization-of-dial-up-bulletin-board-systems/506465/.

Egan, Jennifer, and Jaron Lanier. 2022. "City Arts and Lectures: Jennifer Egan and Jaron Lanier." May 15. https://podcasts.apple.com/us/podcast/jennifer-egan-and-jaron-lanier/id1436346407?i=1000561476977.

Egliston, Ben, and Marcus Carter. 2022. "Oculus Imaginaries: The Promises and Perils of Facebook's Virtual Reality." *New Media & Society* 24 (1): 70–89. https://doi.org/10.1177/1461444820960411.

Eisenstein, Elizabeth L. 1980. *The Printing Press as an Agent of Change : Communications and Cultural Transformations in Early-Modern Europe*. With Internet Archive. Cambridge : Cambridge University Press. http://archive.org/details/printingpressasa001-2eise_l3z7.

Elon University. 2020. "Imagining the Internet's Quick Look at the Early History of the Internet." Imagining the Internet. https://www.elon.edu/u/imagining/time-capsule/early-90s/internet-history/.

Equality and Human Rights Commission. 2021. "What Is the Charter of Fundamental Rights of the European Union?" Equality and Human Rights Commission, January 1. https://www.equalityhumanrights.com/human-rights/what-are-human-rights/what-charter-fundamental-rights-european-union.

Eskens, Sarah. 2022. "The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-Depth Review of La Quadrature Du Net and Others and Privacy International - Joined Cases C-511/18, C-512/18 and C-520/18 La Quadrature Du Net and Others [2020] ECLI:EU:C:2020:791; Case C-623/17 Privacy International [2020] ECLI:EU:C:2020:790 Case Notes." *European Data Protection Law Review (EDPL)* 8 (1): 143–55.

Esposito, Lillian. 2018. "Sexual Ageplay in Virtual Reality: Practicing Free Speech Or Producing Child Pornography Part II: Sex & Gender in the Twenty-First Century: Notes." *Cardozo Law Review* 40 (4): 1913–52.

Ess, Charles. 2006. "Ethical Pluralism and Global Information Ethics." *Ethics and Information Technology* 8 (4): 215–26. https://doi.org/10.1007/s10676-006-9113-3.

Ess, Charles. 2015. "Charles Ess—Commentary on The Onlife Manifesto." In *The Onlife Manifesto: Being Human in a Hyperconnected Era*, edited by Luciano Floridi. Springer International Publishing. https://doi.org/10.1007/978-3-319-04093-6_3.

EU Agency for Fundamental Rights. 2018. *Handbook on European Data Protection Law*. 2018 edition. Publications Office of the European Union. http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition.

European Commission. 2021a. "Better Regulation Guidelines." November. https://commission.europa.eu/document/download/d0bbd77f-bee5-4ee5-b5c4-6110c7605476_en?filename=swd2021_305_en.pdf.

European Commission. 2021b. "Shaping Europe's Digital Future." September 15. https://digital-strategy.ec.europa.eu/en/policies.

European Commission. 2022a. "European Declaration on Digital Rights and Principles." December 15. https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles.

European Commission. 2022b. "Proposal for an ePrivacy Regulation." European Commission, June 7. https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation.

European Commission. 2023a. "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: An EU Initiative on Web 4.0 and Virtual Worlds: A Head Start in the next Technological Transition." July 11. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0442.

European Commission. 2023b. "Towards the next Technological Transition: Commission Presents EU Strategy to Lead on Web 4.0 and Virtual Worlds." July 11.

European Commission. 2025a. "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Commission Work Programme 2025: Moving Forward Together: A Bolder, Simpler, Faster Union." February 11. https://commission.europa.eu/strategy-and-policy/strategy-documents/commission-work-programme/commission-work-programme-2025_en.

European Commission. 2025b. "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Amending Regulations (EU) 2016/679, (EU)

2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as Regards the Simplification of the Digital Legislative Framework, and Repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)." European Commission, November 19. https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal.

European Commission. 2025c. "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as Regards the Simplification of the Implementation of Harmonised Rules on Artificial Intelligence (Digital Omnibus on AI)." European Commission, November 19. https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal.

European Commission. 2025d. "The Virtual and Augmented Reality Industrial Coalition." June 13. https://digital-strategy.ec.europa.eu/en/policies/virtual-and-augmented-reality-coalition.

European Commission. n.d. "Consumer Protection Cooperation Network." European Commission. Accessed October 2, 2025. https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/consumer-protection-cooperation-network_en.

European Court of Human Rights. 2022. "Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Private and Family Life, Home and Correspondence." August 31. https://www.echr.coe.int/documents/guide_art_8_eng.pdf.

European Declaration on Digital Rights and Principles for the Digital Decade, PUB/2023/89, OJ C (2023). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001.

European Parliament. 2018. "The Universal Declaration of Human Rights and Its Relevance for the European Union." European Parliament.

European Parliament. 2025. "Digital Fairness Act | Legislative Train Schedule." European Parliament, December 14. https://www.europarl.europa.eu/legislative-train/theme-protecting-our-democracy-upholding-our-values/file-digital-fairness-act.

European Parliament Committee on Legal Affairs. 2023. "REPORT on Policy Implications of the Development of Virtual Worlds – Civil, Company, Commercial and Intellectual Property Law Issues." With Ibán García Del Blanco and Axel Voss. European Parliament, December 14. https://www.europarl.europa.eu/doceo/document/A-9-2023-0442_EN.html.

European Union. n.d.-a. "Court of Justice of the European Union." Accessed September 19, 2025. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/court-justice-european-union-cjeu_en.

European Union. n.d.-b. "Policy, Law – Decision-Making Process." Accessed September 19, 2025. https://european-union.europa.eu/institutions-law-budget/law/how-eu-policy-decided_en.

European Union Agency for Fundamental Rights. 2013. "What Are Fundamental Rights?" European Union Agency for Fundamental Rights, July 18. https://fra.europa.eu/en/content/what-are-fundamental-rights.

"Experience Doja Cat's Concert in VR." 2024. *Meta*, January 9. https://about.fb.com/news/2024/01/doja-cat-vr-concert/.

Facebook Help Center. 2014. "What Names Are Allowed on Facebook?" July 2. https://web.archive.org/web/20140702180455/https://www.facebook.com/help/112146705538576.

Falchuk, Ben, Shoshana Loeb, and Ralph Neff. 2018. "The Social Metaverse: Battle for Privacy." *IEEE Technology and Society Magazine* 37 (2): 52–61. https://doi.org/10.1109/MTS.2018.2826060.

Fandom. n.d. "LambdaMOO." https://muds.fandom.com/wiki/LambdaMOO.

Farbstein, Susan H. 2023. "A Good Summer for Human Rights Cases in U.S. Courts: Alien Tort Statute Update." *International Human Rights Clinic*, September 5. https://humanrightsclinic.law.harvard.edu/a-good-summer-for-human-rights-cases-in-u-s-courts-alien-tort-statute-update/.

Farrant, Theo. 2024. "UK Police Launch First Investigation into Virtual Rape in Metaverse." Euronews, January 4. https://www.euronews.com/next/2024/01/04/british-police-launch-first-investigation-into-virtual-rape-in-metaverse.

Faulconbridge, Guy, and Andrew Osborn. 2024. "Thousands of Russians Join Navalny-Inspired 'noon against Putin' Election Protest." Europe. *Reuters*, March 17. https://www.reuters.com/world/europe/noon-against-putin-thousands-russians-turn-out-fulfil-navalnys-last-wish-2024-03-17/.

Fauveau, Valentin, Anastasia K. Filimonov, Renata Pyzik, et al. 2024. "Comprehensive Assessment of Physiological and Psychological Responses to Virtual Reality Experiences." *Journal of Medical Extended Reality* 1 (1): 227–41. https://doi.org/10.1089/jmxr.2024.0020.

Fazlioglu, Müge. 2018. "The Top Five Contested Issues in the EU's Developing ePrivacy Regulation." IAPP, January 3. https://iapp.org/news/a/the-top-5-contested-issues-in-the-eus-developing-eprivacy-regulation/.

Fazlioglu, Müge. 2021. "Next-Gen Privacy: Examining the EU's ePrivacy Regulation." IAPP, February 17. https://iapp.org/news/a/nextgen-privacy-the-eus-eprivacy-regulation.

Fernandez, Manny. 2019. "Epilepsy Foundation Was Targeted in Mass Strobe Cyberattack." U.S. *The New York Times*, December 16. https://www.nytimes.com/2019/12/16/us/strobe-attack-epilepsy.html.

"Finland Metaverse Strategy." n.d. *Digital Finland*. Accessed April 28, 2024. https://www.digitalfinland.org.

Fizek, Sonia, and Monika Wasilewska. 2011. *Embodiment and Gender Identity in Virtual Worlds: Reconfiguring Our "Volatile Bodies."*

Fleck, Joshua J., Zane A. Zook, Janelle P. Clark, et al. 2025. "Wearable Multi-Sensory Haptic Devices." *Nature Reviews Bioengineering* 3 (4): 288–302. https://doi.org/10.1038/s44222-025-00274-w.

Floridi, Luciano. 2005. "The Ontological Interpretation of Informational Privacy." *Ethics and Information Technology* 7 (4): 185–200. https://doi.org/10.1007/s10676-006-0001-7.

Floridi, Luciano. 2008. "The Method of Levels of Abstraction." *Minds and Machines* 18 (3): 303–29. https://doi.org/10.1007/s11023-008-9113-7.

Floridi, Luciano, ed. 2015. "The Onlife Manifesto." In *The Onlife Manifesto: Being Human in a Hyperconnected Era*. Springer International Publishing. https://doi.org/10.1007/978-3-319-04093-6_2.

Floridi, Luciano. 2016. "Tolerant Paternalism: Pro-Ethical Design as a Resolution of the Dilemma of Toleration." *Science and Engineering Ethics* 22 (December). https://doi.org/10.1007/s11948-015-9733-2.

Floridi, Luciano. 2017. "Group Privacy: A Defence and an Interpretation." In *Group Privacy: New Challenges of Data Technologies*, edited by Linnet Taylor, Luciano Floridi, and Bart van der Sloot. Philosophical Studies Series. Springer International Publishing. https://doi.org/10.1007/978-3-319-46608-8_5.

Floridi, Luciano. 2019. "Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical." *Philosophy & Technology* 32 (2): 185–93. https://doi.org/10.1007/s13347-019-00354-x.

Floridi, Luciano. 2020a. "AI and Its New Winter: From Myths to Realities." *Philosophy & Technology* 33 (1): 1–3. https://doi.org/10.1007/s13347-020-00396-6.

Floridi, Luciano. 2020b. "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU." *Philosophy & Technology* 33 (3): 369–78. https://doi.org/10.1007/s13347-020-00423-6.

Floridi, Luciano. 2021. "Trump, Parler, and Regulating the Infosphere as Our Commons." *Philosophy & Technology* 34 (1): 1–5. https://doi.org/10.1007/s13347-021-00446-7.

Floridi, Luciano. 2022. "Metaverse: A Matter of Experience." *Philosophy & Technology* 35 (3): 73. https://doi.org/10.1007/s13347-022-00568-6.

Floridi, Luciano. 2023. *The Green and The Blue: Naive Ideas to Improve Politics in the Digital Age*. John Wiley & Sons.

Fornasier, Mateus De Oliveira. 2024. "Freedom of Expression and the Metaverse: On the Importance of Content Creation for the Emergence of a Complex Environment." *Revista de Investigações Constitucionais* 10 (January): e236. https://doi.org/10.5380/rinc.v10i1.87584.

Fowle, Kyle. 2015. "The Vanguard of Virtual Reality: An Embarrassing Arcade Game." Culture. *The Atlantic*, February 4. https://www.theatlantic.com/entertainment/archive/2015/02/when-vr-was-an-arcade-game/385139/.

Franklin, Matija, Hal Ashton, Rebecca Gorman, and Stuart Armstrong. 2022. "Missing Mechanisms of Manipulation in the EU AI Act." *The International FLAIRS Conference Proceedings* 35 (May). https://doi.org/10.32473/flairs.v35i.130723.

Freeman, D., S. Reeve, A. Robinson, et al. 2017. "Virtual Reality in the Assessment, Understanding, and Treatment of Mental Health Disorders." *Psychological Medicine* 47 (14): 2393–400. https://doi.org/10.1017/S003329171700040X.

Freeman, Guo, Divine Maloney, Dane Acena, and Catherine Barwulor. 2022. "(Re)Discovering the Physical Body Online: Strategies and Challenges to Approach Non-Cisgender Identity in Social Virtual Reality." *CHI Conference on Human Factors in Computing Systems*, April 27, 1–15. https://doi.org/10.1145/3491102.3502082.

Freeman, Guo, Samaneh Zamanifard, Divine Maloney, and Alexandra Adkins. 2020. "My Body, My Avatar: How People Perceive Their Avatars in Social Virtual Reality." *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, April 25, 1–8. https://doi.org/10.1145/3334480.3382923.

French, Kristen. 2017. "First They Got Sick, Then They Moved Into a Virtual Utopia." Tags. *Wired*, February 13. https://www.wired.com/2017/02/first-they-got-sick-then-they-moved-into-a-virtual-utopia/.

Frenkel, Sheera, and Kellen Browning. 2021. "The Metaverse's Dark Side: Here Come Harassment and Assaults." Technology. *The New York Times*, December 30. https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html.

Fried, Ina. 2024. "Scoop: Meta Won't Offer Future Multimodal AI Models in EU." Axios, July 17. https://www.axios.com/2024/07/17/meta-future-multimodal-ai-models-eu.

Friederiszick, Paul. 2025. "EU and US Antitrust Is Converging on Anti-Monopoly." *ProMarket*, June 18. https://www.promarket.org/2025/06/18/eu-and-us-antitrust-is-converging-on-anti-monopoly/.

Friedman, David. 1996. "A World of Strong Privacy: Promises and Perils of Encryption." *Social Philosophy and Policy* 13 (2): 212–28. https://doi.org/10.1017/S0265052500003526.

Frier, Sarah. 2017. "How Sheryl Sandberg's Sharing Manifesto Drives Facebook." Bloomberg, April 27. https://web.archive.org/web/20170429000513/https://www.bloomberg.com/news/features/2017-04-27/how-sheryl-sandberg-s-sharing-manifesto-drives-facebook.

Fristed, Emil, Caroline Skirrow, Marton Meszaros, et al. 2022. "A Remote Speech-based AI System to Screen for Early Alzheimer's Disease via Smartphones." *Alzheimer's & Dementia : Diagnosis, Assessment & Disease Monitoring* 14 (1): e12366. https://doi.org/10.1002/dad2.12366.

Furman, Ivo. 2015. "Studying the Influence of Bulletin Board System Technologies on the Communication Culture of Pre-Internet Turkish-Speaking Online Communities: A Socio-Technical Approach." *New Perspectives on Turkey* 53 (November): 37–69. https://doi.org/10.1017/npt.2015.18.

Fury, Andy. 2023. "Diversity in Tech: How Diverse Is the Tech Industry in 2023?" Jefferson Frank, February 27. https://www.jeffersonfrank.com/insights/diversity-in-tech.

Future Stores 2024. 2024. "Nike Is Using Augmented Reality to Drive Experiential Retail in Its Stores." June 3. https://futurestores.wbresearch.com/blog/nike-using-augmented-reality-drive-experiential-retail-stores.

Gallagher, Shaun. 1986. "Body Image and Body Schema: A Conceptual Clarification." *The Journal of Mind and Behavior* 7 (4): 541–54.

Garcia, Michael. 2023. "The Forgotten 'Emerging' Technology." New America, September. https://www.newamerica.org/future-security/reports/the-forgotten-emerging-technology/.

Garrity, Kelly. 2022. "Activists Tackle the Metaverse." POLITICO, November 29. https://www.politico.com/newsletters/digital-future-daily/2022/11/29/activists-tackle-the-metaverse-00071166.

Gesetz Über Die Unternehmerischen Sorgfaltspflichten in Lieferketten, 46 2959 (2021). http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s2959.pdf.

Ghioni, Riccardo, Mariarosaria Taddeo, and Luciano Floridi. 2023. "Open Source Intelligence and AI: A Systematic Review of the GELSI Literature." *AI & Society*, January 28, 1–16. https://doi.org/10.1007/s00146-023-01628-x.

Ghiţă, Alexandra, and José Gutiérrez-Maldonado. 2018. "Applications of Virtual Reality in Individuals with Alcohol Misuse: A Systematic Review." *Addictive Behaviors* 81 (June): 1–11. https://doi.org/10.1016/j.addbeh.2018.01.036.

Gibson, James J. 1979. "The Theory of Affordances." In *The Ecological Approach to Visual Perception: Classic Edition*. Psychology Press. https://doi.org/10.4324/9781315740218.

Gibson, William. 1986. *Neuromancer*. Phantasia Press.

Gibson, William. 2000. *Burning Chrome: And Other Stories*. HarperCollins Publishers.

Gleeson, Cailey. 2024. "Pro-Palestinian Campus Protests Are Happening Around The Globe—Following Encampments At Columbia And UCLA." Forbes, May 7. https://www.forbes.com/sites/caileygleeson/2024/05/03/pro-palestine-campus-protests-are-happening-around-the-globe-following-encampments-at-columbia-and-ucla/.

Glendon, Mary Ann. 2003. "The Forgotten Crucible: The Latin American Influence on the Universal Human Rights Idea." *Harvard Human Rights Journal* 16: 27–39.

"Global Digital Compact." 2024. United Nations Office for Digital and Emerging Technologies, September 22. https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf.

Global Network Initiative. n.d. "Global Network Initiative." Accessed September 15, 2025. https://globalnetworkinitiative.org/.

Goffman, Erving. 1956. *The Presentation of Self in Everyday Life*. University of Edinburgh, Social Sciences Research Centre.

Golia, Angelo Jr. 2024. "Critique of Digital Constitutionalism: Deconstruction and Reconstruction from a Societal Perspective." *Global Constitutionalism* 13 (3): 488–518. https://doi.org/10.1017/S2045381723000126.

Gomez, Juan Felipe, Caio Vieira Machado, Lucas Monteiro Paes, and Flavio P. Calmon. 2024. "Algorithmic Arbitrariness in Content Moderation." arXiv:2402.16979. Preprint, arXiv, February 26. https://doi.org/10.48550/arXiv.2402.16979.

Gongane, Vaishali U., Mousami V. Munot, and Alwin D. Anuse. 2022. "Detection and Moderation of Detrimental Content on Social Media Platforms: Current Status and Future Directions." *Social Network Analysis and Mining* 12 (1): 129. https://doi.org/10.1007/s13278-022-00951-3.

Google. n.d. "Getting to Know Glass - Google Glass Help." Accessed October 6, 2025. https://support.google.com/glass/answer/3063441?hl=en.

Google Account Help. n.d. "Access Age-Restricted Content & Features." Accessed February 13, 2023. https://support.google.com/accounts/answer/10071085?visit_id=638118830802650744-3756593632&p=age-verify&rd=1.

Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12 (ECJ May 13, 2014). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

Google Workspace Blog. n.d. "Duet AI for Google Workspace Now Generally Available." Accessed April 19, 2024. https://workspace.google.com/blog/product-announcements/duet-ai-in-workspace-now-available.

Gorwa, Robert. 2019. "What Is Platform Governance?" *Information, Communication & Society* 22 (6): 854–71. https://doi.org/10.1080/1369118X.2019.1573914.

GOV.UK. n.d. "The Civil Service Code." Accessed April 28, 2024. https://www.gov.uk/government/publications/civil-service-code/the-civil-service-code.

Grady, Patrick. 2023. "[Document] IMCO's Draft Report on Virtual Worlds." July 14. https://www.metaversepolicy.eu/p/document-imcos-draft-report-on-virtual.

Grady, Patrick. 2024. "Metaverse Policy Brief 30.10." *Metaverse EU*, October 30. https://www.metaversepolicy.eu/p/metaverse-policy-brief-3010.

Grady, Patrick. 2025. "There's No Such Thing as 'Mixed Reality.'" September 2. https://www.metaversepolicy.eu/p/theres-no-such-thing-as-mixed-reality.

Granero, Roser, Fernando Fernández-Aranda, Gemma Mestre-Bach, et al. 2016. "Compulsive Buying Behavior: Clinical Comparison with Other Behavioral Addictions." *Frontiers in Psychology* 7 (June): 914. https://doi.org/10.3389/fpsyg.2016.00914.

Grauman, Kristen, Andrew Westbury, Eugene Byrne, et al. 2022. "Ego4D: Around the World in 3,000 Hours of Egocentric Video." arXiv:2110.07058. Preprint, arXiv, March 11. http://arxiv.org/abs/2110.07058.

Gray, Joanne E., Marcus Carter, and Ben Egliston. 2024a. "Conduct Harms in Social VR: Embodied Harassment, Gender-Based Harm and Toxic Cultures." In *Governing Social Virtual Reality: Preparing for the Content, Conduct and Design Challenges of Immersive Social Media*, edited by Joanne E. Gray, Marcus Carter, and Ben Egliston. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-61831-4_3.

Gray, Joanne E., Marcus Carter, and Ben Egliston. 2024b. *Governing Social Virtual Reality: Preparing for the Content, Conduct and Design Challenges of Immersive Social Media*. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-61831-4.

Gray, Joanne E., Marcus Carter, and Ben Egliston. 2024c. "Trust and Safety in Social VR: Current Industry Practices." In *Governing Social Virtual Reality: Preparing for the Content, Conduct and Design Challenges of Immersive Social Media*, edited by Joanne E. Gray, Marcus Carter, and Ben Egliston. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-61831-4_6.

Green, Nicola. 1997. "Beyond Being Digital: Representation and Virtual Corporeality." In *Virtual Politics: Identity & Community in Cyberspace*. https://books.google.com/books?hl=en&lr=&id=x_zOA24lvIIC&oi=fnd&pg=PA59&dq=in

fo:fYIjSoaxsu4J:scholar.google.com&ots=skHcK2BI6T&sig=cEANa3yNVMRDjFv0T2bJwR-qCac.

Griffiths, Mark. 2000. "Excessive Internet Use: Implications for Sexual Behavior." *CyberPsychology & Behavior* 3 (4): 537–52. https://doi.org/10.1089/109493100420151.

"Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them." 2022. European Data Protection Board, March 14. https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf.

Guinn, David E. 2005. "Philosophy and Theory of Freedom of Expression." SSRN Scholarly Paper No. 801344. Rochester, NY, September 17. https://papers.ssrn.com/abstract=801344.

Gunkel, David, and Ann Gunkel. 1997. "Virtual Geographies: The New Worlds of Cyberspace." *Critical Studies in Media Communication - CRIT STUD MEDIA COMM* 14 (June): 123–37. https://doi.org/10.1080/15295039709367003.

Guterres, António. 2020. "The Highest Aspiration: A Call to Action for Human Rights." https://www.un.org/sg/sites/www.un.org.sg/files/atoms/files/The_Highest_Asperation_A_Call_To_Action_For_Human_Right_English.pdf.

Haimson, Oliver L., Daniel Delmonaco, Peipei Nie, and Andrea Wegner. 2021. "Disproportionate Removals and Differing Content Moderation Experiences for Conservative, Transgender, and Black Social Media Users: Marginalization and Moderation Gray Areas." *Proc. ACM Hum.-Comput. Interact.* 5 (CSCW2): 466:1-466:35. https://doi.org/10.1145/3479610.

Halupka, Max. 2014. "Clicktivism: A Systematic Heuristic." *Policy & Internet* 6 (2): 115–32. https://doi.org/10.1002/1944-2866.POI355.

Hamilton, Michael. 2020. "The Meaning and Scope of 'Assembly' in International Human Rights Law." *International & Comparative Law Quarterly* 69 (3): 521–56. https://doi.org/10.1017/S0020589320000160.

Han, Eugy, and Jeremy N. Bailenson. 2024. "Social Interaction in VR." In *Oxford Research Encyclopedia of Communication*, by Eugy Han and Jeremy N. Bailenson. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228613.013.1489.

Harwell, Drew. 2018. "The Accent Gap: How Amazon's and Google's Smart Speakers Leave Certain Voices behind." Washington Post, July 19. https://www.washingtonpost.com/graphics/2018/business/alexa-does-not-understand-your-accent/.

Hayles, N. Katherine. 1996. "Embodied Virtuality: Or How To Put Bodies Back Into the Picture." In *Immersed in Technology: Art and Virtual Environments*, edited by Mary Anne Moser and Douglas MacLeod. Immersed in Technology: Art and Virtual Environments. MIT Press. https://ieeexplore.ieee.org/document/6300716.

Heaney, David. 2024a. "Apple Will Give Enterprise Access To Vision Pro's Cameras." UploadVR, June 10. https://www.uploadvr.com/apple-vision-pro-enterprise-raw-camera-access/.

Heaney, David. 2024b. "Quest Developers Will Get Access To The Passthrough Cameras." UploadVR, September 25. https://www.uploadvr.com/quest-passthrough-api-camera-access-next-year/.

Heidegger, Martin. 1996. *Being and Time: A Translation of Sein Und Zeit*. SUNY Press.

Heim, Michael. 1993. *The Metaphysics of Virtual Reality*. Oxford University Press.

Heller, Brittan. 2020. "Reimagining Reality: Human Rights and Immersive Technology." Carr Center Discussion Paper Series, June 12. https://carrcenter.hks.harvard.edu/publications/reimagining-reality-human-rights-and-immersive-technology.

Heller, Brittan, and Avi Bar-Zeev. 2021. "The Problems with Immersive Advertising: In AR/VR, Nobody Knows You Are an Ad." *Journal of Online Trust and Safety* 1 (1): 1. https://doi.org/10.54501/jots.v1i1.21.

Henshall, Will. 2024. "Big Tech Is Dominating the AI Lobbying Frenzy in Washington." TIME, April 30. https://time.com/6972134/ai-lobbying-tech-policy-surge/.

Herring, Susan. 1996. *Gender Differences in Computer Mediated Communication: Bringing Familiar Baggage to the New Frontier*. January 1.

Hertz, Nora. 2022. "Neurorights – Do We Need New Human Rights? A Reconsideration of the Right to Freedom of Thought." *Neuroethics* 16 (1): 5. https://doi.org/10.1007/s12152-022-09511-0.

Hickey, Daniel, Daniel M. T. Fessler, Kristina Lerman, and Keith Burghardt. 2025. "X under Musk's Leadership: Substantial Hate and No Reduction in Inauthentic Activity." *PLOS ONE* 20 (2): e0313293. https://doi.org/10.1371/journal.pone.0313293.

Higgin, Tanner. 2009. "Blackless Fantasy: The Disappearance of Race in Massively Multiplayer Online Role-Playing Games." *Games and Culture* 4 (1): 3–26. https://doi.org/10.1177/1555412008325477.

Hill, Kashmir. 2022. "This Is Life in the Metaverse." Technology. *The New York Times*, October 7. https://www.nytimes.com/2022/10/07/technology/metaverse-facebook-horizon-worlds.html.

Hill, Kashmir. 2024. "Two Students Created Face Recognition Glasses. It Wasn't Hard." Technology. *The New York Times*, October 24. https://www.nytimes.com/2024/10/24/technology/facial-recognition-glasses-privacy-harvard.html.

Hine, Emmie. 2023. "Content Moderation in the Metaverse Could Be a New Frontier to Attack Freedom of Expression." *Philosophy & Technology* 36 (3): 43. https://doi.org/10.1007/s13347-023-00645-4.

Hine, Emmie. 2024a. "Extended Reality Is a Fundamentally Mediated Reality." *A Metaverse for the Good*, April 18, 115–18. https://doi.org/10.5281/zenodo.10993751.

Hine, Emmie. 2024b. "Virtual Reality, Cyberspace, and Embodiment: A Historical Debate with Contemporary Resonance." SSRN Scholarly Paper No. 4714432. Rochester, NY, February 2. https://doi.org/10.2139/ssrn.4714432.

Hine, Emmie, Josh Cowls, and Luciano Floridi. 2024. "Assembly and Expression in Extended Reality: Transposing Fundamental Rights Across Realities." Paper presented at International Congress Towards a Responsible Development of the Metaverse. *Proceedings of the International Congress Towards a Responsible Development of the Metaverse*, June 13. https://catedrametaverso.ua.es/wp-content/uploads/2024/07/Assembly-and-Expression-in-Extended-Reality-Transposing-Fundamental-Rights-Across-HINE.pdf.

Hine, Emmie, Josh Cowls, and Luciano Floridi. 2025. “Assembly and Expression in Extended Reality: Transposing Human Rights across Realities.” Interactive Entertainment Law Review. *Interactive Entertainment Law Review* 8 (1): 66–80. https://doi.org/10.4337/ielr.2025.0003.

Hine, Emmie, and Luciano Floridi. 2025. “From No-Win to No-Lose:” *Journal of AI Law and Regulation* 2 (3): 196–211. https://doi.org/10.21552/aire/2025/3/4.

Hine, Emmie, Isadora Neroni Rezende, Huw Roberts, David Wong, Mariarosaria Taddeo, and Luciano Floridi. 2024. “Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations.” *Digital Society* 3 (2): 33. https://doi.org/10.1007/s44206-024-00114-1.

Hine, Emmie, David Wong, and Luciano Floridi. 2025. “The Impact of Modern Big Tech Antitrust on Digital Sovereignty.” SSRN Scholarly Paper No. 5248950. Social Science Research Network, May 9. https://doi.org/10.2139/ssrn.5248950.

Hohfeld, Wesley. 1917. “FUNDAMENTAL LEGAL CONCEPTIONS AS APPLIED IN JUDICIAL REASONING.” *Yale Law Journal* 26 (8): 710–70.

Holmes, Samantha. 2022. “Blog: How Lèse-Majesté Laws Are Eroding Free Speech in Southeast Asia.” ARTICLE 19, August 19. https://www.article19.org/resources/lese-majeste-laws-eroding-free-speech-southeast-asia/.

“Home | Ethical Trading Initiative.” n.d. Accessed September 16, 2025. https://www.ethicaltrade.org/.

“Home - Fair Labor Association.” n.d. Accessed September 16, 2025. https://www.fairlabor.org/.

Home Security Heroes. 2024. “2023 State Of Deepfakes: Realities, Threats, And Impact.” Home Security Heroes. https://www.homesecurityheroes.com/state-of-deepfakes/#key-findings.

“How the DAO Works.” 2024. December 18. https://docs.decentraland.org/player/general/dao/overview/how-does-the-dao-work/.

How Virtual Reality Can Create the Ultimate Empathy Machine. 2015. Performed by Chris Milk. TED Talks. https://www.ted.com/talks/chris_milk_how_virtual_reality_can_create_the_ultimate_empathy_machine.

Howell, Courtney. 2024. “Warehouse AR: How Augmented Reality Is Transforming Logistics.” LightGuide, June 11. https://www.lightguidesys.com/resource-center/blog/warehouse-ar-how-augmented-reality-is-transforming-logistics/.

Howkins, Ben, and Julie Vinders. 2022. “Digital Extended Reality through the Lens of Human Rights Law - TechEthos.” TechEthos, October 6. https://www.techethos.eu/digital-extended-reality-through-the-lens-of-human-rights-law/.

Huang, Kalley, and Catherine Perloff. 2025. “Meta Renews Work on Facial Recognition Tech as Privacy Worries Fade.” The Information, May 7. https://www.theinformation.com/articles/meta-renews-work-facial-recognition-tech-privacy-worries-fade.

Huang, Yan, Yi Li, and Zhipeng Cai. 2022. “Security and Privacy in Metaverse: A Comprehensive Survey.” *Big Data Mining and Analytics*, ahead of print, November 17. https://doi.org/10.26599/BDMA.2022.9020047.

Hughes, Tamara. 2021. "Ensuring 'Be Excellent to Each Other.'" *Rec Room Developer Blog*, November 19. https://blog.recroom.com/posts/2021/11/19/ensuring-be-excellent-to-each-other.

Human Rights Council. 2012. "The Promotion, Protection and Enjoyment of Human Rights on the Internet." July 5. https://primarysources.brillonline.com/browse/human-rights-documents-online/promotion-and-protection-of-all-human-rights-civil-political-economic-social-and-cultural-rights-including-the-right-to-development;hrdhrd99702016149.

Human Rights Council. 2024. "Overview of Week 3 (01 – 05 July 2024)." Geneva Centre for Human Rights Advancement and Global Dialogue, July. https://primarysources.brillonline.com/browse/human-rights-documents-online/item-4-human-rights-situations-that-require-the-councils-attention;hrdhrd4021201840210011.

Hupf, Robert. 2014. "Step into the Game: Assessing the Interactive Nature of Virtual Reality Video Games through the Context of Terroristic Speech." *Virginia Journal of Law & Technology* 19 (3): 602–68.

Hutchby, Ian. 2001. "Technologies, Texts and Affordances." *Sociology* 35 (2): 441–56. https://doi.org/10.1177/S0038038501000219.

Ihde, Don. 1990. *Technology and the Lifeworld: From Garden to Earth*. Indiana University Press.

Ihde, Don. 2015. *Technoscience and Postphenomenology: The Manhattan Papers*. Postphenomenology and the Philosophy of Technology. Lexington Books.

Inam, Henna. 2018. "Bring Your Whole Self To Work." Forbes, May 10. https://www.forbes.com/sites/hennainam/2018/05/10/bring-your-whole-self-to-work/.

Internet & Jurisdiction Policy Network. 2021. "Toolkit Cross-Border Content Moderation." March. https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-21-104-Toolkit-Cross-border-Content-Moderation-2021.pdf.

ISO. 2009. *Plastics Piping Systems for Water Supply and for Buried and Above-Ground Drainage and Sewerage under Pressure — Unplasticized Poly(Vinyl Chloride) (PVC-U)*. ISO 1452-1:2009. December. https://www.iso.org/standard/50361.html.

ISO/IEC. 2023. *Information Technology — Digital Compression and Coding of Continuous-Tone Still Images*. ISO 10918-7:2023. November. https://www.iso.org/standard/85635.html.

Italian Data Protection Authority. 2022. "Provvedimento del 7 luglio 2022 [9788429]." July 7. https://www.gpdp.it:443/web/guest/home/docweb/-/docweb-display/docweb/9788429.

ITU Focus Group on Metaverse FGMV-12. 2023. "ITU Focus Group Technical Report: Children's Age Verification in the Metaverse." International Telecommunication Union Standardization Sector, December.

Jacob, Nina, Rhiannon Evans, and Jonathan Scourfield. 2017. "The Influence of Online Images on Self-Harm: A Qualitative Study of Young People Aged 16–24." *Journal of Adolescence* 60 (October): 140–47. https://doi.org/10.1016/j.adolescence.2017.08.001.

Jacob, Robert J.K., Audrey Girouard, Leanne M. Hirshfield, et al. 2008. "Reality-Based Interaction: A Framework for Post-WIMP Interfaces." *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, April 6, 201–10. https://doi.org/10.1145/1357054.1357089.

Jahan, Nusrat, Sadiq Naveed, Muhammad Zeshan, and Muhammad A Tahir. 2016. "How to Conduct a Systematic Review: A Narrative Literature Review." *Cureus* 8 (11): e864. https://doi.org/10.7759/cureus.864.

Jahangir, Ramsha. 2025. "What We Don't Know About DSA Enforcement." Tech Policy Press, April 8. https://techpolicy.press/what-we-dont-know-about-dsa-enforcement.

Jasper, Angelica, Nicholas Cone, Chase Meusel, Michael Curtis, Michael C. Dorneich, and Stephen B. Gilbert. 2020. "Visually Induced Motion Sickness Susceptibility and Recovery Based on Four Mitigation Techniques." *Frontiers in Virtual Reality* 1. https://www.frontiersin.org/articles/10.3389/frvir.2020.582108.

Jensen Schau, Hope, and Mary C. Gilly. 2003. "We Are What We Post? Self-Presentation in Personal Web Space." *Journal of Consumer Research* 30 (3): 385–404. https://doi.org/10.1086/378616.

Johnson-Glenberg, Mina C. 2018. "Immersive VR and Education: Embodied Design Principles That Include Gesture and Hand Controls." *Frontiers in Robotics and AI* 5 (July). https://doi.org/10.3389/frobt.2018.00081.

Joint Research Centre. 2023. "Citizens' Panel on Virtual Worlds." Community of Practice of the Competence Centre on Participatory and Deliberative Democracy. https://cop-demos.jrc.ec.europa.eu/events/citizens-panel-virtual-worlds?utm_source=piano&utm_medium=email&utm_campaign=29541&pnespid=6bhqDSobLqlCxOmRqjnvSZnUphCwV55zPbGmyO5toAdmNnl0ntCzVQTVlh6t6v.npd2W8zZNCg.

Jørgensen, Rikke Frank, ed. 2019. *Human Rights in the Age of Platforms*. Information Policy, edited by Sandra Braman. MIT Press. https://mitpress.mit.edu/9780262039055/human-rights-in-the-age-of-platforms/.

Junghare, Indira. 2012. "'Avatar': Heavenly Descent." *International Journal of Diversity in Organizations, Communities, and Nations* (Patras, United States) 11 (4): 121–38. https://doi.org/10.18848/1447-9532/CGP/v11i04/39032.

Kafai, Yasmin B., Melissa S. Cook, and Deborah A. Fields. 2010. """Blacks Deserve Bodies Too!"": Design and Discussion About Diversity and Race in a Tween Virtual World." *Games and Culture* 5 (1): 43–63. https://doi.org/10.1177/1555412009351261.

Kalpokas, Ignas, and Julija Kalpokienė. 2023. *Regulating the Metaverse: A Critical Assessment*. Routledge. https://doi.org/10.4324/9781003355861.

Kang, Jerry. 2000. "Cyber-Race." *Harvard Law Review* 113 (5): 1130–208. https://doi.org/10.2307/1342340.

Kann, Amanda. 2022. "Voice Assistants Have a Plurilingualism Problem." *Proceedings of the 4th Conference on Conversational User Interfaces*, July 26, 1–5. https://doi.org/10.1145/3543829.3544526.

Kaplan, Joel. 2025. "More Speech and Fewer Mistakes." *Meta*, January 7. https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/.

Kapsoritakis, Stefanos. 2022. "A Comparative Study of Virtual Reality Hand-Tracking and Controllers." Turku University of Applied Sciences. https://www.theseus.fi/bitstream/handle/10024/754933/Kapsoritakis_Stefanos.pdf?isAllowed=y&sequence=2.

Karanicolas, Michael, Melodi Dincer, Maria Fernanda Muñoz, and Noah Keith, eds. 2024. "Governing XR." UCLA Information Policy Lab, October. https://itlp.law.ucla.edu/wp-content/uploads/2024/09/UCLA_ITLP_Governing_XR.pdf.

Kelly, Jonathan W., Stephen B. Gilbert, Michael C. Dorneich, and Kristi A. Costabile. 2023. "Gender Differences in Cybersickness: Clarifying Confusion and Identifying Paths Forward." *2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, March, 283–88. https://doi.org/10.1109/VRW58643.2023.00067.

Kemp, Simon. 2024. "Internet Use in 2024." DataReportal – Global Digital Insights, January 31. https://datareportal.com/reports/digital-2024-deep-dive-the-state-of-internet-adoption.

Kendall, Lori. 1998. "Meaning and Identity in 'Cyberspace': The Performance of Gender, Class, and Race Online." *Symbolic Interaction* 21 (2): 129–53. https://doi.org/10.1525/si.1998.21.2.129.

Kim, Angela, and Pablo Gonzaléz Mellafe. 2024. "Prevention and Management of Lawful but Awful Content Moderation in XR Platforms." Tech Policy Press, May 10. https://techpolicy.press/prevention-and-management-of-lawful-but-awful-content-moderation-in-xr-platforms.

Kim, Monica. 2015. "The Good and the Bad of Escaping to Virtual Reality." Health. *The Atlantic*, February 18. https://www.theatlantic.com/health/archive/2015/02/the-good-and-the-bad-of-escaping-to-virtual-reality/385134/.

Kleinman, Zoe. 2019. "'My Son Spent £3,160 in One Game.'" Technology. *BBC News*, July 15. https://www.bbc.com/news/technology-48925623.

Koops, Bert-Jaap. 2014. "The Trouble with European Data Protection Law." *International Data Privacy Law* 4 (4): 250–61. https://doi.org/10.1093/idpl/ipu023.

Kouijzer, Marileen M. T. E., Hanneke Kip, Yvonne H. A. Bouman, and Saskia M. Kelders. 2023. "Implementation of Virtual Reality in Healthcare: A Scoping Review on the Implementation Process of Virtual Reality in Various Healthcare Settings." *Implementation Science Communications* 4 (June): 67. https://doi.org/10.1186/s43058-023-00442-2.

Kröger, Jacob Leon, Otto Hans-Martin Lutz, and Florian Müller. 2020. "What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking." In *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers*, edited by Michael Friedewald, Melek Önen, Eva Lievens, Stephan Krenn, and Samuel Fricker. IFIP Advances in Information and Communication Technology. Springer International Publishing. https://doi.org/10.1007/978-3-030-42504-3_15.

Kulal, Shalaka, Zhigang Li, and Xin Tian. 2022. "Security and Privacy in Virtual Reality: A Literature Review." *Issues In Information Systems* 23 (2): 185–92. https://doi.org/10.48009/2_iis_2022_125.

La Quadrature Du Net and Others v Premier Ministre and Others, Joined Cases C-511/18, C-512/18, C-520/18 (ECJ October 6, 2020). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0511.

Landgrebe, Ludwig. 1973. "The Phenomenological Concept of Experience." *Philosophy and Phenomenological Research* 34 (1): 1–13. https://doi.org/10.2307/2106776.

Lang, Ben. 2024. "Quest 3 Has Higher Effective Resolution, But This Is Why Vision Pro Still Looks Best." Road to VR, May 9. https://www.roadtovr.com/meta-quest-3-apple-vision-pro-resolution-resolving-power-display-quality/.

Lanier, Jaron. 2017. *Dawn of the New Everything: Encounters with Reality and Virtual Reality*. Random House.

Lanier, Jaron, and Frank Biocca. 1992. "An Insider's View of the Future of Virtual Reality." *Journal of Communication* 42 (4): 150–72. https://doi.org/10.1111/j.1460-2466.1992.tb00816.x.

Lanier, Jaron, and Kevin Kelly. 2014. "Digital Natives: A Conversation between Virtual Reality Visionaries Jaron Lanier and Kevin Kelly." Interview by Casey Newton. August 25. https://www.theverge.com/a/virtual-reality/interview#story.

Latonero, Mark. 2018. *Governing Artificial Intelligence: Upholding Human Rights and Dignity*. Data & Society. https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf.

Lauri, Mary Anne, and Lorleen Farrugia. 2020. "Identity Exploration in Anonymous Online Spaces." In *The Routledge Companion to Digital Media and Children*, edited by Leila Green, Donell Holloway, Kylie Stevenson, Tama Leaver, and Leslie Haddon. Routledge. https://doi.org/10.4324/9781351004107-16.

Laux, Johann, Sandra Wachter, and Brent Mittelstadt. 2021. "Taming the Few: Platform Regulation, Independent Audits, and the Risks of Capture Created by the DMA and DSA." *Computer Law & Security Review* 43 (November): 105613. https://doi.org/10.1016/j.clsr.2021.105613.

Lawson, Eli Cohen. 2022. "Mark Zuckerberg Has Sacrificed Safety in His Pursuit of a Mass-Market Metaverse." Center for Countering Digital Hate, February 17. https://counterhate.com/blog/mark-zuckerberg-has-sacrificed-safety-in-his-pursuit-of-a-mass-market-metaverse/.

Le Goix, Renaud, and Chris J. Webster. 2008. "Gated Communities." *Geography Compass* 2 (4): 1189–214. https://doi.org/10.1111/j.1749-8198.2008.00118.x.

Lea, Martin, and Russell Spears. 1991. "Computer-Mediated Communication, de-Individuation and Group Decision-Making." *International Journal of Man-Machine Studies*, Special Issue: Computer-supported Cooperative Work and Groupware. Part 1, vol. 34 (2): 283–301. https://doi.org/10.1016/0020-7373(91)90045-9.

Leenes, Ronald. 2008. "Privacy in the Metaverse." In *The Future of Identity in the Information Society*, edited by Simone Fischer-Hübner, Penny Duquenoy, Albin Zuccato, and Leonardo Martucci. Springer US. https://doi.org/10.1007/978-0-387-79026-8_7.

"Legacy Verification Policy." n.d. Accessed February 13, 2023. https://help.twitter.com/en/managing-your-account/legacy-verification-policy.

Leland, Andrew. 2024. "I Know What the Apple Vision Pro Is For." Intelligencer, June 13. https://nymag.com/intelligencer/article/apple-vision-pro-disabled-users.html.

Lemley, Mark A., and Eugene Volokh. 2017. "Law, Virtual Reality, and Augmented Reality." *SSRN Electronic Journal*, ahead of print. https://doi.org/10.2139/ssrn.2933867.

Lessig, Lawrence. 1999. *Code: And Other Laws Of Cyberspace*. Basic Books.

Lessig, Lawrence. 2006. *Code: And Other Laws of Cyberspace, Version 2.0*. Basic Books.

LfD Lower Saxony. 2021. "LfD Lower Saxony Imposes a Fine of 10.4 Million Euros on Notebooksbilliger.De." January 8. https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-verhangt-bussgeld-uber-10-4-millionen-euro-gegen-notebooksbilliger-de-196019.html.

Liddicoat, Ian. 2022. "Eye Tracking Does Not Equal Attention." The Drum, December 12. https://www.thedrum.com/opinion/2022/12/12/eye-tracking-does-not-equal-attention.

Lillemose, Jacob, and Mathias Kryger. 2015. "The (Re)Invention of Cyberspace." Commentary. *Nordic Art Review*, August 24. https://kunstkritikk.com/the-reinvention-of-cyberspace.

Lin, Wen-Hsu, Chia-Hua Liu, and Chin-Chun Yi. 2020. "Exposure to Sexually Explicit Media in Early Adolescence Is Related to Risky Sexual Behavior in Emerging Adulthood." *PLoS ONE* 15 (4): e0230242. https://doi.org/10.1371/journal.pone.0230242.

Logan, Ian Taylor. 2018. "For Sale: Window to the Soul Eye Tracking as the Impetus for Federal Biometric Data Protection Comments." *Penn State Law Review* 123 (3): 779–812.

LOI N° 2017-399 Du 27 Mars 2017 Relative Au Devoir de Vigilance Des Sociétés Mères et Des Entreprises Donneuses d'ordre (1), 2017-399 (2017).

Loizides, Branden. 2016. "The Proposed Business and Human Rights Treaty: Four Challenges and an Opportunity." *Harvard International Law Journal*, July 7. https://journals.law.harvard.edu/ilj/2016/07/the-proposed-business-and-human-rights-treaty-four-challenges-and-an-opportunity/.

Lomas, Natasha. 2023. "Meta Tries to Keep Denying EU Users a Free Choice over Tracking -- but Change Is Coming." *TechCrunch*, March 30. https://techcrunch.com/2023/03/30/meta-facebook-gdpr-ads-tracking/.

Loucaides, Darren. 2024. "How Governments Are Using Facial Recognition to Crack down on Protesters." Rest of World, March 27. https://restofworld.org/2024/facial-recognition-government-protest-surveillance/.

Lovato, Silvia B., Anne Marie Piper, and Ellen A. Wartella. 2019. "Hey Google, Do Unicorns Exist?" *Proceedings of the 18th ACM International Conference on Interaction Design and Children*, June 12, 301–12. https://doi.org/10.1145/3311927.3323150.

Low, Jacqueline. 2019. "A Pragmatic Definition of the Concept of Theoretical Saturation." *Sociological Focus* 52 (2): 131–39. https://doi.org/10.1080/00380237.2018.1544514.

Lowood, Henry E. 2024. "Virtual Reality - Education, Training, Immersion." Britannica. https://www.britannica.com/technology/virtual-reality/Education-and-training.

Lü, Qian. 2023. "Tencent Disbands XR Team, ByteDance's Pico Lays Off Staff as Metaverse Fever Fades." Yicai Global, February 17. https://www.yicaiglobal.com/news/tencent-dissolves-xr-team-bytedance-pico-lays-off-staff-as-metaverse-hype-fades?mc_cid=6001f1b13c&mc_eid=c29ab63a8f.

Ma, Shugao, Tomas Simon, Jason Saragih, et al. 2021. "Pixel Codec Avatars." *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June, 64–73. https://doi.org/10.1109/CVPR46437.2021.00013.

Ma, Wayne, and Juro Osawa. 2025. "Amazon Is Developing AR Glasses in Challenge to Meta." The Information, September 10. https://www.theinformation.com/articles/amazon-developing-ar-glasses-challenge-meta.

Macaraniag, Louise. 2022. "The Voices Defining Web3: Is There a First Amendment Right to Assemble in the Metaverse?" *The Daily Dot*, May 4. https://www.dailydot.com/debug/digital-protest-metaverse/.

Maciejewski, Mariusz. 2023. "Metaverse." European Parliament Policy Department for Citizens' Rights and Constitutional Affairs, June 1. https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU(2023)751222_EN.pdf.

MacKinnon, Catharine A. 2004. "Prosecutor v. Nahimana, Barayagwiza, & Ngeze. Case No. ICTR 99-52-T." *The American Journal of International Law* 98 (2): 325–30. https://doi.org/10.2307/3176734.

Madary, Michael, and Thomas K. Metzinger. 2016. "Real Virtuality: A Code of Ethical Conduct. Recommendations for Good Scientific Practice and the Consumers of VR-Technology." *Frontiers in Robotics and AI* 3. https://www.frontiersin.org/articles/10.3389/frobt.2016.00003.

Madiega, Tambiama, Polona Car, Maria Niestadt, and Louise Van de Pol. 2022. *Metaverse: Opportunities, Risks and Policy Implications*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf.

Maister, Lara, Mel Slater, Maria V. Sanchez-Vives, and Manos Tsakiris. 2015. "Changing Bodies Changes Minds: Owning Another Body Affects Social Cognition." *Trends in Cognitive Sciences* 19 (1): 6–12. https://doi.org/10.1016/j.tics.2014.11.001.

Malik, Aisha. 2023. "Instagram Starts Testing Its Age Verification Tools in More Countries." *TechCrunch*, March 2. https://techcrunch.com/2023/03/02/instagram-starts-testing-its-age-verification-tools-in-more-countries/.

Malik, Yuvraj, and Katie Paul. 2024. "Meta Opens Quest Operating System to Third-Party Device Makers." Technology. *Reuters*, April 22. https://www.reuters.com/technology/meta-opens-quest-operating-system-third-party-device-makers-2024-04-22/.

Mallika, Mitra. 2024. "What Are the Magnificent Seven Stocks?" Buy Side from WSJ, April 20. https://www.wsj.com/buyside/personal-finance/magnificent-7-stocks-0d68cab6.

Marchese, Chris. 2023. "NetChoice & CCIA v. Moody (Florida, 2021)." *NetChoice*, March 21. https://netchoice.org/netchoice-ccia-v-moody/.

Marinotti, João. 2022. "Can You Truly Own Anything in the Metaverse? A Law Professor Explains How Blockchains and NFTs Don't Protect Virtual Property." The Conversation, April 21. http://theconversation.com/can-you-truly-own-anything-in-the-metaverse-a-law-professor-explains-how-blockchains-and-nfts-dont-protect-virtual-property-179067.

Marsh v. Alabama, 326 US 501 (Supreme Court 114 AD).

Martens, Marieke AG, Angus Antley, Daniel Freeman, Mel Slater, Paul J Harrison, and Elizabeth M Tunbridge. 2019. "It Feels Real: Physiological Responses to a Stressful Virtual Reality

Environment and Its Impact on Working Memory." *Journal of Psychopharmacology (Oxford, England)* 33 (10): 1264–73. https://doi.org/10.1177/0269881119860156.

Martin, Baily. 2022. "Privacy in a Programmed Platform: How the General Data Protection Regulation Applies to the Metaverse." *Harvard Journal of Law & Technology* 36 (1).

Mazuryk, Tomasz, and Michael Gervautz. 1999. *Virtual Reality - History, Applications, Technology and Future*. December 30.

McCay, Allan. 2022. "Neurorights: The Chilean Constitutional Change." *AI & SOCIETY*, ahead of print, March 2. https://doi.org/10.1007/s00146-022-01396-0.

McCorquodale, Robert. 2024. *Business and Human Rights*. Oxford University Press. https://doi.org/10.1093/law/9780192855855.001.0001.

McStay, Andrew. 2023. "The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons." *Philosophy & Technology* 36 (1): 13. https://doi.org/10.1007/s13347-023-00613-y.

Merritt, Andrew L. 1989. "Damages for Emotional Distress in Fraud Litigation: Dignitary Torts in a Commercial Society." *Vanderbilt Law Review* 42 (1): 1–38.

Meta. 2021a. "Opening Horizon Worlds to Everyone 18+ in the US and Canada." *Meta Newsroom*, December 9. https://about.fb.com/news/2021/12/horizon-worlds-open-in-us-and-canada/.

Meta, dir. 2021b. *The Metaverse and How We'll Build It Together -- Connect 2021*. 1:17:26. https://www.youtube.com/watch?v=Uvufun6xer8.

Meta. 2025. "Learn about Accessibility Features for Meta Quest." Meta Quest Help, July 21. https://www.meta.com/help/quest/674999931400954/.

Meta. n.d. "Meta Quest 3S: Next-Gen Mixed Reality Headset." Accessed October 6, 2025. https://www.meta.com/quest/quest-3s/.

Meta Accessibility. 2022. "Meta Accessibility." Facebook, January 31. https://www.facebook.com/accessibility/photos/a.544973158879747/4925712904139062/.

Meta Developers, dir. 2025. *Meta Connect 2025: Opening Keynote*. 01:30:21. https://www.youtube.com/watch?v=D97ILdUbYww.

Meta Emerging Tech. n.d. "Orion AI Glasses: The Future of AR Glasses Technology." Accessed September 1, 2025. https://www.meta.com/emerging-tech/orion/.

Meta Newsroom. 2023. "How Meta Uses Legal Bases for Processing Ads in the EU." *Meta Newsroom*, January 4. https://about.fb.com/news/2023/01/how-meta-uses-legal-bases-for-processing-ads-in-the-eu/.

Meta Quest, dir. 2024. *Productivity on Meta Quest 3 | Nailed It*. https://www.youtube.com/watch?v=34-DDtOmuJE.

Meta Quest. n.d. "Live Concert: Imagine Dragons." Accessed April 16, 2024. https://www.oculus.com/experiences/event/1606699232705927/.

Meta Quest Blog. 2021. "New Day, New You: Avatars Are More Expressive and Customizable Starting Today." *Meta Quest Blog*, April 23. https://www.oculus.com/blog/new-day-new-you-avatars-are-more-expressive-and-customizable-starting-today/.

Meta Transparency Center. 2023. "Account Integrity and Authentic Identity." https://transparency.fb.com/policies/community-standards/account-integrity-and-authentic-identity/.

Meta Transparency Center. n.d. "Hate Speech." Accessed April 19, 2024. https://transparency.meta.com/policies/community-standards/hate-speech/.

"Metaverse Seoul." n.d. Accessed April 27, 2024. https://metaverseseoul.kr/user/.

Metaverse Standards Forum. 2024. "Principal & Participant Members." Metaverse Standards Forum, December 26. https://metaverse-standards.org/members/list/.

Metz, Rachel. 2017. "Finally, a Useful Application for VR: Training Employees." MIT Technology Review, November 22. https://www.technologyreview.com/2017/11/22/147508/finally-a-useful-application-for-vr-training-employees/.

Mhaidli, Abraham Hani, and Florian Schaub. 2021. "Identifying Manipulative Advertising Techniques in XR Through Scenario Construction." *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA), CHI '21, May 7, 1–18. https://doi.org/10.1145/3411764.3445253.

Mickle, Tripp, and Erin Griffith. 2024. "'This Is Going to Be Painful': How a Bold A.I. Device Flopped." Technology. *The New York Times*, June 6. https://www.nytimes.com/2024/06/06/technology/humane-ai-pin.html.

Microsoft. 2021. "Comfort - Mixed Reality." Microsoft Learn, October 18. https://learn.microsoft.com/en-us/windows/mixed-reality/design/comfort.

Miehlbradt, Jenifer, Luigi F. Cuturi, Silvia Zanchi, Monica Gori, and Silvestro Micera. 2021. "Immersive Virtual Reality Interferes with Default Head–Trunk Coordination Strategies in Young Children." *Scientific Reports* 11 (1): 1. https://doi.org/10.1038/s41598-021-96866-8.

Milgram, Paul, and Fumio Kishino. 1994. "A Taxonomy of Mixed Reality Visual Displays." *IEICE TRANSACTIONS on Information and Systems* E77-D (12): 1321–29.

Miller, Mark Roman, Hanseul Jun, Fernanda Herrera, Jacob Yu Villa, Greg Welch, and Jeremy N. Bailenson. 2019. "Social Interaction in Augmented Reality." *PLOS ONE* 14 (5): e0216290. https://doi.org/10.1371/journal.pone.0216290.

Miller, Rosemarie. 2023. "Microsoft's Industrial Metaverse Aspirations Can Wait." Forbes, February 14. https://www.forbes.com/sites/rosemariemiller/2023/02/14/microsofts-industrial-metaverse-aspirations-can-wait/.

Mitsilegas, Valsamis, Elspeth Guild, Elif Kuskonmaz, and Niovi Vavoula. 2023. "Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks." *European Law Journal* 29 (1–2): 176–211. https://doi.org/10.1111/eulj.12417.

Moody v. NetChoice, LLC, Nos. 22–277 (US Supreme Court July 1, 2024).

Moran, Rachel Elizabeth, Joseph Schafer, Mert Bayar, and Kate Starbird. 2025. "The End of Trust and Safety?: Examining the Future of Content Moderation and Upheavals in Professional Online Safety Efforts." *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA), CHI '25, April 25, 1–14. https://doi.org/10.1145/3706598.3713662.

Morozov, Evgeny. 2024. "The Brave New World of Slacktivism." *Foreign Policy*, April 22. https://foreignpolicy.com/2009/05/19/the-brave-new-world-of-slacktivism/.

Morrow, Allison. 2024. "Meta Is Accused of Censoring a Non-Profit Newspaper and an Independent Journalist Who Criticized the Company." CNN, April 5. https://www.cnn.com/2024/04/05/tech/meta-nonprofit-newspaper-independent-journalist-alleged-censorship/index.html.

Mortice, Zach. 2022. "Augmented Reality Art Makes the Entire World a Canvas." Autodesk, January 21. https://www.autodesk.com/design-make/articles/augmented-reality-art.

Moser, Mary Anne, and Douglas MacLeod. 1996. "Virtual Skin: Articulating Race in Cyberspace." In *Immersed in Technology: Art and Virtual Environments*. Immersed in Technology: Art and Virtual Environments. MIT Press. https://ieeexplore.ieee.org/document/6300705.

Murray, Craig. 1999. "Towards a Phenomenology of the Body in Virtual Reality." *Research in Philosophy and Technology* 19: 149–73.

Musiani, Francesca, Laura DeNardis, Derrick Cogburn, Nanette S. Levinson, and Francesca Musiani. 2020. "Science and Technology Studies Approaches to Internet Governance: Controversies and Infrastructures as Internet Politics." In *Researching Internet Governance: Methods, Frameworks, Futures*. MIT Press. https://direct.mit.edu/books/oa-edited-volume/4936/chapter/625908/Science-and-Technology-Studies-Approaches-to.

Mütterlein, Joschka. 2018. "The Three Pillars of Virtual Reality? Investigating the Roles of Immersion, Presence, and Interactivity." Paper presented at Hawaii International Conference on System Sciences. *Proceedings of the 51st Hawaii International Conference on System Sciences*. https://doi.org/10.24251/HICSS.2018.174.

Nagel, Thomas. 1974. "What Is It Like to Be a Bat?" *The Philosophical Review* 83 (4): 435. https://doi.org/10.2307/2183914.

Nair, Vivek, Wenbo Guo, Justus Mattern, et al. 2023. "Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data." arXiv:2302.08927. Version 1. Preprint, arXiv, February 17. http://arxiv.org/abs/2302.08927.

Nakamura, Lisa. 2002. *Cybertypes: Race, Ethnicity, and Identity on the Internet*. 1st ed. Routledge.

Nakamura, Lisa. 2020. "Feeling Good about Feeling Bad: Virtuous Virtual Reality and the Automation of Racial Empathy." *Journal of Visual Culture* 19 (1): 47–64. https://doi.org/10.1177/1470412920906259.

National Socialist Party of America v. Skokie, 432 US 43 (Supreme Court 1977).

Needleman, Sarah E., and Salvador Rodriguez. 2022. "VR to the ER: Metaverse Early Adopters Prove Accident-Prone." Page One. *Wall Street Journal*, February 1. https://www.wsj.com/articles/metaverse-virtual-reality-vr-accident-prone-meta-11643730489.

Neely, Stuart, and Lise Smit. 2025. "Supply Chain Liability: Court of Appeal Allows Claims against UK Companies for Alleged Forced Labour by Malaysian Supplier to Be Heard in English Courts." Norton Rose Fulbright, April 4. https://www.nortonrosefulbright.com/en/inside-disputes/blog/discussing-the-recent-decision-in-limbu-ors-v-dyson-technology.

NetChoice vs Paxton, No. 21-51178 (US Court of Appeals for the 5th Circuit November 7, 2024).

Newton, Casey. 2021. "Mark Zuckerberg Is Betting Facebook's Future on the Metaverse." The Verge, July 22. https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview.

Nguyen, Terry. 2023. "A Released Soul in Online Form: The Evolution of the Profile Picture." Arkive Magazine, April 27. https://web-d61aocw8l-arkive.vercel.app/.

Nieuwsma, Anastasia. 2025. "Anduril and Meta Join Forces on XR Defense Project." *OPUSfidelis*, June 18. https://opusfidelis.com/insights/anduril-and-meta-join-forces-on-new-xr-defense-project/.

Nix, Naomi. 2024. "Attacks in the Metaverse Are Booming. Police Are Starting to Pay Attention." *Washington Post*, February 8. https://www.washingtonpost.com/technology/2024/02/04/metaverse-sexual-assault-prosecution/.

Nowak, Kristine L., and Christian Rauh. 2005. "The Influence of the Avatar on Online Perceptions of Anthropomorphism, Androgyny, Credibility, Homophily, and Attraction." *Journal of Computer-Mediated Communication* 11 (1): 153–78. https://doi.org/10.1111/j.1083-6101.2006.tb00308.x.

Nwanji, Ngozi. 2024. "Virtual-Reality Concerts Could Redefine the Live-Music Experience — but It'll Take More Time." Business Insider, March 13. https://www.businessinsider.com/extended-reality-meta-quest-vr-music-artist-concerts-2024-3.

Obregon, Liliana. 2009. "The Universal Declaration of Human Rights and Latin America." *Maryland Journal of International Law* 24 (1): 94–98.

O'Brolcháin, Fiachra, Tim Jacquemard, David Monaghan, Noel O'Connor, Peter Novitzky, and Bert Gordijn. 2016. "The Convergence of Virtual Reality and Social Networks: Threats to Privacy and Autonomy." *Science and Engineering Ethics* 22 (1): 1–29. https://doi.org/10.1007/s11948-014-9621-1.

Oculu Video Platform. 2014. "Is Virtual Reality the Next Frontier for Video Serving and Pre Roll Advertising?" November 11. https://oculu.com/is-virtual-reality-the-next-frontier-for-video-serving-and-pre-roll-advertising/.

OECD. 2013. "Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data." OECD, November 7. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

OED Online. n.d. "embody | imbody, v." Oxford University Press. Accessed April 19, 2023. https://www.oed.com/view/Entry/60907.

Office of the United Nations High Commissioner for Human Rights. 2024. "A/HRC/56/45 Mapping Report: Human Rights and New and Emerging Digital Technologies." United Nations, August 20. https://www.ohchr.org/en/documents/thematic-reports/ahrc5645-mapping-report-human-rights-and-new-and-emerging-digital.

Office of the United Nations High Commissioner for Human Rights. 2025. "Practical Application of the Guiding Principles on Business and Human Rights to the Activities of Technology Companies, Including Activities Relating to Artificial Intelligence." United Nations, June 16. https://primarysources.brillonline.com/browse/human-rights-documents-online/promotion-and-protection-of-all-human-rights-civil-political-economic-social-and-cultural-rights-including-the-right-to-development;hrdhrd99702016149.

O'Hagan, Joseph, Jan Gugenheimer, Jolie Bonner, Florian Mathis, and Mark McGill. 2023. "Augmenting People, Places & Media: The Societal Harms Posed by Everyday Augmented Reality, and the Case for Perceptual Human Rights." *Proceedings of the 22nd International Conference on Mobile and Ubiquitous Multimedia* (New York, NY, USA), MUM '23, December 3, 225–35. https://doi.org/10.1145/3626705.3627782.

OHCHR. 2022. "Human Rights Should Be at the Heart of Tech Governance." September 1. https://www.ohchr.org/en/stories/2022/09/human-rights-should-be-heart-tech-governance.

OHCHR. n.d.-a. "BHR Treaty Process." Accessed September 15, 2025. https://www.ohchr.org/en/business-and-human-rights/bhr-treaty-process.

OHCHR. n.d.-b. "International Bill of Human Rights." Accessed April 19, 2024. https://www.ohchr.org/en/what-are-human-rights/international-bill-human-rights.

Oliva, Thiago Dias, Dennys Marcelo Antonialli, and Alessandra Gomes. 2021. "Fighting Hate Speech, Silencing Drag Queens? Artificial Intelligence in Content Moderation and Risks to LGBTQ Voices Online." *Sexuality and Culture* 25 (2): 700–733.

O'Shea, Paul Maynard, Dan Cooper, Siobhán. 2022. "Special Category Data by Inference: CJEU Significantly Expands the Scope of Article 9 GDPR." Inside Privacy, August 10. https://www.insideprivacy.com/eu-data-protection/special-category-data-by-inference-cjeu-significantly-expands-the-scope-of-article-9-gdpr/.

OT v Vyriausioji Tarnybinės Etikos Komisija, Case C-184/20 (ECJ August 1, 2022). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62020CJ0184.

Outlaw, Jessica. 2018. *Virtual Harassment: The Social Experience of 600+ Regular Virtual Reality Users*. The Extended Mind. https://drive.google.com/file/d/1afFQJN6QAwmeZdGcRj9R4ohVr0oZNO4a/view?usp=sharing&usp=embed_facebook.

Packingham v. North Carolina, 137 S. Ct. 1730 (Supreme Court 2017).

Pahi, Suchismita, and Calli Schroeder. 2022. "Extended Privacy for Extended Reality: XR Technology Has 99 Problems and Privacy Is Several of Them." SSRN Scholarly Paper No. 4202913. Rochester, NY, August 28. https://doi.org/10.2139/ssrn.4202913.

Palmisano, Stephen, Robert S. Allison, and Juno Kim. 2020. "Cybersickness in Head-Mounted Displays Is Caused by Differences in the User's Virtual and Physical Head Pose." *Frontiers in Virtual Reality* 1. https://www.frontiersin.org/articles/10.3389/frvir.2020.587698.

Parshall, Allison. 2022. "Why an Assault on Your VR Body Can Feel so Real." *Scienceline*, June 29. https://scienceline.org/2022/06/virtual-reality-assault-psychology/.

Parsons, Thomas D., Christopher Courtney, Louise Cosand, Arvind Iyer, Albert A. Rizzo, and Kelvin Oie. 2009. "Assessment of Psychophysiological Differences of West Point Cadets and Civilian

Controls Immersed within a Virtual Environment." In *Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience*, edited by Dylan D. Schmorrow, Ivy V. Estabrooke, and Marc Grootjen. Lecture Notes in Computer Science. Springer. https://doi.org/10.1007/978-3-642-02812-0_60.

Patchin, Justin W. 2019. "Cyberbullying Data 2019." *Cyberbullying Research Center*, July 9. https://cyberbullying.org/2019-cyberbullying-data.

Patel, Nilay. 2023. "I Wore the Apple Vision Pro. It's the Best Headset Demo Ever." The Verge, June 6. https://www.theverge.com/2023/6/5/23750003/apple-vision-pro-hands-on-the-best-headset-demo-ever.

Patel, Nilay. 2024. "Apple Vision Pro Review: Magic, until It's Not." The Verge, January 30. https://www.theverge.com/24054862/apple-vision-pro-review-vr-ar-headset-features-price.

Patja, Jen, Evelyn Douek, and Charlotte Willner. 2023. "The Lawfare Podcast: The Professionalization of Content Moderation." *Lawfare*, January 18. https://www.lawfaremedia.org/article/lawfare-podcast-professionalization-content-moderation.

Paton, Callum. 2017. "Virtual Reality Gamer Slips And Dies From Blood Loss." Newsweek, December 23. https://www.newsweek.com/virtual-reality-gamer-slips-and-dies-blood-loss-after-falling-glass-table-757966.

Peck, Tabitha C., Sofia Seinfeld, Salvatore M. Aglioti, and Mel Slater. 2013. "Putting Yourself in the Skin of a Black Avatar Reduces Implicit Racial Bias." *Consciousness and Cognition* 22 (3): 779–87. https://doi.org/10.1016/j.concog.2013.04.016.

Penney, Jonathon W. 2016. "Chilling Effects: Online Surveillance and Wikipedia Use." *Berkeley Technology Law Journal* 31 (1): 117–82.

Penny, Simon. 1993. "Virtual Bodybuilding." *Media Information Australia* 69 (1): 17–22. https://doi.org/10.1177/1329878X9306900105.

Perez, Sarah. 2022. "Meta to Allow Horizon Worlds Users to Turn Their Avatar's Personal Safety Boundary off." TechCrunch, March 14. https://techcrunch.com/2022/03/14/meta-to-allow-horizon-worlds-users-to-turn-their-avatars-personal-safety-boundary-off-despite-virtual-world-sexual-assaults/.

Perry, John, Elizabeth Macken, Neil Scott, and Jan Mckinley. 1996. *Disability, Inability and Cyberspace*. January 1.

Peršak, Nina. 2022. "Criminalising Hate Crime and Hate Speech at EU Level: Extending the List of Eurocrimes Under Article 83(1) TFEU." *Criminal Law Forum* 33 (2): 85–119. https://doi.org/10.1007/s10609-022-09440-w.

Peters, Jay. 2023. "Comedians Are Trying to Make the Metaverse Cool, but It Won't Let Them." The Verge, March 21. https://www.theverge.com/2023/3/21/23645512/meta-horizon-worlds-metaverse-comedians.

Petter, Olivia. 2018. "Apple Has Been Criticised by Women for Making Phones That Are 'Too Big' to Fit in Their Hands." The Independent, September 15. https://www.independent.co.uk/life-style/women/apple-iphone-xs-max-new-too-big-size-women-sexist-feminist-a8537171.html.

Phandroid, dir. 2013. *Google Glass: Navigation*. 0:06. https://www.youtube.com/watch?v=IZdkIVS53Uw.

Pico. n.d. "Live the Game with PICO 4 All-in-One VR Headset." PICO Global. Accessed October 6, 2025. https://www.picoxr.com/global/products/pico4.

Picons. n.d. "Picons Archive." Accessed November 8, 2023. http://kinzler.com/picons/ftp/.

Plait, Phil. 2010. "Resolving the iPhone Resolution." Bad Astronomy. *Slate*, June 10. https://slate.com/technology/2010/06/resolving-the-iphone-resolution.html.

Plantin, Jean-Christophe, Carl Lagoze, Paul N Edwards, and Christian Sandvig. 2018. "Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook." *New Media & Society* 20 (1): 293–310. https://doi.org/10.1177/1461444816661553.

Poeschl, Sandra, and Nicola Doering. 2015. "Measuring Co-Presence and Social Presence in Virtual Environments - Psychometric Construction of a German Scale for a Fear of Public Speaking Scenario." *Studies in Health Technology and Informatics* 219: 58–63.

Polonioli, Andrea, Riccardo Ghioni, Ciro Greco, Prathm Juneja, Jacopo Tagliabue, and Luciano Floridi. 2022. "The Ethics of Online Controlled Experiments (A/B Testing)." SSRN Scholarly Paper No. 4282827. Rochester, NY, November 1. https://doi.org/10.2139/ssrn.4282827.

Potkonjak, Veljko, Michael Gardner, Victor Callaghan, et al. 2016. "Virtual Laboratories for Education in Science, Technology, and Engineering: A Review." *Computers & Education* 95 (April): 309–27. https://doi.org/10.1016/j.compedu.2016.02.002.

Potvin v. Metropolitan Life Ins. Co., 997 P. 2d 1153 (Supreme Court 2000).

Pozharliev, Rumen, Matteo De Angelis, and Dario Rossi. 2022. "The Effect of Augmented Reality versus Traditional Advertising: A Comparison between Neurophysiological and Self-Reported Measures." *Marketing Letters* 33 (1): 113–28. https://doi.org/10.1007/s11002-021-09573-9.

Pratt, Mary K. 2024. "Today's Virtual Reality Use Cases and Industry Applications." TechTarget, March 5. https://www.techtarget.com/searchcio/tip/Todays-virtual-reality-use-cases-and-industry-applications.

Pritchard, Tom. 2025. "Apple Glasses Just Tipped for 2027 Launch — Here's Everything We Know." Tom's Guide, June 30. https://www.tomsguide.com/computing/smart-glasses/apple-smart-glasses-just-tipped-for-2027-launch-and-theres-6-other-head-mounted-wearable-devices-on-the-way.

"Procedural Fairness." 2022. Text. June 1. https://www.jcu.edu.au/students/feedback-and-complaints/procedural-fairness.

Proposal for a Directive of the European Parliament and of the Council on Adapting Non-Contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive), Pub. L. No. 2022/0303 (COD) (2022). https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf.

Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (2017). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

PruneYard Shopping Center v. Robins, 447 US 74 (Supreme Court 1980).

"PwC Digital Ethics for Responsible Metaverse." 2022.

Ramzan, Muddasir. 2023. "'Making up Stories Is an Inherently Political Act': Mohsin Hamid in Conversation." *Journal of Postcolonial Writing* 59 (1): 113–24. https://doi.org/10.1080/17449855.2022.2093439.

Ranking Digital Rights. 2025. "The 2025 Ranking Digital Rights Big Tech Edition." https://rankingdigitalrights.org/bte25/.

Ravenscraft, Eric. 2023. "What Is the Metaverse, Exactly?" Tags. *Wired*, June 15. https://www.wired.com/story/what-is-the-metaverse/.

Raz Mobility. 2024. "6 Top Cell Phones for People Who Are Blind or Visually Impaired." RAZ Mobility, July 12. https://www.razmobility.com/assistive-technology-blog/6-top-cell-phones-for-people-who-are-blind-or-visually-impaired-in-2023/.

Reed, Nelson, and Katie Joseff. 2022. *Kids and the Metaverse: What Parents, Policymakers, and Companies Need to Know*. Common Sense Media. https://www.commonsensemedia.org/sites/default/files/featured-content/files/metaverse-white-paper.pdf.

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), 119 OJ L 1 (2016). http://data.europa.eu/eli/reg/2016/679/2016-05-04/eng.

Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online, 172 OJ L (2021). https://eur-lex.europa.eu/eli/reg/2021/784/oj.

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), 265 OJ L (2022). http://data.europa.eu/eli/reg/2022/1925/oj/eng.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 277 OJ L (2022). http://data.europa.eu/eli/reg/2022/2065/oj/eng.

Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on General Product Safety, Amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and Repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (Text with EEA Relevance), 135 OJ L (2023). http://data.europa.eu/eli/reg/2023/988/oj/eng.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (2024). http://data.europa.eu/eli/reg/2024/1689/oj/eng.

Renieris, Elizabeth M. 2023. *Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse*. MIT Press. https://mitpress.mit.edu/9780262047821/beyond-data/.

Reno v. ACLU, 521 U.S. 844, No. 96-511 (US Supreme Court June 26, 1997). https://supreme.justia.com/cases/federal/us/521/844/.

Rheingold, Howard. 1994. "PARC Is Back!" Tags. *Wired*, February 1. https://www.wired.com/1994/02/parc/.

Richter, Felix. 2024. "Infographic: The Most Spoken Languages: On the Internet and in Real Life." Statista Daily Data, February 21. https://www.statista.com/chart/26884/languages-on-the-internet.

Ridder, Denise de, Floor Kroese, and Laurens van Gestel. 2022. "Nudgeability: Mapping Conditions of Susceptibility to Nudge Influence." *Perspectives on Psychological Science* 17 (2): 346–59. https://doi.org/10.1177/1745691621995183.

Roberts, Huw. 2022. *Inferential Biometrics: Towards a Governance Framework*. Tony Blair Institute for Global Change. https://www.institute.global/insights/politics-and-governance/inferential-biometrics-towards-governance-framework.

Roberts, Huw, Emmie Hine, and Luciano Floridi. 2023. "Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance." In *Quo Vadis, Sovereignty?*, edited by Marina Timoteo, Barbara Verri, and Riccardo Nanni, vol. 154. Philosophical Studies Series. Springer. https://papers.ssrn.com/abstract=4483271.

Roberts, Lynne D., and Malcolm R. Parks. 1999. "The Social Geography of Gender-Switching in Virtual Environments on the Internet." *Information, Communication & Society* 2 (4): 521–40. https://doi.org/10.1080/136911899359538.

Robertson, Adi. 2022. "Meta Is Adding a 'Personal Boundary' to VR Avatars to Stop Harassment." The Verge, February 4. https://www.theverge.com/2022/2/4/22917722/meta-horizon-worlds-venues-metaverse-harassment-groping-personal-boundary-feature.

Rodriguez, Salvador. 2024. "Meta Finally Finds Success in AR, VR Three Years after Changing Name." CNBC, October 10. https://www.cnbc.com/2024/10/10/meta-finally-finds-success-in-ar-vr-three-years-after-changing-name.html.

Roessler, Beate. 2005. *The Value of Privacy*. Polity.

Roessler, Beate. 2018. "Three Dimensions of Privacy." In *Handbook of Privacy Studies: An Interdisciplinary Introduction*. Amsterdam University Press. https://www-cambridge-org.ezproxy.unibo.it/core/books/abs/handbook-of-privacy-studies/three-dimensions-of-privacy/F759F4050608495A318D894AEBBCD672.

Rosenberg, Louis. 2022a. "Deception vs Authenticity: Why the Metaverse Will Change Marketing Forever." *VentureBeat*, August 21. https://venturebeat.com/ai/deception-vs-authenticity-why-the-metaverse-will-change-marketing-forever/.

Rosenberg, Louis. 2022b. "Migration to the Metaverse: We Need Guaranteed Basic Immersive Rights." *VentureBeat*, September 11. https://venturebeat.com/virtual/metaverse-we-need-guaranteed-basic-immersive-rights/.

Rosenberg, Louis. 2022c. "Mind Control: The Metaverse May Be the Ultimate Tool of Persuasion." *VentureBeat*, October 22. https://venturebeat.com/virtual/mind-control-the-metaverse-may-be-the-ultimate-tool-of-persuasion/.

Rosenberg, Louis. 2022d. "The Metaverse Will Be Filled with 'Elves.'" *TechCrunch*, January 12. https://techcrunch.com/2022/01/12/the-metaverse-will-be-filled-with-elves/.

Rossen, Jake. 2017. "Losing Their Grip: An Oral History of Nintendo's Power Glove." Mental Floss, February 22. https://www.mentalfloss.com/article/91939/losing-their-grip-oral-history-nintendos-power-glove.

Rudnicki, Seweryn. 2017. "The Body, Technology and Translation: Mapping the Complexity of Online Embodiment." *Sociological Research Online* 22 (2): 35–47. https://doi.org/10.5153/sro.4322.

Rupp, Heather A., and Kim Wallen. 2007. "Sex Differences in Viewing Sexual Stimuli: An Eye-Tracking Study in Men and Women." *Hormones and Behavior* 51 (4): 524–33. https://doi.org/10.1016/j.yhbeh.2007.01.008.

Saarikoski, Petri. 2020. "The Rise and Fall of BBS Culture in Finland, 1982–2002." *WiderScreen* 23 (June): 2–3.

Sabri, Nazanin, Bella Chen, Annabelle Teoh, Steven P. Dow, Kristen Vaccaro, and Mai Elsherief. 2023. "Challenges of Moderating Social Virtual Reality." *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, April 19, 1–20. https://doi.org/10.1145/3544548.3581329.

Saghafi, Arash, and Spyros Angelopoulos. 2025. *Blurred Boundaries: Governance Challenges in Human-Like AI Interactions in Immersive Virtual Reality Platforms*.

Salát, Orsolya. 2015. *The Right to Freedom of Assembly: A Comparative Study*. Bloomsbury Publishing.

Salcito, Kendyl, Jürg Utzinger, Mitchell G. Weiss, et al. 2013. "Assessing Human Rights Impacts in Corporate Development Projects." *Environmental Impact Assessment Review* 42 (September): 39–50. https://doi.org/10.1016/j.eiar.2013.03.002.

Sanchez-Vives, Maria V., Bernhard Spanlang, Antonio Frisoli, Massimo Bergamasco, and Mel Slater. 2010. "Virtual Hand Illusion Induced by Visuomotor Correlations." *PLOS ONE* 5 (4): e10381. https://doi.org/10.1371/journal.pone.0010381.

Sandu, Bogdan. 2024. "How to Run Android on iPhone: Easy Steps." TMS Outsource, October 24. https://tms-outsource.com/blog/posts/how-to-run-android-on-iphone/.

Santa Clara Principles. 2021. "Santa Clara Principles on Transparency and Accountability in Content Moderation." https://santaclaraprinciples.org/images/santa-clara-OG.png.

Saunders, Benjamin, Julius Sim, Tom Kingstone, et al. 2018. "Saturation in Qualitative Research: Exploring Its Conceptualization and Operationalization." *Quality & Quantity* 52 (4): 1893–907. https://doi.org/10.1007/s11135-017-0574-8.

S.B., Abhinaya, Aafaq Sabir, and Anupam Das. 2024. "Enabling Developers, Protecting Users: Investigating Harassment and Safety in VR." arXiv:2403.05499. Preprint, arXiv, March 8. https://doi.org/10.48550/arXiv.2403.05499.

Scanlon, T.M. Jr. 1978. "Freedom of Expression and Categories of Expression." *University of Pittsburgh Law Review* 40 (4): 519–50.

Schlenker, Barry R. 2003. "Self-Presentation." In *Handbook of Self and Identity*. https://web.mit.edu/curhan/www/docs/Articles/15341_Readings/Self-presentation_Impression_Formation/Schlenker%20Self-Presentation%20492-518.pdf.

Schmälzle, Ralf, Sue Lim, Hee Jung Cho, Juncheng Wu, and Gary Bente. 2023. "The VR Billboard Paradigm: Using VR and Eye-Tracking to Examine the Exposure-Reception-Retention Link in Realistic Communication Environments." Preprint, bioRxiv, June 6. https://doi.org/10.1101/2023.06.03.543559.

Schmitz, Matheus, Keith Burghardt, and Goran Muric. 2022. "Quantifying How Hateful Communities Radicalize Online Users." *2022 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, November 10, 139–46. https://doi.org/10.1109/ASONAM55673.2022.10068644.

Schroeder, Ralph. 1993. "Virtual Reality in the Real World: History, Applications and Projections." *Futures* 25 (9): 963–73. https://doi.org/10.1016/0016-3287(93)90062-X.

Schroeder, Ralph. 2007. "An Overview of Ethical and Social Issues in Shared Virtual Environments." *Futures* 39 (6): 704–17. https://doi.org/10.1016/j.futures.2006.11.009.

Schroeder, Ralph. 2010. *Being There Together: Social Interaction in Shared Virtual Environments*. Oxford University Press.

Schulenberg, Kelsea, Guo Freeman, Lingyuan Li, and Catherine Barwulor. 2023. "'Creepy Towards My Avatar Body, Creepy Towards My Body': How Women Experience and Manage Harassment Risks in Social Virtual Reality." *Proceedings of the ACM on Human-Computer Interaction* 7 (CSCW2): 236:1-236:29. https://doi.org/10.1145/3610027.

Schulenberg, Kelsea, Lingyuan Li, Guo Freeman, Samaneh Zamanifard, and Nathan J. McNeese. 2023. "Towards Leveraging AI-Based Moderation to Address Emergent Harassment in Social Virtual Reality." *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, April 19, 1–17. https://doi.org/10.1145/3544548.3581090.

Scorgie, D., Z. Feng, D. Paes, F. Parisi, T. W. Yiu, and R. Lovreglio. 2024. "Virtual Reality for Safety Training: A Systematic Literature Review and Meta-Analysis." *Safety Science* 171 (March): 106372. https://doi.org/10.1016/j.ssci.2023.106372.

Searle, John R. 2018. *Constitutive Rules*. Version 1. https://doi.org/10.14275/2465-2334/20187.SEA.

"Second Life Incident Reports Repository." n.d. Accessed November 8, 2023. http://www.gridsurvey.com/blotter.php.

Segovia, Kathryn Y., and Jeremy N. Bailenson. 2009. "Virtually True: Children's Acquisition of False Memories in Virtual Reality." *Media Psychology* 12 (4): 371–93. https://doi.org/10.1080/15213260903287267.

Seoul Metropolitan Government. 2023. "Official Release of Metaverse Seoul." Seoul Metropolitan Government, January 25. https://english.seoul.go.kr/official-release-of-metaverse-seoul/.

Sethi, Aarushi. 2022. "Security and Privacy in Metaverse: Issues, Challenges, and Future Opportunities." *Cyber Security Insights Magazine*.

Shaffer Van Houweling, Molly. 2000. "Sidewalks, Sewers and State Action in Cyberspace." Preprint, June. https://cyber.harvard.edu/is02/readings/stateaction-shaffer-van-houweling.html.

Shakespeare, Tom. 2016. "The Social Model of Disability." In *The Disability Studies Reader*, edited by Lennard J. Davis. Routledge.

Shue, Henry. 1996. *Basic Rights: Subsistence, Affluence, and U.S. Foreign Policy*. Princeton University Press.

"SideQuest: Oculus Meta Quest Games & Apps Including AppLab Games (Oculus App Lab)." n.d. Accessed December 5, 2024. https://sidequestvr.com/.

Siegler, M.G. 2025. "There Is No VR Market, There Is a (Small) Meta Quest Market." Spyglass, March 19. https://spyglass.org/vr-market-share-meta-apple/.

Signorelli, Colleen. 2018. "Augmenting Our Reality: The (Un)Official Strategy Guide to Providing First Amendment Protection for Players and Designers of Location-Based Augmented Reality Video Games Notes." *St. John's Law Review* 92 (4): 943–76.

SimplyMac. 2024. "Can You Install Android on an iPhone?" May 16. https://www.simplymac.com/iphone/can-you-install-android-on-an-iphone.

Sittig, Dean F., and Hardeep Singh. 2010. "A New Sociotechnical Model for Studying Health Information Technology in Complex Adaptive Healthcare Systems." Original Research. *BMJ Quality & Safety* 19 (Suppl 3): i68–74. https://doi.org/10.1136/qshc.2010.042085.

Slater, Mel. 2009. "Place Illusion and Plausibility Can Lead to Realistic Behaviour in Immersive Virtual Environments." *Philosophical Transactions of the Royal Society B: Biological Sciences* 364 (1535): 3549–57. https://doi.org/10.1098/rstb.2009.0138.

Slater, Mel. 2021. "Beyond Speculation About the Ethics of Virtual Reality: The Need for Empirical Results." *Frontiers in Virtual Reality* 2 (August). https://doi.org/10.3389/frvir.2021.687609.

Slater, Mel, Cristina Gonzalez-Liencres, Patrick Haggard, et al. 2020. "The Ethics of Realism in Virtual and Augmented Reality." *Frontiers in Virtual Reality* 1 (March). https://doi.org/10.3389/frvir.2020.00001.

Slater, Mel, and Maria V. Sanchez-Vives. 2016. "Enhancing Our Lives with Immersive Virtual Reality." *Frontiers in Robotics and AI* 3 (December). https://doi.org/10.3389/frobt.2016.00074.

Slater, Mel, Bernhard Spanlang, Maria V. Sanchez-Vives, and Olaf Blanke. 2010. "First Person Experience of Body Transfer in Virtual Reality." *PLOS ONE* 5 (5): e10564. https://doi.org/10.1371/journal.pone.0010564.

Smith, Sophy. 2018. "Dance Performance and Virtual Reality: An Investigation of Current Practice and a Suggested Tool for Analysis." *International Journal of Performance Arts and Digital Media* 14 (2): 199–214. https://doi.org/10.1080/14794713.2018.1509256.

Snyder, Hannah. 2019. "Literature Review as a Research Methodology: An Overview and Guidelines." *Journal of Business Research* 104 (November): 333–39. https://doi.org/10.1016/j.jbusres.2019.07.039.

Solove, Daniel J. 2006. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154 (3): 477. https://doi.org/10.2307/40041279.

Sora-Domenjó, Carles. 2022. "Disrupting the 'Empathy Machine': The Power and Perils of Virtual Reality in Addressing Social Issues." *Frontiers in Psychology* 13 (September). https://doi.org/10.3389/fpsyg.2022.814565.

Sorrel, Charlie. 2024. "Vision Pro Teardown Part 2: What's the Display Resolution?" iFixit, March 23. https://www.ifixit.com/News/90409/vision-pro-teardown-part-2-whats-the-display-resolution.

Special Representative of the Secretary-General. 2008. "Report of the Special Representative of the Secretary- General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie' Human Rights Council Eighth Session." United Nations, April 7. https://documents.un.org/doc/undoc/gen/g08/128/61/pdf/g0812861.pdf.

Spiegel, James S. 2018. "The Ethics of Virtual Reality Technology: Social Hazards and Public Policy Recommendations." *Science and Engineering Ethics* 24 (5): 1537–50. https://doi.org/10.1007/s11948-017-9979-y.

Stamps, Norman L. 1942. "Freedom of Assembly." *University of Kansas City Law Review* 11 (4): 187–202.

Stanford HAI, dir. 2022. *Jeremy Bailenson: Your Mind on the Metaverse*. 57:27. https://www.youtube.com/watch?v=idD1rZ7UqT0.

Stanton, Aaron. 2016. "Dealing With Harassment in VR." UploadVR, October 25. https://www.uploadvr.com/dealing-with-harassment-in-vr/.

Star, Susan Leigh. 1999. "The Ethnography of Infrastructure." *American Behavioral Scientist* 43 (3): 377–91. https://doi.org/10.1177/00027649921955326.

Star, Susan Leigh. 2002. "Infrastructure and Ethnographic Practice." *Scand. J. Inf. Syst.*, September 1. https://www.semanticscholar.org/paper/Infrastructure-and-Ethnographic-Practice-Star/a2c21b02dc9264d25aaf6d9e625fdaf9329f78f2?p2df.

Statista. 2025. "AR & VR - China." Statista, August. https://www.statista.com/outlook/amo/ar-vr/china.

Stein, Scott. 2025a. "Samsung's Trifold Phone and AI Glasses Reportedly Set for Sept. 29 Launch." CNET, September 16. https://www.cnet.com/tech/computing/i-tried-snaps-upcoming-ar-glasses-again-get-ready-for-more-apps/.

Stein, Scott. 2025b. "Xreal One Review: Glasses That Make Me Forget the Vision Pro." CNET, January 30. https://www.cnet.com/tech/computing/xreal-one-review-glasses-that-make-me-forget-the-vision-pro/.

Stephens, Melodena. 2022. "The IEEE Global Initiative on Ethics of Extended Reality (XR) Report—Metaverse and Its Governance." IEEE.

Stephenson, Neal. 2003. *Snow Crash*. Random House Worlds.

Steuer, Jonathan. 1992. "Defining Virtual Reality: Dimensions Determining Telepresence." *Journal of Communication* 42 (4): 73–93. https://doi.org/10.1111/j.1460-2466.1992.tb00812.x.

Stone, Allucquere Rosanne. 1991. "Will the Real Body Please Stand up? Boundary Stories about Virtual Cultures." In *Cyberspace: First Steps*. MIT Press.

Stoner, Grant. 2022. "VR Is Here to Stay. It's Time to Make It Accessible." January 3. https://www.wired.com/story/virtual-reality-accessibility-disabilities/.

Suler, John. 2001. "The Psychology of Avatars and Graphical Space in Multimedia Chat Communities or: How I Learned to Stop Worrying and Love My Palace Props." In *Chat Communication*, edited by Michael Beiswenger.

Suler, John. 2004. "The Online Disinhibition Effect." *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society* 7 (3): 321–26. https://doi.org/10.1089/1094931041291295.

Sutherland, Ivan E. 1965. "The Ultimate Display." *Proceedings of IFIP Congress* 2 (January): 506–8. https://scispace.com/papers/the-ultimate-display-35zd3b9ucp.

TAKE IT DOWN Act, S.146, US Congress 119th (2025). https://www.congress.gov/bill/119th-congress/senate-bill/146.

Talus, Anu. 2023. "EDPB Reply to the Commission's Initiative for a Voluntary Business Pledge to Simplify the Management by Consumers of Cookies and Personalised Advertising Choices." European Data Protection Board, December 19. https://www.edpb.europa.eu/our-work-tools/our-documents/letters/edpb-reply-commissions-initiative-voluntary-business-pledge_en.

Tassi, Paul. 2021. "Mark Zuckerberg Is Building The Wrong Metaverse." Forbes, July 29. https://www.forbes.com/sites/paultassi/2021/07/29/mark-zuckerberg-is-building-the-wrong-metaverse/.

Team Counterpoint. 2025. "Global VR Market Declines 12% YoY in 2024; 'AR+AI' Smart Glasses to Take Centre Stage in 2025." Counterpoint, March 18. https://counterpointresearch.com/en/insights/global-xr-arvr-headsets-market-2024.

TechPolicy, dir. 2025. *AR/VR Policy Conference 2025*. 06:29:04. https://www.youtube.com/watch?v=dXY1bJCqO_w.

Tele2 Sverige AB v Post- Och Telestyrelsen and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis, Joined Cases C-203/15 and C-698/15 (Kammarrätten i Stockholm and the Court of Appeal (England & Wales) July 19, 2016). https://curia.europa.eu/juris/liste.jsf?num=C-203/15.

The Editors of Encyclopaedia Brittanica. 2025a. "Bhopal Disaster." In *Encyclopaedia Brittanica*. July 31. https://www.britannica.com/event/Bhopal-disaster.

The Editors of Encyclopaedia Brittanica. 2025b. "Damocles." In *Britannica*. August 26. https://www.britannica.com/topic/Damocles.

The Jargon File. n.d.-a. "Cracker." Accessed October 17, 2023. http://www.catb.org/jargon/html/C/cracker.html.

The Jargon File. n.d.-b. "Gender and Ethnicity." Accessed May 22, 2023. http://www.catb.org/jargon/html/demographics.html.

The Jargon File. n.d.-c. "Hacker." Accessed October 17, 2023. http://www.catb.org/jargon/html/H/hacker.html.

"THE PROJECT." 2024. *META-TOO*. https://meta-too.eu/the-project/.

"The Uncensored Library – Reporters without Borders." n.d. Accessed April 12, 2024. https://www.uncensoredlibrary.com/.

The Virtual Reality Show, dir. 2022. *VRChat's MAJOR Drinking Problem.* 7:51. https://www.youtube.com/watch?v=XS99QBGTS7E.

TheRodParticle. 2023. "The First Protest in Metaverse History! Creators protest in Horizon World because of Meta's prioritization of it's own events over creators." Reddit Post. R/HorizonWorlds, January 24. www.reddit.com/r/HorizonWorlds/comments/10k6i4d/the_first_protest_in_metaverse_history_creators/.

Thomson, Ewan. 2023. "These 3 Cities Already Have Their Own Metaverse." World Economic Forum, November 28. https://www.weforum.org/agenda/2023/11/metaverse-digital-cities-urban/.

Thorbecke, Catherine. 2023. "What Metaverse? Meta Says Its Single Largest Investment Is Now in 'Advancing AI.'" CNN, March 15. https://www.cnn.com/2023/03/15/tech/meta-ai-investment-priority/index.html.

Tinari, George. 2023. "A History of Apple AirPods: From Controversial Launch to Universal Triumph." MUO, June 7. https://www.makeuseof.com/history-of-apple-airpods/.

Tong, Goh Chiew. 2023. "Employee Surveillance Is on the Rise — and That Could Backfire on Employers." CNBC, April 24. https://www.cnbc.com/2023/04/24/employee-surveillance-is-on-the-rise-that-could-backfire-on-employers.html.

Torres, Isabelle Hupont, Vasiliki Charisi, Giuditta De Prato, et al. 2023. "Next Generation Virtual Worlds: Societal, Technological, Economic and Policy Challenges for the EU." European Commission, July 3. https://doi.org/10.2760/51579.

Treffers, Stefan R., and Randy K. Lippert. 2020. "Condominium Self-Governance? Issues, External Interests, and the Limits of Statutory Reform." *Housing Studies* 35 (6): 1025–49. https://doi.org/10.1080/02673037.2019.1646217.

Tucker, Joshua, Andrew Guess, Pablo Barbera, et al. 2018. "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature." *SSRN Electronic Journal*, ahead of print. https://doi.org/10.2139/ssrn.3144139.

Turkle, Sherry. 1994. "Constructions and Reconstructions of Self in Virtual Reality: Playing in the MUDs." *Mind, Culture, and Activity* 1 (3): 158–67.

Turkle, Sherry. 1997. *Life on the Screen*. Simon & Schuster.

Turner, Fred. 2010. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. University of Chicago Press.

Turner, Pixie G., and Carmen E. Lefevre. 2017. "Instagram Use Is Linked to Increased Symptoms of Orthorexia Nervosa." *Eating and Weight Disorders - Studies on Anorexia, Bulimia and Obesity* 22 (2): 277–84. https://doi.org/10.1007/s40519-017-0364-2.

Ugarte, Ramiro Álvarez. 2024. "From Soft Law to Hard Law: Human Rights Impact Assessments in the Digital Services Act Era." Tech Policy Press, June 20. https://techpolicy.press/from-soft-law-to-hard-law-human-rights-impact-assessments-in-the-digital-services-act-era.

"UN Global Compact." 2025. June 9. https://unglobalcompact.org/take-action/events/embed.

UN Secretary-General. 2020. "Roadmap for Digital Cooperation." June.

United Nations General Assembly. 1948a. "Universal Declaration of Human Rights." United Nations. https://www.un.org/en/about-us/universal-declaration-of-human-rights.

United Nations General Assembly. 1948b. "Universal Declaration of Human Rights." United Nations. https://www.un.org/en/about-us/universal-declaration-of-human-rights.

United Nations General Assembly. 2014. "The Right to Privacy in the Digital Age." January 21. https://documents.un.org/doc/undoc/gen/n13/449/47/pdf/n1344947.pdf.

United Nations General Assembly Human Rights Council. 2012. "Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development." July 16. https://primarysources.brillonline.com/browse/human-rights-documents-online/promotion-and-protection-of-all-human-rights-civil-political-economic-social-and-cultural-rights-including-the-right-to-development;hrdhrd99702016149.

United Nations High Commissioner for Human Rights. 2024. "Mapping Report: Human Rights and New and Emerging Digital Technologies." United Nations General Assembly, August 20. https://primarysources.brillonline.com/browse/human-rights-documents-online/promotion-and-protection-of-all-human-rights-civil-political-economic-social-and-cultural-rights-including-the-right-to-development;hrdhrd99702016149.

United Nations Human Rights Committee. 2011. "General Comment No. 34 on Article 19: Freedoms of Opinion and Expression." UN, September 12. https://digitallibrary.un.org/record/715606.

United Nations Human Rights Committee. 2020. "General Comment No. 37 (2020) on the Right of Peaceful Assembly (Article 21)." September 17. https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-37-article-21-right-peaceful.

United Nations Human Rights Office of the High Commissioner. 2011a. "Guiding Principles on Business and Human Rights." United Nations. https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf.

United Nations Human Rights Office of the High Commissioner. 2011b. "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework." https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

"Updates to User Reporting Requirements and Developer Tools in VR." 2023. *Meta Horizon Developer's Blog*, May 31. https://developers.meta.com/horizon/blog/user-reporting-requirements-developer-tools-updates.

Utz, Christine, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. "(Un)Informed Consent: Studying GDPR Consent Notices in the Field." *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, November 6, 973–90. https://doi.org/10.1145/3319535.3354212.

Vale, Sebastião Barros, and Daniel Berrick. 2023. "Reality Check: How Is the EU Ensuring Data Protection in XR Technologies? — The Digital Constitutionalist." January 25. https://digi-con.org/reality-check-how-is-the-eu-ensuring-data-protection-in-xr-technologies/.

Van Den Eede, Yoni. 2011. "In Between Us: On the Transparency and Opacity of Technological Mediation." *Foundations of Science* 16 (2): 139–59. https://doi.org/10.1007/s10699-010-9190-y.

Vanian, Jonathan. 2025. "Ray-Ban Meta Smart Glasses Revenue Tripled over the Year, EssilorLuxottica Says." CNBC, July 28. https://www.cnbc.com/2025/07/28/ray-ban-meta-revenue-tripled-essilorluxottica.html.

Vantrappen, Herman, and Frederic Wirtz. 2017. "When to Decentralize Decision Making, and When Not To." Organizational Restructuring. *Harvard Business Review*, December 26. https://hbr.org/2017/12/when-to-decentralize-decision-making-and-when-not-to.

Verbeek, Peter-Paul. 2012. "Expanding Mediation Theory." *Foundations of Science* 17 (4): 391–95. https://doi.org/10.1007/s10699-011-9253-8.

Verbeek, Peter-Paul. 2016. "Toward a Theory of Technological Mediation: A Program for Postphenomenological Research." In *Technoscience and Postphenomenology: The Manhattan Papers*. Lexington Books.

VerifyMyContent. n.d. "Live Streaming Moderation." Accessed April 19, 2024. https://verifymycontent.com/live-streaming.

Verizon. n.d. "Understanding the Models of the Metaverse." Verizon. Accessed September 3, 2024. https://www.verizon.com/about/blog/understanding-the-models-of-the-metaverse.

Vinciguerra, Robert A. 2015. "Tom Kalinske Talks About His Time Overseeing Sega As Its CEO In the 90s; Reveals That Sega Passed On Virtual Boy Technology, Considered Releasing 3DO." The Rev. Rob Times, September 21. https://web.archive.org/web/20150924024256/http://revrob.com/sci-tech/264-tom-kalinske-talks-about-his-time-overseeing-sega-as-its-ceo-in-the-90s-reveals-that-sega-passed-on-virtual-boy-technology-considered-releasing-3do.

Vindenes, Joakim, and Barbara Wasson. 2021. "A Postphenomenological Framework for Studying User Experience of Immersive Virtual Reality." *Frontiers in Virtual Reality* 2 (April). https://doi.org/10.3389/frvir.2021.656423.

Vinders, Julie. 2023. "Enhancing Legal Frameworks at the National and International Level: For the Governance of Climate Engineering, Neurotechnologies and Digital Extended Reality (D5.2)." European Commission, June 30. https://www.techethos.eu/wp-content/uploads/2023/07/TechEthos-D5.2-Enhancing-National-and-International-Legal-Frameworks-Draft.pdf.

Visual Venture, dir. 2023. *The Dark World of VRChat (Ft. iamLucid)*. 22:50. https://www.youtube.com/watch?v=exLtUH2bO6M.

Viture. n.d. "Introduction to VITURE XR Glasses." Accessed October 6, 2025. https://academy.viture.com/xr_glasses/introduction.

Vive Business. n.d. "VR in the Military." Accessed September 16, 2025. https://business.vive.com/us/stories/vr-in-the-military/.

VRChat. 2019. "Celebrating 5 Years of VRChat." *VRChat*, January 15. https://medium.com/vrchat/celebrating-5-years-of-vrchat-ffa0e8116929.

VRChat. 2023. “Announcing the Avatars for Everyone Winners.” VRChat, April 7. https://hello.vrchat.com/blog/avatars-everyone-winners.

W3C Working Group. 2021. “XR Accessibility User Requirements: W3C Working Group Note 25 August 2021.” August 25. https://www.w3.org/TR/2021/NOTE-xaur-20210825/.

Wachter, Sandra, and Brent Mittelstadt. 2019. “A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI.” *Columbia Business Law Review* 2019 (2): 2. https://doi.org/10.7916/cblr.v2019i2.3424.

Wagner, Justine. 2019. “Immersive Virtual Reality: Minnesota Legislature’s Opportunity to Protect Children from Sexual Exploitation by Enacting a Well-Defined Criminal Statute.” *Mitchell Hamline Law Review* 46 (2): 407–46.

Walker, Tom. 2025. “Apple’s Vision Air Could Conquer the Enterprise Market in 2027.” *XR Today*, September 8. https://www.xrtoday.com/virtual-reality/apples-vision-air-could-conquer-the-enterprise-market-in-2027/.

Wang, Dangxiao, Yuan Guo, Shiyi Liu, Yuru Zhang, Weiliang Xu, and Jing Xiao. 2019. “Haptic Display for Virtual Reality: Progress and Challenges.” *Virtual Reality & Intelligent Hardware*, Haptic Interaction, vol. 1 (2): 136–62. https://doi.org/10.3724/SP.J.2096-5796.2019.0008.

Wang, Yuntao, Zhou Su, Ning Zhang, et al. 2022. “A Survey on Metaverse: Fundamentals, Security, and Privacy.” *IEEE Communications Surveys & Tutorials*, 1–1. https://doi.org/10.1109/COMST.2022.3202047.

Wareham, Jamie. 2023. “New Maps Show Where It’s Illegal To Be LGBTQ In 2023.” Forbes, April 7. https://www.forbes.com/sites/jamiewareham/2023/04/07/new-maps-show-where-its-illegal-to-be-lgbtq-in-2023/.

Weatherbed, Jess. 2025. “Grok’s ‘Spicy’ Video Setting Instantly Made Me Taylor Swift Nude Deepfakes.” The Verge, August 5. https://www.theverge.com/report/718975/xai-grok-imagine-taylor-swifty-deepfake-nudes.

Welch, Chris. 2014. “Indian Politician Morphs into Hologram to Reach Millions of Voters.” The Verge, May 7. https://www.theverge.com/2014/5/7/5691714/indian-politician-uses-holograms-to-reach-voters.

Wells, Georgia, Jeff Horwitz, and Deepa Seetharaman. 2021. “Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show.” *The Wall Street Journal*, September 14. https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

Werner, John. 2024. “Catchup With Ivan Sutherland - Inventor Of The First AR Headset.” Forbes, February 23. https://www.forbes.com/sites/johnwerner/2024/02/23/catchup-with-ivan-sutherlandinventor-of-the-first-ar-headset/.

Whelan, Robbie, and Joe Flint. 2023. “Disney Eliminates Its Metaverse Division as Part of Company’s Layoffs Plan.” The Wall Street Journal, March 28. https://www.wsj.com/articles/disney-eliminates-its-metaverse-division-as-part-of-companys-layoffs-plan-94b03650?mod=djemalertNEWS&utm_source=substack&utm_medium=email.

WHO Team. 2020. "Addictive Behaviours: Gaming Disorder." October 22. https://www.who.int/news-room/questions-and-answers/item/addictive-behaviours-gaming-disorder.

Wildt, Lars de, Thomas H. Apperley, Justin Clemens, Robbie Fordyce, and Souvik Mukherjee. 2020. "(Re-)Orienting the Video Game Avatar." *Games and Culture* 15 (8): 962–81. https://doi.org/10.1177/1555412019858890.

Will, Pierre-Etienne. 2008. *The Chinese Contribution to the Universal Declaration of Human Rights, 1947-48*. January 1.

Williams, Maxine. 2022. "How We're Helping Build the Metaverse with Diversity, Equity and Inclusion in Mind." Meta Newsroom, June 16. https://about.fb.com/news/2022/06/how-were-helping-build-the-metaverse-with-diversity-equity-and-inclusion-in-mind/.

Wilson, Harry Robert. 2020. "New Ways of Seeing, Feeling, Being: Intimate Encounters in Virtual Reality Performance." *International Journal of Performance Arts and Digital Media* 16 (2): 114–33. https://doi.org/10.1080/14794713.2020.1770531.

Wilson, John R. 1996. "Effects of Participating in Virtual Environments a Review of Current Knowledge." *Safety Science* 23 (1): 39–51. https://doi.org/10.1016/0925-7535(96)00026-4.

Wisconsin Council of the Blind & Visually Impaired. 2021. "Accessible Cell Phones: Which Model Is Best for You?" Wisconsin Council of the Blind & Visually Impaired, November 18. https://wcblind.org/2021/11/accessible-cell-phones-which-is-best-for-you/.

Wodajo, Kebene, and Catherine McDonald. 2024. "Platform Enabled Structural Harms & The Limits of the Current Accountability Regime." Tech Policy Press, June 19. https://techpolicy.press/platform-enabled-structural-harms-the-limits-of-the-current-accountability-regime.

Won, Andrea Stevenson, Jeremy Bailenson, Jimmy Lee, and Jaron Lanier. 2015. "Homuncular Flexibility in Virtual Reality." *Journal of Computer-Mediated Communication* 20 (3): 241–59. https://doi.org/10.1111/jcc4.12107.

Wong, Geoff, Trish Greenhalgh, Gill Westhorp, Jeanette Buckingham, and Ray Pawson. 2013. "RAMESES Publication Standards: Meta-Narrative Reviews." *BMC Medicine* 11 (1): 20. https://doi.org/10.1186/1741-7015-11-20.

Woon, Chih Yuan. 2011. "'Protest Is Just a Click Away!' Responses to the 2003 Iraq War on a Bulletin Board System in China." *Environment and Planning D: Society and Space* 29 (1): 131–49. https://doi.org/10.1068/d3609.

World Economic Forum. 2022. "Shaping the Future of Media, Entertainment and Sport: Defining and Building the Metaverse." May.

worstnerd. 2020. "Understanding hate on Reddit, and the impact of our new policy." Reddit Post. R/Redditsecurity, August 20. www.reddit.com/r/redditsecurity/comments/idclo1/understanding_hate_on_reddit_and_the_impact_of/.

XR Association. 2024. "REALITY CHECK: The Importance of U.S. Engagement in Standards Development for Immersive Technology." XR Association, July. https://xra.org/wp-content/uploads/2023/05/XRA-Standards-Engagement-Advocacy-Sheet.pdf.

Yee, Nick, and Jeremy Bailenson. 2007. "The Proteus Effect: The Effect of Transformed Self-Representation on Behavior." *Human Communication Research* 33 (3): 271–90. https://doi.org/10.1111/j.1468-2958.2007.00299.x.

Yeh, Shih-Ching, Yuan-Yuan Li, Chu Zhou, Pin-Hua Chiu, and Jun-Wei Chen. 2018. "Effects of Virtual Reality and Augmented Reality on Induced Anxiety." *IEEE Transactions on Neural Systems and Rehabilitation Engineering* 26 (7): 1345–52. https://doi.org/10.1109/TNSRE.2018.2844083.

Yoti. 2023. "Yoti Facial Age Estimation White Paper." March. https://www.yoti.com/wp-content/uploads/Yoti-Age-Estimation-White-Paper-March-2023.pdf.

Yubo. n.d. "Yubo Scales Real-Time Audio Moderation Technology across Four Major International Markets." Accessed April 19, 2024. https://www.yubo.live/newsroom/yubo-scales-real-time-audio-moderation-technology-across.

Zallio, Matteo, and P. John Clarkson. 2022. "Designing the Metaverse: A Study on Inclusion, Diversity, Equity, Accessibility and Safety for Digital Immersive Environments." *Telematics and Informatics* 75 (December): 101909. https://doi.org/10.1016/j.tele.2022.101909.

Zenor, Jason. 2014. "Sins of the Flesh? Obscenity Law in the Era of Virtual Reality." *Communication Law and Policy* 19 (4): 563–89. https://doi.org/10.1080/10811680.2014.955778.

Zenou, Theo. 2022. "A Novel Predicted the Metaverse (and Hyperinflation) 30 Years Ago." *Washington Post*, June 30. https://www.washingtonpost.com/history/2022/06/30/snow-crash-neal-stephenson-metaverse/.

Zeno-Zencovich, Vincenzo. 2008. *Freedom of Expression: A Critical and Comparative Analysis*. Routledge-Cavendish. https://doi.org/10.4324/9780203893081.

Zhao, Jun. 2015. "China and the Uneasy Case for Universal Human Rights." *Human Rights Quarterly* 37 (1): 29–52.

Zhao, Yuhang, Edward Cutrell, Christian Holz, Meredith Ringel Morris, Eyal Ofek, and Andrew D. Wilson. 2019. "SeeingVR: A Set of Tools to Make Virtual Reality More Accessible to People with Low Vision." *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA), CHI '19, May 2, 1–14. https://doi.org/10.1145/3290605.3300341.

Zimmerman, Antonia. 2021. "European Countries Where Insulting the Head of State Can Land You in Prison." POLITICO, March 25. https://www.politico.eu/article/european-countries-where-insulting-head-of-state-can-land-prison-belgium-denmark-france-germany/.

Ziosi, Marta, Jakob Mökander, Claudio Novelli, Federico Casolari, Mariarosaria Taddeo, and Luciano Floridi. 2023. "The EU AI Liability Directive: Shifting the Burden From Proof to Evidence." SSRN Scholarly Paper No. 4470725. Rochester, NY, June 6. https://doi.org/10.2139/ssrn.4470725.

Zolides, Andrew. 2021. "Gender Moderation and Moderating Gender: Sexual Content Policies in Twitch's Community Guidelines." *New Media & Society* 23 (10): 2999–3015. https://doi.org/10.1177/1461444820942483.

Zuckerberg, Mark. 2021. "Founder's Letter, 2021." Meta Newsroom, October 29. https://about.fb.com/news/2021/10/founders-letter/.

Appendix 1: Disclaimer from Josh Cowls

Oxford, 6-9-2025

Subject: Collaboration with Emmie Hine

Dear University of Bologna Examiners,

This letter is to certify that Emmie Hine (legal name: Emma Elizabeth Hine) was the sole first author of the following article:

Hine, Emmie, Cowls, Josh, & Floridi, Luciano. Assembly and Expression in Extended Reality: Transposing Human Rights Across Realities. *Interactive Entertainment Law Review* (2025). https://doi.org/10.4337/ielr.2025.0003

Emmie, as first author, generated the idea for the article, conducted the literature review, and drafted the manuscript. My contributions were to provide feedback on initial drafts and to help to revise the manuscript before publication. I am happy for Emmie to include lightly edited versions of the articles in her dissertation.

Sincerely,

Josh Cowls

[electronically signed]

josh.cowls@gmail.com

Appendix 2: Disclaimer from Luciano Floridi

New Haven, 3 September 2025

Subject: Collaboration with Emmie Hine

Dear University of Bologna Examiners,

This letter is to certify that Emmie Hine (legal name: Emma Elizabeth Hine) was the sole first author of the following articles:

Hine, E., Rezende, I.N., Roberts, H., Wong, D., Taddeo, M., Floridi, L. Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations. *Digital Society* (2024). https://doi.org/10.1007/s44206-024-00114-1

Hine, Emmie, Cowls, Josh, & Floridi, Luciano. Assembly and Expression in Extended Reality: Transposing Human Rights Across Realities. *Interactive Entertainment Law Review* (2025). https://doi.org/10.4337/ielr.2025.0003

Emmie, as first author, came up with the idea for the article, conducted the literature review, and drafted the manuscript. As her supervisor, I gave input to Emmie's ideas, gave feedback to the presentation of the arguments, and helped edit the manuscripts. I am happy for Emmie to include lightly edited versions of the articles in her dissertation.

I also grant her permission to include the below piece for which I was a contributing author in an Appendix.

Neroni Rezende, Isadora and Hine, Emmie and Taddeo, Mariarosaria and Floridi, Luciano, Policing across and within metaverses: How immersiveness changes the role of police in cyberspace (January 30, 2025). Forthcoming in the European Journal of Criminal Policy and Research. Available at SSRN: https://ssrn.com/abstract=5117546 or http://dx.doi.org/10.2139/ssrn.5117546.

Sincerely,

Luciano Floridi

Luciano Floridi

luciano.floridi@yale.edu

Appendix 3: Disclaimer from Isadora Neroni Rezende

Bologna, 3rd of September 2025

Subject: Collaboration with Emmie Hine

Dear University of Bologna Examiners,

This letter is to certify that Emmie Hine (legal name: Emma Elizabeth Hine) was the sole first author of the following article:

Hine, E., Rezende, I.N., Roberts, H., Wong, D., Taddeo, M., Floridi, L. Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations. *Digital Society* (2024). https://doi.org/10.1007/s44206-024-00114-1

Emmie, as first author, came up with the idea for the article, conducted the literature review, and drafted the manuscript. I contributed to Sections 5 and 6 and helped revise the manuscript before publication. I am happy for Emmie to include a lightly edited version of the article in her dissertation.

I also grant her permission to include the below piece for which I was first author in an Appendix. Emmie contributed to the writing and revisions.

Neroni Rezende, Isadora and Hine, Emmie and Taddeo, Mariarosaria and Floridi, Luciano, Policing across and within metaverses: How immersiveness changes the role of police in cyberspace (January 30, 2025). Forthcoming in the European Journal of Criminal Policy and Research. Available at SSRN: https://ssrn.com/abstract=5117546 or http://dx.doi.org/10.2139/ssrn.5117546.

Sincerely,

Isadora Neroni Rezende

Isadora Neroni Rezende

isadora.neroni2@unibo.it

Appendix 4: Disclaimer from Huw Roberts

Oxford, UK 05/09/2025

Subject: Collaboration with Emmie Hine

Dear University of Bologna Examiners,

This letter is to certify that Emmie Hine (legal name: Emma Elizabeth Hine) was the sole first author of the following article:

Hine, E., Rezende, I.N., Roberts, H., Wong, D., Taddeo, M., Floridi, L. Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations. *Digital Society* (2024). https://doi.org/10.1007/s44206-024-00114-1

Emmie, as first author, came up with the idea for the article, conducted the literature review, and drafted the manuscript. I contributed to revising the manuscript before publication. I am happy for Emmie to include a lightly edited version of the article in her dissertation.

Sincerely,

Huw Roberts

Huw Roberts

huw.roberts@oii.ox.ac.uk

Appendix 5: Disclaimer from Mariarosaria Taddeo

Oxford, 9 September 2025

Subject: Collaboration with Emmie Hine

Dear University of Bologna Examiners,

This letter is to certify that Emmie Hine (legal name: Emma Elizabeth Hine) was the sole first author of the following article:

Hine, E., Rezende, I.N., Roberts, H., Wong, D., Taddeo, M., Floridi, L. Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations. *Digital Society* (2024). https://doi.org/10.1007/s44206-024-00114-1

Emmie, as first author, came up with the idea for the article, conducted the literature review, and drafted the manuscript. I contributed to revising the manuscript before publication. I am happy for Emmie to include a lightly edited version of the article in her dissertation.

I also grant her permission to include the below piece for which I was a contributing author in an Appendix.

Neroni Rezende, Isadora and Hine, Emmie and Taddeo, Mariarosaria and Floridi, Luciano, Policing across and within metaverses: How immersiveness changes the role of police in cyberspace (January 30, 2025). Forthcoming in the European Journal of Criminal Policy and Research. Available at SSRN: https://ssrn.com/abstract=5117546 or http://dx.doi.org/10.2139/ssrn.5117546.

Sincerely,

Mariarosaria Taddeo

mariarosaria.taddeo@oii.ox.ac.uk

Appendix 6: Supplementary Article 1

Content Moderation in the Metaverse Could Be a New Frontier to Attack Freedom of Expression

Emmie Hine

Note: This article was originally published as a Commentary in *Philosophy & Technology* (see (Hine 2023)). It is presented below in unedited format.

Abstract

This Commentary examines the challenges faced by metaverse platforms in cross-border content moderation, focusing on the implications for freedom of expression and nondiscrimination. It highlights the difficulties in determining what to remove for which users as well as how to do so, which has serious implications for freedom of expression and our shared sense of reality. Proto-metaverse platforms such as Roblox and Minecraft face similar questions, but have not yet encountered major cross-jurisdictional issues because, as looking at traditional social media platforms reveals, content moderation is not merely a question of law and policy, but also of geopolitics and government priorities. To avoid a "Lowest Common Denominator Effect" where freedom of expression is infringed upon worldwide and discrimination is entrenched, this Commentary argues that metaverse platforms must clarify their moderation policies, assess their entry into specific markets based on local laws and their own values, and be prepared to exit overly restrictive markets.

1. Introduction

Artificial intelligence (AI) has overtaken the "metaverse"[135] as the technology topic of the day. However, despite headlines announcing the demise of the metaverse (such as (Olinga 2023)), rumors of its death have been much exaggerated. Companies are certainly scaling back investments—as they are in many areas—but development continues. Mark Zuckerberg, CEO of the "metaverse company," Meta, pushed back against the narrative "that we're somehow moving away from focusing on the metaverse vision," reiterating that Meta remains committed to investing in the metaverse as a long-term project (Dean 2023). Apple is reportedly planning on releasing a virtual reality (VR) headset this summer (Miller 2023), and the government of China, which last year released a five-year action plan on VR[136] remains committed to following through in industrial applications even as consumer investment pulls back (Jiang 2023).

This cooling of investment may benefit governance efforts. The EU is preparing to regulate "virtual worlds" after several Citizens' Panels.[137] One issue that must be considered but that will be difficult to regulate domestically is that of cross-border content moderation, which has implications for freedom of expression worldwide. In general, online platforms remove content based on the laws of the countries in which they operate and have users, either proactively or in response to takedown requests from governments. This problem is theoretically well-characterized: platforms remove or restrict locally illegal content for the users and/or website version based in that country (Goldman 2021). However, this Commentary will argue that in reality, economic and political factors significantly complicate cross-border content moderation. In the metaverse, the politics and the fundamental issue of determining for whom and where to remove content will be much trickier, both because users from different jurisdictions will mingle in the same environment and because the immersive nature of the metaverse means that expression goes beyond speech to avatar representation and behavior, making the question of what is

---

[135] The definition of "metaverse" and whether there is one "Metaverse" or many "metaverses" have yet to be settled (Floridi 2022). In this piece, I use the term broadly to include any immersive virtual world accessible to users from many different places.

[136] 虚拟现实与行业应用融合发展行动计划（2022—2026年）[Action Plan for the Integration and Development of Virtual Reality and Industrial Applications (2022-2026)], 2022.

[137] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13757-Virtual-worlds-metaverses-a-vision-for-openness-safety-and-respect_en

allowed even more political and pressing. The sense of presence created by immersion means that experiences trigger the same physiological and psychological responses as in the physical world (Parsons et al. 2009), and in platforms where users are represented by an avatar, they may identify with their avatar as an extension or representation of their own self (Freeman et al. 2020). Thus, experiences—including negative ones—impact users much like experiences in the physical world, meaning that, for example, hate speech in the metaverse could have an even more deleterious impact than hate speech on a traditional social media platform.

In this Commentary, I will address the difficulties metaverse platforms will face in cross-border content moderation, especially in cases where required removals violate a platform's stated values, and how they may impact individual freedoms of expression and non-discrimination guaranteed by the Universal Declaration of Human Rights[138] (UDHR). I will also consider the precedents (and lack thereof) of proto-metaverses such as Minecraft and Roblox, as well as traditional social media platforms.

2. The Difficulties of the Inevitable Cross-Border Moderation Conflicts

At the most fundamental level, content moderation is a question of *what* to remove *where* and *for whom,* as well as *how*. The metaverse presents difficulties across all four. I will first address the *how*. Moderating user-created worlds has already proven challenging for Meta's metaverse platform, Horizon Worlds. In Horizon Worlds, journalists created a world called the "Qniverse" and filled it with content and misinformation that violated Meta's Community Guidelines. Meta did not remove it even after multiple users reported it; it was only removed when the journalists inquired directly with Meta's communications department (Baker-White 2022). Horizon Worlds has only around 200,000 active users (Horwitz et al. 2022), but scale is already proving to be an issue. Automated moderation of immersive content, which involves not just posts but entire worlds, avatars, and other user-created content, is not as straightforward as 2D audiovisual content. However, if metaverse platforms become as popular as they themselves

[138] *Universal Declaration of Human Rights*, United Nations, 1948.

predict, human moderation will not be feasible at the scale required. New processes will have to be developed to ensure that content is appropriate (to say nothing of user behavior).

This brings us to the question of *what* is to be removed. Both platform standards and local laws must be considered. Platform standards are not always easy to apply, though. One theory the "Qniverse" journalists put forth was that moderators may have thought the world was parody, something that is difficult to judge when the content in question is an immersive world instead of text, images, and videos, which may contain more obvious context clues that identify their parodic nature. If this is difficult for human moderators, it will be even more so for automated moderation tools. Metaverse and proto-metaverse platforms require their users and content moderation to abide by local laws, but local laws may be in conflict with these platforms' stated values, which include community diversity,[139] inclusion,[140] and the ability to express yourself. [141] Under laws restricting free expression across the world, not just content but also user behavior and expression may be subject to moderation.[142] Countries have always had different standards regarding what speech is acceptable online and governments often issue takedown requests to platforms for violating content, but the embodied nature of metaverse platforms creates new avenues of restriction. For example, in 2022, Vladimir Putin signed into law an amendment to Russia's existing "gay propaganda law,"[143] banning all depictions of LGBTQ+ "propaganda" in media and prohibiting positive depictions of LGBTQ+ relationships (Rajvanshi 2022)—which could include the mere existence of avatars presenting an LGBTQ+ identity. The law has already been used to fine TikTok for not taking down LGBTQ+ content (Marrow 2022) and to arrest two gay content creators (Padgett 2023). This is one entry in a long list of laws restricting the expression of LGBTQ+ identity, including in Hungary (whose law was noted as similar to Russia's in a European Parliament resolution condemning

---

139 https://en.help.roblox.com/hc/en-us/articles/203313410-Roblox-Community-Standards
140 https://www.minecraft.net/en-us/community-standards
141 https://www.meta.com/en-gb/blog/quest/meta-avatar-puma-new-body-shapes-hair-clothing-textures
142 Some local laws may hinder any content moderation, such as a Texas law (currently blocked pending a Supreme Court case) attempting to ban political "censorship" that is written so broadly as to bar companies from blocking any content that is not explicitly illegal (Dwoskin 2023).
143 *On the Introduction of Amendments into Article 5 of the Federal Law "On the Protection of Children from Information Liable to Be Injurious to Their Health and Development" and Individual Legislative Documents of the Russian Federation Aimed at Protecting Children from Information Promoting the Denial of Traditional Family Values* No. 135-FZ, 2013.

it[144]) and Uganda (Bhandari 2023). According to Russia's law, displaying LGBTQ+ identity in online spaces is illegal, meaning that metaverse platforms could either be forced to prohibit Russian users from accessing spaces where any portrayal whatsoever of LGBTQ+ content could be present (i.e., everywhere), restrict LGBTQ+ content to specific areas where Russian users are prohibited (infringing on the freedom of expression of all non-Russian users), or selectively alter the appearance of avatars expressing LGBTQ+ identities to appear "straight" to Russian users (another severe violation of non-Russian users' autonomy and freedom of expression). Restricting LGBTQ+ expression on metaverse platforms would also be overtly discriminatory, violating Article 7 of the UDHR. These same questions apply to any case where some jurisdictions ban expression that others do not.

The question of *what* to remove overlaps with *for whom* content is to be banned. Metaverse platforms would have to restrict content for users based in the country where it is illegal. If they choose to remove content for only those users, the immersive nature of metaverse platforms would create situations where two users from different countries could be standing right next to each other and see completely different worlds, undermining any shared sense of reality. If they choose to remove such content for all users, other users' autonomy and freedom of expression (which includes the right to "seek and impart information" according to Article 19 of the UDHR) will be infringed on. Many social medial platforms ban wholesale content like pro-Nazi propaganda, which is illegal in Germany[145] but not elsewhere. This is generally accepted as benefitting everyone's online experience. Returning to the example of LGBTQ+ content, though, it would be discriminatory and severely curtail freedom of expression to ban it altogether. Despite this, platforms may face pressure from governments to broadly ban content. In January of 2023, the Indian government invoked emergency laws to block a BBC documentary unfavorable to Prime Minister Narendra Modi, ordering Twitter and YouTube to remove accounts sharing clips (Ellis-Petersen 2023). In an immersive metaverse, these actions would be akin to

[144] *European Parliament Resolution of 8 July 2021 on Breaches of EU Law and of the Rights of LGBTIQ Citizens in Hungary as a Result of the Legal Changes Adopted by the Hungarian Parliament* 2021/2780(RSP), 2021.
[145] Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322), as last amended by Article 2 of the Act of 22 November 2021 (Federal Law Gazette I, p. 4906).

storming movie theaters and television stations and confiscating all copies of a film, impacting not merely the content available to users, but their very realities.

The final issue platforms face regarding content moderation is *where* content is to be removed, i.e., on what version of the site and if different standards apply for public and private spaces. It has already been established that the very premise of the metaverse is that there are not different versions for different countries, but the public/private divide question remains. The journalists who created the "Qniverse" flagged the lack of clarity around Horizon Worlds community standards and content moderation in public versus private spaces, even though Facebook's Community Standards apply to both public and private groups.[146] Issues of who can access what content are likely to persist in private spaces as well, but could be more egregious because users may expect that their private spaces are a place where they can freely express themselves. Restricting specific content for users from specific countries in private spaces would violate that expectation and infringe on not only peoples' social experiences, but their freedom of expression.

3. Proto-Metaverse and Social Media Platform Precedent

One might assume that proto-metaverses like Roblox and Minecraft might provide precedent for how platforms can deal with these issues. After all, many of the above content moderation questions also apply to non-immersive platforms where users are depicted via avatars. However, neither metaverse nor proto-metaverse platforms have had to address significant cross-border content moderation issues. For metaverse platforms, part of the reason may be their operating area or scale. Meta's Horizon Worlds is (as of May 2023) only available in seven countries, all in Europe and North America,[147] and daily active VRChat users number in the tens of thousands.[148] Proto-metaverse platforms are larger, though. Roblox boasts millions of users in Russia and has games that would seem to fall afoul of the "gay propaganda

[146] https://about.fb.com/news/2020/09/keeping-facebook-groups-safe/
[147] https://www.meta.com/help/quest/articles/horizon/explore-horizon-worlds/horizon-supported-countries/
[148] https://metrics.vrchat.community/d/wnQj2Qjnk/vrchat-api-metrics?orgId=1&refresh=30s&from=now-5y&to=now

law," such as "LGBTQ+ Hangout,"[149] so the government could theoretically take action at any time. However, this would likely provoke significant international outrage, and there is precedent for governments ignoring virtual worlds that technically violate their laws. A Minecraft server called the "Uncensored Library" hosts articles that have been banned by various governments and is accessible to Minecraft users in any country. It was widely celebrated in the media, which perhaps contributed to its security—any government forcing its takedown would face widespread condemnation. Still, Nick Feamster of University of Chicago warned that "Governments will know about this - the articles are going across the internet. It's not going to be foolproof against a determined adversary" (Gerken 2020). The unknown factor is at what point governments will consider it worthwhile to take on platforms over content they disagree of, and it is here that social media platforms provide some insight, revealing the complex political dynamics of cross-border content moderation.

Best practices documentation for cross-border content moderation states that content restriction for locally illegal content should be "geographically proportionate" and preserve the broadest availability of "legitimate content" (Internet & Jurisdiction Policy Network 2021). When defining "legitimate content" and restrictions, platforms should look to Articles 19 of the UDHR and International Covenant on Civil and Political Rights (ICCPR)[150] (Internet & Jurisdiction Policy Network 2021), which protect the rights to freedom of opinion and expression, including the right to "seek, receive, and impart" information. Indeed, Meta states that if takedown requests are "inconsistent with international human rights standards,"[151] they may take no action. However, moderation decisions appear to be influenced more by political and commercial interests than the multi-step evaluation process laid out by Meta.[152] Meta's transparency reports reveal that they are not acting on takedown requests from the Russian government regarding pro-Ukraine content,[153] which could indicate that they are upholding their commitment to the right to free expression. Contradicting this is a May 2023 case regarding so-called

[149] https://www.roblox.com/games/5373028495/LGBTQ-Hangout
[150] *International Convention on Civil and Political Rights*, United Nations, 1966.
[151] https://transparency.fb.com/data/content-restrictions/content-violating-local-law/
[152] Ibid.
[153] https://transparency.fb.com/data/content-restrictions/case-studies/

anti-state content where Meta blocked access to 110 items alleging crimes and corruption by the Turkish government (which did *not* violate Meta's Community Standards) under threat of having Facebook banned altogether. [154] Twitter similarly restricted anti-government accounts and Tweets, and owner Elon Musk offered insight into the decision when he responded to a critical Tweet: "The choice is to have Twitter throttled in its entirety or limit access to some tweets. Which do you want?" (Musk 2023).[155] Though the implication is that this was the trade-off necessary to protect free speech more broadly, commercial interests are no doubt at play, as no platform wants the bottom-line impact of being blocked (Gillespie 2018). Despite the similar nature of these cases, one of the reasons Meta likely did not remove pro-Ukraine content at the behest of the Russian government is that Facebook is already blocked in Russia (Allyn and Selyukh 2022), so the government had limited leverage.[156] Furthermore, given the overwhelming pro-Ukraine sentiment in the West, complying with such requests would create a public relations nightmare that would damage their business elsewhere.

Thus far, proto-metaverse and metaverse platforms have not faced the content moderation battles that traditional social media companies have, likely due to their comparatively smaller size and reach. However, as they grow, it is almost certain that they will clash with governments over content moderation, and what happens will depend on a variety of political factors independent of the human rights impact of banning the content. For platforms to truly avoid infringing on freedom of expression, they would have to concretely establish what values they want to uphold and stand by them, but this may come at a cost of their ability to operate in certain countries.

4. Conclusion

[154] Ibid.
[155] Musk has been criticized for hypocrisy in his content moderation decisions after professing to be a "free speech absolutist" (Musk 2022). Even the most libertarian platforms are subject to laws and commercial pressures that force them to moderate content; the famously anti-moderation Parler still expanded its moderation policy when Apple and Google removed it from their app stores for allowing hate speech (Grant 2022), and all platforms are vulnerable to financial pressure from threats of blocking.
[156] Other forms of leverage may include fines and "hostage-taking laws" requiring platforms to have domestic staff who can be pressured and even detained (Elliott 2021).

Metaverse platforms will be subject to the same political and economic pressures in content moderation as traditional social media platforms and proto-metaverses, but with higher stakes due to the implications for user identity and expression in an immersive context. And yet, they will probably be governed primarily by private companies, especially when it comes to content moderation. Any forthcoming EU metaverse regulation may spread to other jurisdictions via the Brussels Effect, but it will not be able to address cross-border content moderation. In an interview, Meta CEO Mark Zuckerberg was asked about how the metaverse will be governed and expressed a vision of a regime of industry-set standards (Newton 2021), which in reality would likely have to co-exist with some amount of hard law. However, unless a standards body can devise a universally accepted standard for content moderation, platforms will continue to set their own, which risks creating a "Lowest Common Denominator Effect" where, for technical and political ease, metaverse platforms adopt the most restrictive content regulations worldwide, severely limiting user expression. Platforms are poised to have enormous control over metaverse content and thus the realities of their users. Governments will have power as well, but only in restricting otherwise legitimate content, not in compelling certain forms of speech to be permitted outside their borders.

The status quo where traditional social media platforms are in constant battles over platform availability may spell doom for the vision of a universal Metaverse—unless it is one where freedom of expression is significantly restricted. Instead of this dystopic vision, platforms should concede that the Metaverse will be a set of "splinterverses" and a) clarify how they will moderate content illegal in specific jurisdictions, b) select and justify which markets they enter based on their laws and the platform's professed values, and c) be prepared to exit markets that become overly restrictive, rather than capitulate to restrictions over threats of being banned. So long as different countries have different standards for free expression online, disparities in platform and content availability will exist. In the absence of international regulations establishing global content norms, the metaverse is set to be a critical new battleground in the fight for freedom of expression.

Works Cited

Alison, Tom. 2020. "Our Latest Steps to Keep Facebook Groups Safe." *Meta Newsroom*, September 17. https://about.fb.com/news/2020/09/keeping-facebook-groups-safe/.

Allyn, Bobby, and Alina Selyukh. 2022. "Russia Blocks Access to Facebook." Technology. *NPR*, March 4. https://www.npr.org/2022/03/04/1084580235/russia-blocks-facebook-twitter.

Baker-White, Emily. 2022. "Meta Wouldn't Tell Us How It Enforces Its Rules In VR, So We Ran A Test To Find Out." *Buzzfeed News*, February 11. https://www.buzzfeednews.com/article/emilybakerwhite/meta-facebook-horizon-vr-content-rules-test.

Bhandari, Aditi. 2023. "Uganda's Anti-Gay Bill Is the Latest and Worst to Target LGBTQ Africans." *Reuters*, April 7. https://www.reuters.com/graphics/UGANDA-LGBT/movakykrjva/.

Dean, Grace. 2023. "Mark Zuckerberg Says He Is Absolutely Not Abandoning the Metaverse as Company Division Loses $4 Billion." Business Insider, April 27. https://www.businessinsider.com/zuckerberg-says-he-isnt-abandoning-metaverse-as-division-loses-mount-2023-4.

Dwoskin, Elizabeth. 2023. "Tech Companies Are Gaming out Responses to the Texas Social Media Law." *Washington Post*, January 21. https://www.washingtonpost.com/technology/2022/10/01/texas-social-media-impact/.

Elliott, Vittoria. 2021. "New Laws Requiring Social Media Platforms to Hire Local Staff Could Endanger Employees." Rest of World, May 14. https://restofworld.org/2021/social-media-laws-twitter-facebook/.

Ellis-Petersen, Hannah. 2023. "India Invokes Emergency Laws to Ban BBC Modi Documentary." World News. *The Guardian*, January 23. https://www.theguardian.com/world/2023/jan/23/india-emergency-laws-to-ban-bbc-narendra-modi-documentary.

European Commission. 2023. "European Commission - Have Your Say." Text. European Commission - Have Your Say, May 3. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13757-Virtual-worlds-metaverses-a-vision-for-openness-safety-and-respect_en.

"European Parliament Resolution of 8 July 2021 on Breaches of EU Law and of the Rights of LGBTIQ Citizens in Hungary as a Result of the Legal Changes Adopted by the Hungarian Parliament (2021/2780(RSP))." 2021.

Film Family. 2023. "LGBTQ+ Hangout🌈." Roblox, May 1. https://www.roblox.com/games/5373028495/LGBTQ-Hangout.

Floridi, Luciano. 2022. "Metaverse: A Matter of Experience." *Philosophy & Technology* 35 (3): 73. https://doi.org/10.1007/s13347-022-00568-6.

Freeman, Guo, Samaneh Zamanifard, Divine Maloney, and Alexandra Adkins. 2020. "My Body, My Avatar: How People Perceive Their Avatars in Social Virtual Reality." *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, April 25, 1–8. https://doi.org/10.1145/3334480.3382923.

Gerken, Tom. 2020. "Minecraft 'Loophole' Library of Banned Journalism." US & Canada. *BBC News*, March 13. https://www.bbc.com/news/world-us-canada-51883247.

"German Criminal Code (Strafgesetzbuch – StGB)." n.d. Accessed April 28, 2023. https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.

Gillespie, Tarleton. 2018. "Regulation of and by Platforms." In *The SAGE Handbook of Social Media*, by Jean Burgess, Alice Marwick, and Thomas Poell. SAGE Publications Ltd. https://doi.org/10.4135/9781473984066.n15.

Goldman, Eric. 2021. "Content Moderation Remedies." *Michigan Technology Law Review* 28 (1): 1–60. https://doi.org/10.36645/mtlr.28.1.content.

Grafana. 2023. "VRChat API Metrics." https://metrics.vrchat.community/d/wnQj2Qjnk/vrchat-api-metrics?orgId=1&refresh=30s&from=now-5y&to=now.

Grant, Nico. 2022. "Parler Returns to Google Play Store." Technology. *The New York Times*, September 2. https://www.nytimes.com/2022/09/02/technology/parler-google-play.html.

Hine, Emmie. 2023. "Content Moderation in the Metaverse Could Be a New Frontier to Attack Freedom of Expression." *Philosophy & Technology* 36 (3): 43. https://doi.org/10.1007/s13347-023-00645-4.

Horwitz, Jeff, Salvador Rodriguez, and Meghan Bobrowsky. 2022. "Company Documents Show Meta's Flagship Metaverse Falling Short." Tech. *Wall Street Journal*, October 15. https://www.wsj.com/articles/meta-metaverse-horizon-worlds-zuckerberg-facebook-internal-documents-11665778961.

Internet & Jurisdiction Policy Network. 2021. "Toolkit Cross-Border Content Moderation." March. https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-21-104-Toolkit-Cross-border-Content-Moderation-2021.pdf.

Jiang, Yaling. 2023. "China's Metaverse Is All About Work." Tags. *Wired*, April 25. https://www.wired.com/story/china-metaverse-work-health-care/.

Marrow, Alexander. 2022. "Russia Fines TikTok for 'LGBT Propaganda', Twitch over Ukraine Content." Technology. *Reuters*, October 4. https://www.reuters.com/technology/russian-court-fines-tiktok-50000-over-refusal-delete-lgbt-content-2022-10-04/.

Meta Quest Blog. 2023. "Customize Your Meta Avatar With New Body Shapes, Hair and Clothing Textures, and More Ways to Express Yourself." April 27. https://www.meta.com/blog/quest/meta-avatar-puma-new-body-shapes-hair-clothing-textures.

Meta Store. 2022. "Supported Countries for Meta Horizon Worlds." September. https://www.meta.com/en-gb/help/quest/articles/horizon/explore-horizon-worlds/horizon-supported-countries/.

Meta Transparency Center. n.d. "Content Restrictions Based on Local Law." Accessed May 4, 2023. https://transparency.fb.com/data/content-restrictions/content-violating-local-law/.

Miller, Chance. 2023. "Apple 'Reality Pro' Headset Will Toggle between AR/VR, Serve as Mac Display, 2-Hour External Battery Packs, More." *9to5Mac*, January 23. https://9to5mac.com/2023/01/23/apple-reality-pro-headset-features-details/.

Minecraft. 2023. "Community Standards for Minecraft." April 13. https://www.minecraft.net/en-us/community-standards.

Ministry of Industry and Information Technology. 2022. "虚拟现实与行业应用融合发展行动计划（2022—2026年）[Action Plan for the Integration and Development of Virtual Reality and Industrial Applications (2022-2026)]." November 1. https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2022/art_775aaa3f77264817a5b41421a8b2ce22.html.

Musk, Elon [@elonmusk]. 2022. "Starlink has been told by some governments (not Ukraine) to block Russian news sources. We will not do so unless at gunpoint. Sorry to be a free speech absolutist." Tweet. Twitter, March 5. https://twitter.com/elonmusk/status/1499976967105433600.

Musk, Elon [@elonmusk]. 2023. "@mattyglesias Did your brain fall out of your head, Yglesias? The choice is have Twitter throttled in its entirety or limit access to some tweets. Which one do you want?" Tweet. Twitter, May 13. https://twitter.com/elonmusk/status/1657422401754259461.

Newton, Casey. 2021. "Mark Zuckerberg Is Betting Facebook's Future on the Metaverse." The Verge, July 22. https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview.

Olinga, Luc. 2023. "Mark Zuckerberg Quietly Buries the Metaverse." TheStreet, March 18. https://www.thestreet.com/technology/mark-zuckerberg-quietly-buries-the-metaverse.

On the Introduction of Amendments into Article 5 of the Federal Law "On the Protection of Children from Information Liable to Be Injurious to Their Health and Development" and Individual Legislative Documents of the Russian Federation Aimed at Protecting Children from Information Promoting the Denial of Traditional Family Values, Nos. 135-FZ (2013).

Padgett, Donald. 2023. "Gay TikTok Couple Arrest Under Anti-LGBTQ+ Law." April 9. https://www.advocate.com/russia/tiktok-russian-gay-couple.

Parsons, Thomas D., Christopher Courtney, Louise Cosand, Arvind Iyer, Albert A. Rizzo, and Kelvin Oie. 2009. "Assessment of Psychophysiological Differences of West Point Cadets and Civilian Controls Immersed within a Virtual Environment." In *Foundations of Augmented Cognition. Neuroergonomics and Operational Neuroscience*, edited by Dylan D. Schmorrow, Ivy V. Estabrooke, and Marc Grootjen. Lecture Notes in Computer Science. Springer. https://doi.org/10.1007/978-3-642-02812-0_60.

Rajvanshi, Astha. 2022. "What to Know About Russia's So-Called 'Gay Propaganda' Bill." Time, November 24. https://time.com/6236822/russia-gay-propaganda-law-discrimination/.

Roblox Support. 2023. "Roblox Community Standards." March 15. https://en.help.roblox.com/hc/en-us/articles/203313410-Roblox-Community-Standards.

Transparency Center. n.d. "Case Studies." Accessed May 17, 2023. https://transparency.fb.com/data/content-restrictions/case-studies/.

United Nations General Assembly. 1948. "Universal Declaration of Human Rights." United Nations. https://www.un.org/en/about-us/universal-declaration-of-human-rights.

United Nations General Assembly. 1966. "International Covenant on Civil and Political Rights." December 16. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

Appendix 7: Supplementary Article 2

Policing *Across* and *Within* Metaverses: How Immersiveness Changes the Role of Police in Cyberspace

Isadora Neroni Rezende, Emmie Hine, Mariarosaria Taddeo, Luciano Floridi

Note: This article was originally published as a peer-reviewed journal article in the *European Journal on Criminal Policy and Research* (see (Neroni Rezende et al. 2025)). It is presented below in unedited format. For author statements, please see Appendices 1, 2, and 5.

Abstract

Explicit abusive behaviour in the metaverse is increasing, so regulators and other supranational bodies are considering whether this immersive virtual space should be policed and how. In this article, we address this question by arguing that involving national and international police organizations in the metaverse is necessary and demands regulatory action. First, we show that the scope of criminal law should extend to the metaverse and that a policing mechanism is needed to ensure its enforcement. Then, we highlight the shortcomings of existing ways of policing the Web and argue that only a co-governance system involving platforms, online communities, and law enforcement agencies can address the challenges of policing the metaverse. We examine how this undertaking may work using two Levels of Abstraction (LoAs). Through the first LoA, we analyse the metaverse environment from the outside and investigate how policing efforts should be allocated between States across multiple platforms, suggesting ways to solve jurisdictional conflicts. Through the second LoA, we analyse a given metaverse from within and assess the limits of police powers concerning user surveillance and the possibility of performing virtual 'arrests'. In both cases, we show how the immersiveness of the metaverse will change the role of the police online. We conclude the article with recommendations for establishing a policing mechanism in the metaverse.

1. Introduction

The metaverse is an emerging type of immersive virtual environment (Hine et al., 2024).[157] Explicit abusive behaviour in this type of environment is a growing concern for regulators and other supranational bodies. The European Parliament and European Union Agency for Law Enforcement Cooperation (EUROPOL) commissioned studies on this topic (EUROPOL, 2022; Madiega et al., 2022), and the EU Commission launched a public consultation on virtual worlds, emphasising the need to ensure their safety and security (European Commission, 2023). The International Criminal Police Organization (INTERPOL) is also investigating how to police the metaverse (Cieslak & Gerken, 2023) and released a report on its challenges for law enforcement (INTERPOL, 2024). Users too are raising demands for safety (Zallio & Clarkson, 2022) and have reported being harassed in the metaverse (Basu, 2021; Sales, 2024). How the metaverse may be policed is the topic of this article. Before developing our analysis, some remarks are necessary to clarify and contextualise the exact nature of the problem.

The metaverse is not a unique environment but comprises a plurality of specific 'metaverses', built according to different logics. Many distinguish between centralised-proprietary (also called 'private') and decentralised-distributed (often defined as 'public') metaverses. Corporations (e.g., Meta or VRChat) develop metaverses as centralised platforms where the business model is based on paid services, such as games, and advertisements targeted to users by leveraging their data. Distributed metaverses are instead run by decentralised autonomous organisations (DAOs), owned collectively by their communities (Nabben, 2021, p. 2). They may be inspired by 'crypto-anarchist' and libertarian thinking and rely on distributed ledger technologies like smart contracts to replace traditional hierarchical governance (Atzori, 2017; Santana & Albareda, 2022). While this distinction revolves around the ownership regime of the metaverse, one may argue that the infrastructural model behind a given platform will not be relevant

[157] There is no agreed definition of what the metaverse is. The European Parliamentary Research Service describes it as 'an immersive and constant virtual 3D world where people interact by means of an avatar to carry out a wide range of activities', see (Madiega et al., 2022, p. 1) The metaverse is supported by extended reality (XR) technologies, a spectrum that includes virtual reality (VR, when users are immersed in a virtual environment, often with a headset), augmented reality (AR, where virtual information is juxtaposed with the physical world), and mixed reality (MR, where objects of the physical and virtual worlds are presented together in a single display) (Milgram & Kishino, 1994) Contemporary versions of the metaverse are distinguished from 'proto-metaverses' like *Second Life*, *Fortnite*, and *Roblox,* which lack the immersive (XR) element.

regarding the demand for safety. Therefore, keeping users safe will raise similar issues in centralised (or 'private') and decentralised (or 'public') metaverses, although policing the latter will be more challenging due to their hostility toward State intervention.

In light of this, the distinction between public and private metaverses should not be based on who owns the platform but on how users experience this virtual environment (Floridi, 2022), as further explained in Section 5. Therefore, here we focus on immersiveness, a crucial characteristic of the metaverse, which is its added value but may also elicit malicious behavior and expose users to harm.

Scholars and regulators have only begun exploring the ethical and legal implications of the metaverse (Cheong, 2022; Garon, 2022) and still debate whether specific behaviors committed there amount to criminal offenses (Haber, 2024; Lemley & Volokh, 2017). For instance, financial crime is significant in crypto-markets and may soon expand in this environment (Mackenzie, 2022), while live speech and quasi-physical interactions may increase other forms of crime in the metaverse, as we will show in Section 2.

Against this background, a study by the European Parliament asks whether we should create a 'metaverse criminal justice system' (Madiega et al., 2022, p. 8). In this article, we address this question by arguing that involving policing organisations in the metaverse is necessary and demands regulatory action. After showing that the metaverse should be policed, we examine how immersiveness will change police activities online to offer policy recommendations using two levels of abstraction (LoAs) (Floridi, 2008). Through the first LoA, we observe the metaverse from the *outside*, analysing how States can ensure an adequate distribution of policing powers across multiple metaverses. Immersive technologies create a new kind of virtual space where avatars will move around and interact as in the analogue world. The consequence will be to prompt responses by public authorities, in terms of real-time assistance to users and crime prevention, as well as transnational police cooperation. Through the second LoA, we examine how policing should work *within* a given metaverse, exploring what powers the police can exercise and under which circumstances. Immersiveness generates new avenues for police action online and, therefore, risks to users' fundamental rights, which regulators should address too.

The metaverse is a pan-jurisdictional space, so it should be governed at the transnational level. Therefore, our analysis offers some policy recommendations addressed to States at the international level but also considers the EU context due to its potential Brussels effect. We do not provide an exhaustive analysis of all the issues related to policing the metaverse, such as using emotional data in surveillance or ensuring cross-border access to digital evidence. These issues are metaverse-*relevant*, but not metaverse-*specific*.

The rest of this article is structured as follows. In Section 2, we explain why criminal law should apply to some metaverse behaviours. In Section 3, we argue that existing ways of policing the Web are not enough to ensure the enforcement of criminal law and that specific regulatory intervention is needed to address the criminal potential of the metaverse. In the remainder of the analysis, we examine how metaverse policing should be regulated at the two LoAs. In Section 4, we analyse how police efforts should be allocated among States and suggest ways to solve jurisdictional conflicts. In Section 5, we assess how police powers should be exercised within a given metaverse by focusing on the limits to platform surveillance and the possibility of performing virtual 'arrests' to prevent crimes. In Section 6, we conclude the article by suggesting some recommendations for policing the metaverse.

2. On the applicability of criminal law in the metaverse

Identifying harmful behaviour and defining crimes are a priority to ensure user safety in virtual worlds (INTERPOL, 2024, p. 12)—even more so, as immersive technologies will also offer new avenues for committing crimes. Experts are debating whether (and which) criminal law should cover metaverse actions. Interpretations vary according to national laws and theoretical approaches (Gómez-Quintero et al., 2024; Haber, 2024). In the past, some have raised 'law of the horse'[158] arguments, contending that illicit actions within the metaverse do not raise new legal questions and should be treated, where possible, as regular crimes (S. Brenner, 2001; Laue, 2011). Nonetheless, many of these claims were elaborated in

[158] See (Easterbrook, 1996; Lessig, 1999).

reaction to the first developments of virtual worlds (e.g., multi-player games) and thus fail to acknowledge the potential of immersive technologies of the latest versions of the metaverse.

We argue that the scope of criminal law should extend to the metaverse and that, to do so, specific policy action for both existing cybercrimes and emerging criminal behaviours is required to address gaps in legislation. This is because (i) the applicability of criminal law in the metaverse will justify the involvement of State authorities in its policing, in the terms explained in Sections 4 and 5; (ii) an effective police response, including at the supranational level, will also depend on clear legislation on the matter (INTERPOL, 2024, p. 11).

The distinction between *illicit*, *illegal*, and *criminal* behaviour illustrates why regular cybercrime will become more problematic in the metaverse, and why new virtual behaviours should be criminalised. *Illicit* conduct refers to actions forbidden or disapproved of by moral or social codes (including the law) (Stevenson, 2010). When some conduct directly violates positive law, it is also considered *illegal*. At the same time, illegal behaviour is not always *criminal*. Only actions that wrongfully cause significant harm to others can be criminalised (Ashworth, 2006, p. 31). Indeed, the harm principle is a cornerstone of criminal law in common and civil law systems (Ashworth, 2006; Keiler & Roef, 2019). Criminal law traditionally focuses on 'hard' (i.e., physical) harms, although it has expanded to 'soft' harms of a moral or emotional nature (S. W. Brenner, 2008, p. 3), leading to the criminalisation of gambling, harassment, and stalking. However, criminal law does not encompass *any* harmful behaviour, such as trifling wrongs, and presupposes that perpetrators deserve blame for their actions. In fact, although the scope of criminal law protection has expanded, some argue that the legal approach remains selective and fragmented, often failing to address the full spectrum of harm (Michalowski, 2016, pp. 182–185). Traditional legal frameworks tend to focus narrowly on individual wrongdoing, often neglecting the broader structural causes of harm, particularly when they originate from systemic inequalities or powerful institutions (Hillyard & Tombs, 2007, pp. 12–13). Instead, an approach based on social harms would widen the scope of protection to include physical, economic, emotional, psychological and cultural harms — issues that sometimes fall outside the remit of criminal justice despite their significant social impact (Hillyard &

Tombs, 2021, pp. 23–24; Pemberton, 2007, p. 37). Therefore, this perspective should be incorporated into discussions about the criminalisation of behaviour in emerging digital environments such as the metaverse. This would ensure that harmful virtual conduct is recognised and addressed appropriately, without being limited by conventional definitions of crime.

In the metaverse, illicit behaviour will generate both soft and hard harms that should be addressed by criminal legislation. In particular, the quality and quantity of harmful experiences for users will increase because of the combination of three features of immersive technologies: (i) interactivity; (ii) telepresence; and (iii) immersiveness (Mütterlein, 2018).

Concerning interactivity, the metaverse increases users' capabilities to influence the form or content of the digital environment, adding the possibility of 'spatial harms' through gestures, postures, and digital assets (World Economic Forum, 2023b). Individuals will be harmed not only by content (e.g., hate speech) but also through interactions that will resemble analogue-world ones. As a three-dimensional space, the metaverse will provide new avenues for offenses like stalking, sexual harassment, assault, or virtual 'rape' (Sethi, 2022, pp. 2–3). From the early days of the metaverse, users (especially those using female avatars) reported distressing invasions of their personal space, often coupled with crude sexual gestures (Basu, 2021). In 2024, British police started investigating the virtual gang rape of a girl below the age of 16 (Sales, 2024) and different inquiries have highlighted that all kinds of sexual assaults (especially against women's avatars and minors) are a matter of routine in the metaverse (Bates, 2025; Centre for Countering Digital Hate, 2023; SumOfUs, 2022). Although the criminal (or even illegal) nature of such abusive behaviour has been questioned for proto-metaverses (S. W. Brenner, 2008), immersive technologies force users to experience these interactions vividly, even without a physical component (Haber, 2024, p. 870), causing genuine psychological harm (Hine et al., 2024). Furthermore, the possibility to move around and interact with virtual objects will also generate new forms of property crime: criminals may steal or damage metaverse assets, or intrude into users' personal space, generating emotional distress or financial loss in the analogue world as well (INTERPOL, 2024, p. 14). This type of crimes dates to the early days of social worlds. In 2005, for example, a Japanese man was arrested on suspicion of 'virtual mugging' for using a bot to rob and beat up characters in the Lineage II game (Knight, 2005). A few years later, a Dutch teenager was also arrested for stealing virtual furniture worth €4,000 from the Habbo Hotel platform (BBC, 2007). Some countries – such as China, Japan, and the United Kingdom –now recognise the possibility of taking legal action against the deprivation of digital assets, provided that they have monetary value in the analogue world (Fortis, 2023; Qin et al., 2025, p. 4). However, some argue that in the metaverse this protection should extend beyond financial assets to include digital possessions that hold emotional significance for users, even if they lack economic value (Qin et al., 2025, p. 4; H. Wang, 2023, p. 3).

Metaverse equipment (e.g., headsets) fosters users' sense of telepresence – that is, the state of presence reached using a medium (Mütterlein, 2018, p. 1408) – but also provides opportunities for new forms of manipulation (INTERPOL, 2024, p. 15). Malicious actors can hack these devices and introduce sensory stimuli, altering people's perception of the surroundings (Tseng et al., 2022, p. 4), potentially harming individuals' physical integrity and personal autonomy. One potential avenue for harm is redirected walking, which steers users' physical path by unperceptively rotating the virtual scene. Redirect walking can be used to improve user experience by making users believe they are walking a long distance in a straight line when they are actually walking around a confined space (De Back et al., 2024); however, studies have shown that criminals may employ it to harass users (Casey et al., 2021), causing emotional distress, or exposing them to dangerous situations, for example, by pushing them towards stairs or a street (Gómez-Quintero et al., 2024, p. 11; Nichols, 2022; Y. Wang et al., 2022, p. 22). Equipment such as headsets, haptics, or teledildonics may also offer more realistic sexual experiences and encourage the commission of related offenses, such as the provision of AI-generated child sexual abuse materials (Gómez-Quintero et al., 2024, p. 18). In South Korea, for example, a man was sentenced to four years imprisonment for producing and storing sexually explicit contents involving minors he groomed in the metaverse (Adejumo, 2022).

Combined with interactivity and telepresence, emotional immersiveness will also increase the harmfulness of existing crimes and other illicit behaviours in the metaverse. Research shows that immersive technologies increase users' psychological presence or their sense of 'being there' (Makransky & Mayer, 2022; Murray & Sixsmith, 1999); that is, a feeling of embodiment created by freedom of movement; stereoscopy, a broader field of view that strengthen the impression of being within an environment (Cummings & Bailenson, 2016); and a sensory realism from visual, auditory, tactile, and even olfactory stimuli (Cadet & Chainay, 2020; Gromer et al., 2019). Such features create a correlation between users' virtual bodily actions and their physical counterparts (Cummings & Bailenson, 2016, p. 3). As a result, users will experience metaverse events and encounters almost like their analogue correspondents (Dwivedi et al., 2022, p. 4). Research shows that virtual reality (VR) experiences trigger many of the same psychological and physiological reactions as experiences in the physical world (Martens et al., 2019). Therefore, illicit behaviour committed in the metaverse may have illegal consequences that are best addressed with criminal law instruments (Haber, 2024, p. 845). Illustrating this, police in the UK are investigating a case of 'virtual rape' that reportedly left a girl traumatised, even if it is unclear whether existing criminal law will be able to address her case (Farrant, 2024). Thus, there is a chance that illegal actions may remain unpunished. The risk of harm is even more serious for children, who may be more vulnerable to exploitation and struggle to distinguish what is real and what is make-believe (Sales, 2024). In Horizon Worlds, it has been found that nearly 7 out of 10 worlds are visited by minors, including 'Mature Worlds', where Meta permits sexually explicit content, legal drugs promotion, and gambling (Centre for Countering Digital Hate, 2023, pp. 4–5). Although adult users are permitted access to such environments, there are no safety measures in place to prevent children from entering. Consequently, researchers have uncovered many instances of harassment against underage users, who were frequently subjected to sexually explicit insults (Centre for Countering Digital Hate, 2023, p. 6).

In this perspective, existing crimes aimed at causing fear and emotional distress – such as blackmail, cyberbullying, incitement to self-harm, harassment, or stalking – will have a heightened negative impact on users, as immersion will increase the sense of threat perceived by victims. Similar effects will be achieved by other cybercrimes, like identity and data theft, illegal use of deepfakes, or property crimes, which usually cause non-material damages beyond financial loss. Griefing and other violations of game rules may not be considered trifling wrongs anymore, as immersion will enhance their emotional and long-term impact on victims (Oppenheim, 2022). Beyond individual harms, the metaverse may also be leveraged as a tool to commit crimes against public safety, like propaganda, misinformation, radicalisation, and indoctrination, also related to terrorism. For instance, the Australian Federal Police has warned that extremist groups are infiltrating proto-metaverses such as Roblox to target child users (Australian Associated Press, 2023). In these cases, immersion may intensify the potential for manipulation, causing users to make uninformed decisions with harmful consequences at the collective level (INTERPOL, 2024, p. 15). Terrorist groups may even use metaverse spatiality to rehearse their plans in three-dimensional environments, leading to improved coordination of real-world attacks (Hine et al., 2024; INTERPOL, 2024, p. 15). Exemplifying this, a self-radicalised Singaporean teenager was issued with a restriction order for joining ISIS-themed settings on Roblox, where he role-played as a soldier of the Caliphate in replicas of conflict zones such as Syria and Marawi City. The teenager also used footage from the game to create propaganda videos depicting ISIS factions carrying out attacks (Singapore Ministry of Home Affairs, 2023). Another controversial case involves a Russian teenager who was sentenced to five years in prison for allegedly planning to blow up a virtual Federal Security Service (FSB) building in Minecraft (France-Presse, 2022).

Empirical evidence of crimes committed in the metaverse is, often, still limited to specific incidents reported in the news, so more extensive research would certainly be needed to gain a comprehensive understanding of the phenomenon. Nevertheless, the accounts and scenarios presented show the risks of the metaverse causing actual harm to people, and yet, users may not be protected under existing criminal legislation, which has been mainly designed to address the physical and emotional harms of the analogue world. A theoretical and a practical reason supports the need for enacting specific legislation on metacrimes (i.e., crimes committed in the metaverse).

At the theoretical level, harms prompted in the metaverse will differ in nature and intensity, so specific legislation is needed to criminalise such behaviours or adjust sanctions accordingly. Concerning the nature of the harms, traditional crimes, such as rape or kidnapping, may be simulated in the metaverse, but the physical element of the *actus reus* will be missing. Therefore, these experiences will not compare to their analogue correspondents, and the harm suffered by victims will be qualitatively different. If the criminalisation of rape and kidnapping aims to protect values such as (physical) sexual integrity and personal freedom, corresponding metacrimes will have to be mainly construed to address emotional distress. Speaking instead of the intensity of the harm, the negative consequences of existing cybercrimes (e.g., hate speech or indoctrination) will easily extend to the metaverse but may deserve more severe sanctions when committed there, considering the higher intensity of the psychological impact on users.

Enacting *ad-hoc* legislation for crimes committed in the metaverse is also needed for a practical reason: to ensure the effectiveness of transnational criminal cooperation. Following the 'law of the horse' argument, one may contend that existing legislation may be enough to address illegal behaviours since, for example, virtual rapes will not qualify as such under national law but may still be prosecuted as battery or harassment. However, such an approach will likely cause fragmentation because States may not agree on the legal qualification of the same conduct or have conflicting definitions for similar crimes committed in the metaverse, as in the case of the 'virtual rape' mentioned above. Under such conditions, States may refuse to cooperate and bring suspects and accused to justice, undermining the effective enforcement of criminal law for crimes perpetrated in this kind of environment.

The need to apply criminal law in the metaverse highlights the importance of policing virtual worlds. Platforms and the police are already active on the Web, but their efforts may not be enough to address the challenges of immersive environments. The following section explains why and provides arguments for establishing a specific policing mechanism for the metaverse.

3. From platform moderation to policing the metaverse

If criminal law applies in the metaverse, then policing is necessary to ensure its effective enforcement. In this section, we examine how private actors and the police act on the Web to moderate user behaviour, highlighting the strengths and weaknesses of current approaches. Privately enforced mechanisms of content moderation are prominent but arguably problematic from a fundamental rights perspective, while police initiatives are scarce but potentially more safeguarding for users. Given this situation, we argue that only the combined intervention of private and public entities can effectively address crime threats in the metaverse.

In the traditional Web, platforms address user behaviour through Terms of Service (ToS) and/or community guidelines. Platforms manage infringements through content moderation mechanisms (Hine, 2023), but, occasionally, they also determine criminal liability under national legislation (Toolkit: Cross-Border Content Moderation, 2021). Content moderation can be oriented more towards platform moderators, like on Reddit, or automated systems can be used as a first line of defence, such as on Facebook. Many platforms use some combination of both.

Online communities also have a role in ensuring public safety and order on the Internet. Traditionally, community self-policing has contributed to the police function in society (Robinson & Scaglion, 1987, p. 116), and it has applicability in virtual environments as well (Headleand et al., 2020, p. 121). For example, in *World of Warcraft*, game communities established regulations to counter misconduct, such as cheating, toxic behaviour, and verbal aggressions, and participate in self-surveillance to enforce them (Collister, 2014). In Meta's Horizon Worlds, 'volunteer moderators' monitor spaces in real-time and intervene in escalating situations by muting or removing other users in more serious cases (Meta, 2024).

Although platform content moderation systems and communities will be helpful in the metaverse to manage user behaviour, more needs to be done to keep users safe, as current mechanisms are not enough to address the crime potential of the metaverse. Two reasons support this need. The first relates to the quality of the policing from a user fundamental rights perspective. Even when no crime occurs, policing affects how individuals experience an environment, whether analogue or digital. Generally, police efforts increasingly focus on offenses yet to be committed. Their presence in specific areas is often linked to deterrence (Marthews & Tucker, 2017, pp. 438–439) but may also affect communities of colour and other disadvantaged groups disproportionately, fostering mistrust between communities and the police (Babe Howell, 2016; European Roma Rights Centre, 2023; Jackson et al., 2023). Police surveillance and abuses may have a chilling effect on how users enjoy the metaverse and express themselves in this virtual space. Moreover, upholding fundamental rights standards in police conduct is essential for the consequences that irregularities may further have on criminal proceedings in the analogue world. It is part of a general debate on digital sovereignty (Floridi, 2020). Those who commit offenses in the metaverse should eventually bear the consequences of their endeavours in one legal system, for example, by paying fines, serving prison time, or another alternative punishment. Consequently, the prevention and ascertainment of criminal acts in the metaverse must be governed by similar guarantees, for instance, due process considerations such as equality, accountability, and the right to an effective remedy.

Given how policing interferes with individuals' rights, those responsible for this task in the metaverse should comply with the highest standards of independence and impartiality. It is doubtful, however, that platforms and online communities acting alone will meet such requirements, as highlighted by the shortcomings of current content moderation mechanisms. These often lack oversight mechanisms or checks and balances provided by law, meaning that private platforms retain wide latitude on how they handle content (European Commission, 2020, p. 25). Studies have also shown that, when claims about the illegality of content are uncertain, platforms will often remove the information to avoid liability (Riis & Schwemer, 2018, p. 13; Urban et al., 2017, p. 41), suggesting that businesses do not manage content moderation impartially but according to corporate logics (Qiwei et al., 2024). In addition, there is often a lack of transparency and accountability in the decisions taken unilaterally by platforms. For instance, the European Commission's impact assessment on the proposal for the Digital Service Act (DSA) reports that very few online platforms are used to subject their content moderation policies to systematic independent oversight (European Commission, 2020, pp. 18–19). The same document mentions a Eurobarometer survey, in which 17% of respondents declared that online platforms erroneously removed their content but were never informed about the reason for the removal (European Commission, 2020, p. 26).

In the metaverse, replicating these mechanisms could be very damaging for users. While metaverse platforms currently are using primarily human moderation (Gray et al., 2024; Schulenberg et al., 2023), they could use automated technologies to control avatar behaviour rather than content, for example, by pre-emptively blocking their actions whenever a situation of potential danger arises. Additionally, these tools may be tuned to avoid platform liability, thus resulting in overly stringent restrictions on user interactions (we will elaborate on this in Section 5). For this reason, such sensitive decisions should not be entirely delegated to opaque technologies, devised according to platforms' corporate needs.

Similar concerns apply to policing by online communities, which might engage in in-game harassment and bullying (i.e., griefing), phenomena that may disproportionately affect women, LGBTQ+ players, and players of colour in VR platforms (Ajibola, 2022; Beres et al., 2021, p. 1; Centre for Countering Digital Hate, 2021; Crawford & Smith, 2022; Outlaw, 2018). Beyond discrimination, accountability is also an issue in online community policing, which often lacks redress mechanisms for affected users. Empirical research indicates that punishment before community 'game tribunals' (e.g., in *League of Legends*) can be too hasty. Behavioural standards of misbehaviour are unclear, and the mere fact of being reported often leads to a sanction (Ehrett, 2016). The users participating in the sentencing appreciate the flexibility of this process, which, however, raises issues regarding the rights to equality and effective remedy. In *VRChat*, a 'social VR' platform, users organised themselves into a vigilante police department. Though it began as a roleplaying game of questioning and 'arresting' willing avatars, 'officers' have also been accused of planting evidence and harassing users (Ajibola, 2022). Against this background, community policing online appears helpful in addressing minor misconduct but insufficient to protect users from abuse.

The second reason for supporting a different policing scheme in the metaverse stems from observing the limited effectiveness of mechanisms enforced only by private actors. When content moderation depends only on platforms' voluntary actions, detection of illegal content, assistance to victims, and coordination with law enforcement are affected negatively. For example, the European Commission has facilitated the adoption of self-regulatory mechanisms in the EU, but these have shown structural limitations in scope and scalability. Given their voluntary nature, these initiatives were limited to their signatories, and compliance could not be supervised or sanctioned appropriately (European

Commission, 2020, p. 30). The European Commission's impact assessment on the proposal for a Regulation to prevent and combat child sexual abuse also highlights that many service providers have not implemented measures to detect child sexual abuse materials (CSAM) despite their proliferation online (European Commission, 2022, p. 38). Even when platforms undertake similar initiatives, they often do so unsuccessfully. For example, in the past, Twitter (now X) failed in essential enforcement against CSAM by allowing already-flagged images to circulate on the platform (Corse, 2023), while Instagram facilitated a commercial network of CSAM (Horwitz & Blunt, 2023). Voluntary cooperation between private and public actors depends on *ad-hoc* temporary solutions that are rarely effective in addressing child sexual abuse (European Commission, 2022, p. 49). The DSA now foresees obligations for service providers in the EU to detect illegal content online. Still, after its adoption, some large platforms have engaged in legal disputes to escape its application (Goujard, 2024), displaying an unwillingness to bear the administrative costs stemming from this legislation.

As we mentioned at the beginning of this section, law enforcement authorities also struggle to tackle criminal behaviour online. EUROPOL's report on the metaverse mentions that only a few countries have made notable efforts to build a presence on social media, although this work will be very different from policing metaverses (EUROPOL, 2022, pp. 24–25). In this context, officers should not just be approachable as on social media, but proactively intervene, for instance, if a user is in danger. In this regard, some pilot projects have begun experimenting with how the police should act in the metaverse and proto-metaverses. In France, for example, the NGO *Enfant Bleu* partnered with *Fortnite* to launch an undercover police operation that involved over 1,200 children and teenagers who reported personal issues and situations of danger (Agence France-Presse, 2023). While successful, such initiatives are sporadic, time-bound, and insufficient to address crime in immersive environments. In fact, police forces will likely struggle to keep up with the task of online policing, due to the structural lack of knowledge and technical capabilities to inspect complex digital services (European Commission, 2020, p. 22). Moreover, the legal requirements and practical hurdles of police's international cooperation represent an additional concern for future metaverse policing. Currently, cooperation is often limited to high-profile cases and requires burdensome interactions between national authorities (Greenberg, 2022), while in the metaverse, crimes that generally do not trigger such mechanisms (e.g., stalking) will also demand a prompt response by the police.

Both the limitations concerning private-led initiatives and law-enforcement efforts to keep the metaverse safe can be overcome if policing the metaverse is framed as a task for private and public entities acting together in a co-governance regime. While providers and communities may be best placed to detect criminal behaviour on their platforms, law enforcement will need to supervise their actions to check compliance with fundamental rights, be able to intervene directly, and ensure follow-up in the analogue world through international cooperation. Such coordination is necessary because individuals cannot be prosecuted, convicted, or imprisoned in the metaverse, a virtual space where physically coercive acts (e.g., arrests) cannot be performed. Restraining individuals and imposing criminal sanctions will thus remain an exclusive competence of criminal justice authorities in the analogue world. Instead, policing activities that do not require physical force – such as crime prevention, assistance to the public, and surveillance – will be possible, and should be ensured, in the metaverse. These tasks could be performed or facilitated by a dedicated supranational body, structured in the terms outlined in Section 4, ensuring platform compliance and coordinating jurisdictional conflicts when crimes are detected. As argued in Section 2, specific legislation should be enacted to set up this policing mechanism. In the EU, the DSA already provides a legal basis for tackling illegal content online. Still, this legislation would arguably leave out the new forms of criminal behaviour that, as described above, are now made possible by spatial harms. An *ad-hoc* framework is thus necessary to legitimise police action in the metaverse, avoid legal uncertainty for private entities, and foster coordination with public authorities. The new regime will also have to allocate policing efforts among all the actors involved, as an unorganised police presence could cause excessive surveillance or create jurisdictional conflicts between States. The following section explores policy options to organise police cooperation in the metaverse to address these issues.

4. Policing *across* metaverses: Transnational cooperation in the metaverse

Having established the criminal relevance of some metaverse behaviours (Section 2) and the need for a specific mechanism for metaverse policing (Section 3), we now address how this may work in practice. We do so through a LoA that examines how policing efforts should be allocated across multiple metaverses. By reviewing different models of international police cooperation, we explain how a supranational body may perform this task in the metaverse, and how jurisdictional problems can be addressed.

Historically, international police cooperation has been structured according to two models. On the one hand, police forces may engage in bilateral or multilateral agreements on extradition or information sharing. That is the case of INTERPOL and EUROPOL, which do not have authoritative powers but rely on those exercised by national police forces. On the other hand, States may cooperate by establishing a supranational police body, endowed with autonomous powers to arrest and collect evidence. However, because this solution entails a significant waiver of sovereignty, States have been reluctant to pursue this path (Deflem, 2000, pp. 749–750), with limited exceptions. In the EU, for example, the European Anti-Fraud Office (OLAF) conducts administrative investigations on fraud and other crimes against the financial interests of the Union, performing acts like on-the-spot checks and inspections. The European Public Prosecutor Office (EPPO) operates in the same domain and prosecutes individuals before Member States' domestic courts. Both Offices have autonomous and enforceable powers in national jurisdictions, but they mainly act *ex-post,* i.e., after the criminal facts have occurred. At the national level, federal states also implement forms of police cooperation across their federated territories. For example, the United States Federal Bureau of Investigation (FBI) investigates federal crime and performs preventive surveillance and intelligence operations.

Translating these two models to the metaverse, two forms of police cooperation are foreseeable: *intergovernmental coordination* and the creation of a *supranational police body*.

In intergovernmental coordination, national law enforcement agencies (LEAs) and platforms would police the metaverse while being coordinated by a supranational agency like INTERPOL or EUROPOL. Such an entity would facilitate coordination if crimes were detected, ensuring that information is transmitted to the competent analogue-world authorities, but it would not have the power to perform coercive acts. Arguably, this model would be easier to set up at the political level but would not ensure an equal allocation of State efforts, since national LEAs would still perform policing. For the same reason, 'positive' conflicts of jurisdiction may arise between States imposing their competence over the same portion of the metaverse, while 'negative' conflicts would appear when no police force claims jurisdiction over a given space, leaving users unsafe.

Conversely, an optimal—but maybe utopian—solution would be creating a supranational body ('the metaverse police') endowed with autonomous powers to police the metaverse. This entity would be composed of detached officers from national LEAs, following the model of the United Nations Blue Helmets (Cox, 1999). If this seems unorthodox, one should consider that several armies in the world, for example, have reorganised themselves to add a new branch entirely dedicated to defensive and offensive operations in cyberspace, besides the conventional domains of war: land, sea, air, and space. Such a development could also affect law enforcement, thus supporting the creation of a supranational body to address metaverse crimes. This scenario, where a unique entity performs policing, would mitigate jurisdictional issues and ensure an ideal distribution of policing efforts across metaverses.

As explained in Section 3, an *ad-hoc* legal basis would be necessary to set up one of these policing mechanisms. An international treaty, gathering the support of as many States as possible, would be the ideal framework. However, this may not be politically possible in the early phases of metaverse development. Conversely, undertaking this initiative at the macro-regional level, like in the EU, appears more feasible and could still impact many users thanks to the so-called Brussels Effect (Floridi, 2021, p. 217). Besides, the history of the EPPO shows that 'starting small' can be a promising path in this domain: conceived as a form of 'enhanced cooperation' among a restricted group of Member States, the Office now operates in 24 EU countries. Should a similar initiative be taken for the metaverse, the policing mechanism could expand to other States beyond the EU. Currently, the Treaty of the Functioning European Union (TFEU) allows adopting, respectively, measures to strengthen the harmonisation of the internal market (Article 114 TFUE) and police cooperation (Article 87 TFEU). Based on these legal provisions, an EU regulation would be the appropriate framework to create a policing mechanism in the metaverse, establishing common rules for digital platforms and a mechanism of cross-border cooperation between LEAs in the EU.

Nonetheless, enacting an international instrument for police cooperation would not be helpful if the States involved did not have a robust jurisdictional claim over the metaverse platforms involved. As underlined by INTERPOL, a major challenge this new environment presents to law enforcement is determining national jurisdiction (INTERPOL, 2024, p. 20). In fact, the police function has always been tied to the principle of sovereignty, which allows States to exercise public powers within their territories. However, the metaverse is a fully digitised environment where no State can claim territorial sovereignty. Moreover, before criminal acts are committed, determining national jurisdiction over a portion of the metaverse is even more challenging, given that the nationality of the perpetrator and the victim are still unknown. Establishing the competence of a police body in a preventive context, in a fully transnational environment like the metaverse, is thus a relatively new issue for criminal justice. Only the high seas or outer space offer similar examples of non-territorial spaces in the analogue world. However, these do not pose the same crime risks to the average individual as the metaverse. The problem of determining jurisdiction also emerges *ex-post facto*, when multiple States can claim jurisdiction over the same metaverse crimes.

The most appropriate solution for the metaverse should be found in the criteria for establishing State jurisdiction in international law (Oxman, 2007; Schmitt, 2017):

- *Territory*. Each State has jurisdiction over the persons, properties, and activities located within its borders;
- *Nationality* is in the form of both *active* and *passive personality* principles. Under the former, the State applies its rules to its nationals and companies established in its territory, even if the crime occurs abroad. The latter anchors jurisdiction to the nationality of the victim;
- *Residence or domicile*. This implies that States can enforce their norms on subjects who reside or domicile in their territory;

- *Protective principle*. It allows States to claim jurisdiction over activities that occur abroad but encroach on their governmental functions (e.g., counterfeiting their currency);
- *Universal jurisdiction*. It defines the right of a State to prosecute some internationally defined crimes (e.g., genocide), even if committed abroad and by foreigners.

Among these, neither the protective nor the universal criteria seem to adapt to the nature and seriousness of metaverse crimes. The lack of a physical dimension in metaverse behaviours makes it impossible to commit serious international offenses, such as war crimes or crimes against humanity, as defined by the Statute of the International Criminal Court. The protective principle could apply to the counterfeiting of digital currencies or official documents, but the specificity of the object of these offenses makes this criterion challenging to extend on a large scale. Consequently, the nationality and residence/domicile principles will be the most useful in determining state jurisdiction in the metaverse, although they have different relevance in *ex-ante* and *ex-post facto* situations.

In the *ex-ante facto* context, the nationality or location of future suspects and victims is still unknown, so that the metaverse police could be competent under another nationality criterion, such as the place of establishment of the platform concerned. This is a recurrent mechanism in EU legislation applying to digital providers, notably in the General Data Protection Regulation (GDPR).[159] Often, EU law also requires that platforms that are not established in the Union, but provide services to many users, designate a representative in its territory.[160] Under this system, digital platforms would fall under the competence of the metaverse police whenever they are established or operate in a State member of the EU or the international treaty mentioned above.

In an *ex-post facto* situation, jurisdictional criteria identify the competent authorities in the analogue world for investigating, prosecuting, and sentencing metaverse crimes. The most adequate basis for jurisdiction should be chosen to ensure the efficiency of the cooperation mechanism, given that the

[159] Art. 3(1) of the 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) OJ L 119, 4.5.2016, p. 1–88.

[160] Art. 27 GDPR; art. 7 Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, OJ L 191, 28.7.2023, p. 118–180.

metaverse police, since its first intervention, will have to identify which national LEA must be informed of the alleged criminal facts. Considering this, although potentially applicable, the nationality criterion may not be the best solution. Relying on platforms' place of establishment may create a disproportionate workload for some States. At the same time, claiming jurisdiction for the victim's nationality might be controversial,[161] while that of the suspect may not always be useful because the person concerned might be located outside of their State of nationality.

Conversely, a practical solution is to use the residence or domicile criterion. LEAs may not be willing to initiate burdensome surrender procedures if suspects live in remote countries and are suspected of minor offenses (Lemley & Volokh, 2017, pp. 1071–1073). Hence, physical surrender should be avoided to prioritise information exchange between police forces, through the coordination of the metaverse police. A national LEA would thus be informed that someone in their territory has committed an offense in the metaverse, allowing them to take the most appropriate course of action. Still, one must consider that if the State where the suspect is located is not a party to the treaty or the EU – continuing with our example – it may refuse to initiate any criminal proceedings. In this case, other States may claim jurisdiction under the remaining criteria (i.e., nationality of the platform, suspect, or victim), even though they would still need the cooperation of the residence country to inform the suspect of their rights in the proceedings, or ultimately to enforce a sanction.

Therefore, as in the analogue world, the ultimate enforcement of criminal law in the metaverse will rest on the States' goodwill. If cooperation is refused, some crimes committed in the metaverse could be left unpunished in the analogue world, but other instruments would still be available in the metaverse to keep users safe, at least temporarily. In this respect, the following section examines under which conditions the police could intervene online against users engaging in criminal behaviour.

5. Policing *within* a metaverse: Surveillance and arrests

[161] The passive nationality principle has been criticized because it may intrude on the right of another State to prescribe and enforce legislation in its territory or to its nationals, and on the rights of individuals who cannot be expected to know the criminal laws of every State when travelling abroad (Oxman 2007, §34).

In this section, we outline further how metaverse policing should function through the second identified LoA, which aims to determine what powers the police can exercise in the metaverse. As anticipated in Section 3, police efforts online are mainly devoted to detecting and preventing crimes. In the metaverse, the police will first have to carry out general surveillance activities. Occasionally, the police will also have to interact with avatars in real-time to block criminal offenses. In the analogue world, the instrument dedicated to this task is the flagrancy arrest, but its applicability in a virtual environment is doubtful.

To understand if and how the police could exercise these powers, we analyse how privacy norms limit general police surveillance in public and private places of the metaverse, and if the notion of arrest can be translated into immersive environments. While measures like freezing or blocking users cannot be compared to arrests, they have similar fundamental rights implications. Consequently, we identify the basic legal requirements of these virtual measures by looking at the human rights framework for restrictions of liberty and personal security.

For starters, avatars in the metaverse will be able to move around and will have expectations of where they can find the police or be arrested, and when their activities can be monitored also through data collection. As we wrote in the introduction, the distinction between private and public metaverses should not be founded on who owns the platform when it comes to policing, but on how users experience this environment. As individuals feel immersed in the metaverse, they will perceive the distinction between public and private places as in the physical world; that is, looking at the accessibility of a given location and not its ownership regime (Altman & Zube, 1989; Ruppert, 2006). For instance, Seoul has launched a metaverse allowing users to access government services in a virtual replica of the city (De Almeida, 2023; Maresca, 2023). While this metaverse is built as a centralised platform, its spaces and services are freely accessible to everyone, meaning this environment should be considered a public place. Likewise, Meta defines the metaverse as a 'public place' (*Meta Horizon Worlds Frequently Asked Questions*) but this may not apply to every space in the platform. For example, the metaverse may include places that should be considered private, like those created for training and work (e.g., Meta Horizon's Workrooms), or by users to retreat in their bubbles (Falchuk et al., 2018, p. 56). In this perspective, policing in the metaverse must respect the distinction between public and private spaces, as in the physical world, in the terms explained below.

Moreover, policing may be affected by similar limitations as those of the analogue world, meaning that not all surveillance activities will be equally intrusive. While 'beat policing' and other forms of manual observation in the metaverse will be resource-constrained and provide a limited amount of information, real-time acquisition and automated analysis of data will give a more comprehensive picture of users' activities beyond officers' standard capacities of observation (Hine et al., 2024).

These activities will interfere with the right to privacy, which is enshrined in several human rights instruments (Article 12 of the Universal Declaration of Human Rights, UDHR; Article 17 of the International Covenant on Civil and Political Rights, ICCP; Article 8 of the European Convention on Human Rights, ECHR). These provisions protect not only the 'home' strictly speaking, but also business premises, as clarified by international jurisprudence.[162] Moreover, case law generally recognises that individuals may claim some expectations of privacy also in public places,[163] as these serve social and political functions (Cohen, 2013, p. 1927; Habermas, 1991; Regan, 2015). Therefore, police activities should be regulated and supervised in these spaces too.

In the metaverse, the police should be able to access public venues freely and observe avatars' activities 'manually'. However, privacy expectations would require specific safeguards for more intrusive forms of surveillance, like real-time data analysis of user data.[164] Even if the monitoring occurs publicly, such measures should be allowed only for the most serious offenses and require authorisation (or *ex-post* validation) from an independent authority. A similar regime should also apply to policing and surveillance

[162] In the European domain, the leading case is ECtHR, *Niemietz v. Germany*, judgment of 16 December 1992, App. no. 13710/88. At the international level, the concept of 'home' in Article 17 ICCP includes the place where the individual 'carries out his usual occupation', as clarified in the CCPR General Comment no. 16 (1988), §5.

[163] In the US context, see e.g., *Carpenter v. United States*, 585 U.S. (2018). In the European one, see ECtHR, *P.G. and J. H. v. United Kingdom,* judgment of 25 September 2001, App. no. 44787/98, §56; ECtHR, *Peck v. the United Kingdom,* §57; ECtHR, 5 September 2017, *Bărbulescu v. Romania*, App. no. 61496/08, §70; ECtHR, *Boulois v. Luxembourg*, judgment of 3 April 2012, App no. 37575/04, §63; ECtHR, *National Federation of Sportspersons' Associations and Unions (Fnass) and Others v. France*, judgment of 18 January 2018, App. nos. 48151/11 and 77769/13, §151; ECtHR, 17 October 2019, *López Ribalda and Others v. Spain*, App. nos. 1874/13 and 8567/13, §89.

[164] Cf., *mutatis mutandis,* USSC, *United States v. Jones*, p. 3, Sotomayor concurring.

of private metaverse spaces, such as users' private bubbles[165] or those created for work purposes. Specifically, the police would have access to these private venues only in limited circumstances and with previous authorisation by an independent entity, while emergency interventions would be justified only upon a user or platform alert, and if validated *ex-post* by the same authority.

During surveillance, the police may also spot users committing crimes and take the initiative to stop them. Intuitively, these interventions may resemble arrests, but it is unclear whether this is their right legal qualification. Indeed, the etymology of 'arrest' involves the idea of stoppage or staying something ("Arrest"), but in criminal procedural systems, arrests imply an act of material apprehension (Garner, 2014). In proto-metaverses like *Second Life*, the platform simulated arrests by 'freezing' other avatars and programmatically confining them to a jail cell for some time (Leenes, 2008, p. 107). Nonetheless, these temporary bans had minor consequences on the well-being of users, who could always log off for a period to escape the consequences of the block. Nowadays, similar actions are possible in the new versions of the metaverse (Ajibola, 2022), but since these do not entail a forcible seizure of an individual, they cannot qualify as arrests in strict legal terms. We will instead refer to them as 'blocking measures'.

To be clear, the analysis of the legal requirements for these blocking measures does not concern the arrests that may be performed subsequently in the physical world. There is not necessarily correspondence between virtual measures and physical arrests. Nonetheless, as blocking measures will have implications in the analogue world, they should be governed by similar principles, such as fairness and proportionality. In this sense, some illicit actions, such as vulgar behaviour, will not legitimise any kind of arrest and should instead be addressed by game rules (for instance, through temporary bans); some illegal or criminal behaviours may justify only a blocking measure, while more serious ones will also demand a physical arrest. Furthermore, applying a virtual or physical arrest will not necessarily lead to a prison sentence in the analogue world, such as when the accused is eventually acquitted or sanctioned with a fine or other alternative punishment.

---

[165] In the metaverse, private bubbles may refer to users' homes bases or other portions of space, surrounding the avatar, 'walled off' temporarily for personal use (Falchuk et al., 2018, p. 58)

The resemblance between physical arrests and their virtual correspondents should not be underestimated, at least from a fundamental rights perspective. Two reasons support this point. First, if one considers the etymological idea of arrest, blocking measures are also something that stops the perpetrator from interacting normally with the virtual environment. Therefore, even without any physical apprehension, these measures will still have similar psychological and social implications as traditional arrests, also considering that immersiveness will amplify the humiliating and distressful impact for users. Second, as described in Section 2, sudden intrusions on avatars' movements can also have physical consequences for users. Even if they do not entail an actual restriction of liberty, blocking measures can be traumatic for individuals because being frozen could generate cybersickness or aggressive responses from users experiencing a loss of control over their surroundings (Behr et al., 2005, p. 671).

Considering these similarities, the fundamental rights regime for arrests should apply to blocking measures in the metaverse. The basic legal requirements for restrictions to individual liberty, like arrests, are set in human rights treaties that protect the rights to liberty and personal security. Article 3 UDHR and Article 9 ICCP provide that '[n]o one shall be subjected to arbitrary arrest and detention'.[166] Under Articles 9 ICCP and 5 ECHR, arrests must always have a basis in the law, and the individuals apprehended shall be informed promptly of the reasons behind the arrest, be brought within a reasonable timeframe before a court (*habeas corpus*), and have a right to compensation in case of unlawful arrests. Even if the rights of liberty and personal security are often mentioned together in legal sources, they have different scopes. While the right to liberty may be interpreted extensively but remains tied to the physical dimension (Schabas, 2015, p. 226), personal security covers both bodily and mental harm and applies beyond situations of formal deprivation of liberty (Taylor, 2020, p. 246). For example, the Human Rights Committee has applied the right to security of the person in cases involving death threats, harassment, and various forms of intimidation.[167]

---

[166] UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III); UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171. The prohibition of arbitrary detention is also foreseen in Article 5 ECHR, Article 5 CFREU, Article 7 of the American Convention, Article 6 of the African Charter, and Article 14 of the Arab Charter.

[167] *Delgado Páez v Colombia,* Communication No 195/1985 (Application No) UN Doc CCPR/C/39/D/195/1985 [emphasis added]. See also *Gunaratna v Sri Lanka*, no. 1432/2005, UN Doc CCPR/95/D/1432/2005, §8.4; *Chongwe v Zambia*, no.

Given this, the right to liberty would arguably not apply to blocking measures in the metaverse for the lack of material apprehension. However, the right to personal security would still be interfered with for the psychological – and potentially physical – impact on users. In particular, blocking measures may have similar legal effects as non-coercive pre-trial measures, like those that prevent suspects from attending specific venues. Therefore, the procedural safeguards imposed by international treaties should apply to metaverse blocking measures.

For their potential physical impact on users, blocking measures should also respect requirements preventing the risk of abuse by the police. The freedom from torture and cruel, inhuman, or degrading treatment is foreseen in several international human rights instruments (Articles 5 UDHR, 7 ICCP, 3 ECHR). Specifically, the United Nations Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (UNCAT) describes torture as any intentional act by a public official that inflicts severe physical or mental suffering, but its Article 1 excludes from this definition any pain arising only from, inherent in or incidental to lawful sanctions. The distinction between ill-treatment and legal measures such as arrests is a matter of concrete evaluation. According to the European Court of Human Rights, police behaviour amounts to torture or other ill-treatment when it attains a minimum level of severity, which is assessed against the circumstances of the case, such as the nature and context of the treatment, the manner and method of its execution, its duration, its physical or mental effects and, in some instances, the sex, age, and state of health of the victim.[168] Extending this reasoning to the metaverse, blocking measures should not be considered illegal *per se* for their potential consequences on users (i.e., cybersickness). However, States should take precautions to hamper abuses, for instance, limiting their execution to the time strictly necessary to prevent the commission of a serious crime or excluding their application to child users.

In our case, these norms should be integrated into the treaty or the EU Regulation governing the actions of the metaverse police presented in Section 4. Such a framework should establish a legal basis

821/1998, UN Doc. CCPR/C/79/D/821/1998, §5.4; *Dias v Angola*, no. 711/1996, UN Doc. CCPR/C/68/D/711/1996, §8.3; *Jayawardena v Sri Lanka,* no. 916/2000, UN Doc. CCPR/C/675/D/916/2000, §7.2.

[168] ECtHR, 26 October 2000, *Kudła v. Poland,* App. no. 30210/96, §§91 ff.

for blocking measures, define their scope and safeguards, foresee information rights for blocked users, and identify a competent, independent authority to review blocking measures and decide on compensation if necessary.

Drawing on the analysis developed thus far, the following section provides policy recommendations to begin this process.

6. Policy recommendations and conclusions

In this section, we formulate some policy recommendations (PR) for EU regulators, but also for States beyond the EU, should they take the initiative to regulate policing in the metaverse:

PR$_1$: *Regulators should recognise the implications of harmful experiences caused by illicit behaviour in the metaverse and adopt specific legislation to criminalise the conducts that generate the most serious harm.* For instance, dedicated resources should be urgently allocated toward empirical research that systematically investigates the extent, nature, and evolving patterns of criminal activity within the metaverse.

PR$_2$: *The metaverse should be policed through a co-governance mechanism involving private actors and State authorities.* Multiple actors – such as platforms, communities, and LEAs – should act together to police virtual worlds. While providers may be best placed to detect criminal behaviour on their platforms and mitigate harms through code functionalities (like *Horizon Worlds*' 'Safe Zone'), law enforcement will need to supervise their actions, be able to intervene directly, and ensure incidents are followed up on in the analogue world through international cooperation. For instance, the role of communities in policing should be emphasised for addressing minor misconduct, provided that public authorities supervise them. Such a co-governance mechanism should be enacted at the transnational level to ensure that policing efforts are not allocated disproportionally among LEAs or in some areas of the metaverse.

PR$_3$: *Given the pan-jurisdictional nature of the metaverse, policing should be regulated at the international level (or at least at the EU level for EU Member States).* An international treaty is the best option to ensure equal allocation of responsibilities and avoid excessive policing. Alternatively, as far as the EU is concerned, a Regulation may be the appropriate solution. This legal framework should provide:

- minimum elements of metaverse offenses;
- the composition and tasks of the metaverse police (see also **PR$_4$**);
- rules to establish jurisdiction *ex-ante* and *ex-post facto* (see also **PR$_5$**);
- procedural safeguards for police activities (see also **PR$_{6-7}$**);
- platform obligations.

PR$_4$: *States should entrust the policing of the metaverse to a unique supranational body (the metaverse police).* This entity should be endowed with autonomous coercive powers and be composed of national officers of the adhering States. Alternatively, national police forces could be directly involved in policing the metaverse, but a supranational body like EUROPOL or INTERPOL should coordinate them.

PR$_5$: *Regulators should establish specific criteria to solve jurisdictional conflicts in the metaverse.* For crime prevention, digital platforms would fall under the competence of the metaverse police whenever they are established or operate in a State member of the EU, or the international treaty mentioned above (nationality criterion). After the commission of a criminal offense, the residence or domicile criterion will be the most practical solution to identify the competent body to take action in the analogue world. National LEAs would thus be informed that someone in their territory has committed an offense in the metaverse, allowing them to initiate investigations where appropriate.

PR$_6$: *Regulators should distinguish private and public places in the metaverse and regulate police surveillance accordingly.* The police should be able to access public metaverse spaces to observe avatars' interactions 'manually', but gathering data in real-time should be subject to stricter conditions. Private metaverse spaces and the data generated therein should be subject to the same protection as the home in physical spaces. They should be accessed by the police only under prior authorisation by an independent authority.

PR$_7$: *Regulators should protect users' personal security and provide safeguards for metaverse 'arrests' (blocking measures).* Blocking measures cannot be appropriately defined as arrests but have similar fundamental rights implications. While the right to liberty cannot extend to such measures because of the impossibility of material apprehension, their psychological and physical consequences should be covered by the right to personal security and freedom from torture and cruel, inhuman, and degrading treatment.

Before implementing these recommendations, States must decide which illicit behaviours will be criminalised in the immersive environments. Currently, existing laws cannot always extend to crimes committed in the metaverse. Although aggressive virtual behaviours may soon induce physical stimuli in other avatars (Cheong, 2022, p. 16), these sensations would not compare to analogue-world equivalents. Nevertheless, their psychological effects should not be underestimated either. Criminalising behaviours in immersive environments will require creating a metaverse policing system, to which States may choose to adhere. Their decision will be a matter of power and politics. The chance to profit from the metaverse market is a compelling incentive for States (World Economic Forum, 2023a) because social and economic benefits will develop only if users feel safe in this environment. An equal allocation of police responsibilities might be another factor in embracing this system. If States decide not to do so, users will have to realise that some metaverses may be under-policed or not be policed at all, with very different degrees of safety. The legitimacy of metaverse policing will depend not only on enforcement mechanisms, but on shared norms that treat virtual harm as real.

Works Cited

Adejumo, O. (2022, September 12). South Korea sentences metaverse sexual abuser to 4 years imprisonment. *CryptoSlate*. https://cryptoslate.com/south-korea-sentences-metaverse-sexual-abuser-to-4-years-imprisonment/

Agence France-Presse. (2023, September 7). New Fortnite mission: Reaching out to abused children. *Technology Inquirer*. https://technology.inquirer.net/101040/new-fortnite-mission-reaching-out-to-abused-children

Ajibola, O. (2022). The Metaverse Has A Police Department For Arresting People In VR. *Techbooky*.

Altman, I., & Zube, E. H. (Eds.). (1989). *Public places and spaces*. Plenum Press.

Arrest. In *Online Etymology Dictionary*. https://www.etymonline.com/word/arrest

Ashworth, A. (2006). *Principles of Criminal Law*. Oxford University Press.

Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? *Journal of Governance and Regulation*, *6*(1), 45–62. https://doi.org/10.22495/jgr_v6_i1_p5

Australian Associated Press. (2023, December 3). Online gaming platforms such as Roblox used as 'Trojan horse' for extremist recruitment of children, AFP warns. *The Guardian*. https://www.theguardian.com/australia-news/2023/dec/03/online-gaming-platforms-such-as-roblox-used-as-trojan-horse-for-extremist-recruitment-of-children-afp-warns

Babe Howell, K. (2016). The Costs of Broken Windows Policing: Twenty Years and Counting. *Cardozo Law Review*, *37*(3), 1059–1074.

Basu, T. (2021). The metaverse has a groping problem already. *MIT Technology Review*.

Bates, L. (2025, June 10). Misogyny in the metaverse: Is Mark Zuckerberg's dream world a no-go area for women? *The Guardian*. https://www.theguardian.com/society/2025/jun/10/the-misogyny-of-the-metaverse-is-mark-zuckerbergs-dream-world-a-no-go-area-for-women

BBC. (2007, November 14). *"Virtual theft" leads to arrest*. http://news.bbc.co.uk/2/hi/7094764.stm

Behr, K.-M., Nosper, A., Klimmt, C., & Hartmann, T. (2005). Some Practical Considerations of Ethical Issues in VR Research. *Presence: Teleoperators and Virtual Environments*, *14*(6), 668–676. https://doi.org/10.1162/105474605775196535

Beres, N. A., Frommel, J., Reid, E., Mandryk, R. L., & Klarkowski, M. (2021). Don't You Know That You're Toxic: Normalization of Toxicity in Online Gaming. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–15. https://doi.org/10.1145/3411764.3445157

Brenner, S. (2001). Is There Such a Thing as "Virtual Crime"? *California Criminal Law Review*, *4*, 1–72.

Brenner, S. W. (2008). Fantasy Crime: The Role of Criminal Law in Virtual Worlds. *Vanderbilt Journal of Entertainment & Technology Law*, *11*(1).

Cadet, L. B., & Chainay, H. (2020). Memory of virtual experiences: Role of immersion, emotion and sense of presence. *International Journal of Human-Computer Studies*, *144*, 102506. https://doi.org/10.1016/j.ijhcs.2020.102506

Casey, P., Baggili, I., & Yarramreddy, A. (2021). Immersive Virtual Reality Attacks and the Human Joystick. *IEEE Transactions on Dependable and Secure Computing*, *18*(2), 550–562. IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2019.2907942

Centre for Countering Digital Hate. (2021). *New research shows Metaverse is not safe for kids*.

https://counterhate.com/blog/new-research-shows-metaverse-is-not-safe-for-kids/

Centre for Countering Digital Hate. (2023). *Horizon Worlds Exposed.* https://counterhate.com/research/horizon-worlds-exposed/

Cheong, B. C. (2022). Avatars in the metaverse: Potential legal issues and remedies. *International Cybersecurity Law Review*, *3*(2), 467–494. https://doi.org/10.1365/s43439-022-00056-9

Cieslak, M., & Gerken, T. (2023). *Interpol working out how to police the metaverse.* https://www.bbc.com/news/technology-64501726

Cohen, J. (2013). What privacy is for. *Harvard Law Review*, *126*(7), 1904–1933.

Collister, L. B. (2014). Surveillance and Community: Language Policing and Empowerment in a World of Warcraft Guild. *Surveillance & Society*, *12*(3), 337–348. https://doi.org/10.24908/ss.v12i3.4956

Corse, A. (2023, June 5). *Twitter Missed Dozens of Known Images of Child Sexual Abuse Material, Researchers Say*. https://www.wsj.com/articles/twitter-missed-dozens-of-known-images-of-child-sexual-abuse-material-researchers-say-58d44f7b

Cox, K. E. (1999). Beyond Self-Defense: United Nations Peacekeeping Operations & (and) the Use of Force. *Denver Journal of International Law & Policy*, *27*(2), 239–273.

Crawford, A., & Smith, T. (2022). Metaverse app allows kids into virtual strip clubs. *BBC*. https://www.bbc.com/news/technology-60415317?uuid=qFhIDbLg6IVsy6Lp2152

Cummings, J. J., & Bailenson, J. N. (2016). How Immersive Is Enough? A Meta-Analysis of the Effect of Immersive Technology on User Presence. *Media Psychology*, *19*(2), 272–309. https://doi.org/10.1080/15213269.2015.1015740

De Almeida, G. G. F. (2023). Cities and Territorial Brand in The Metaverse: The Metaverse SEOUL Case. *Sustainability*, *15*(13), 10116. https://doi.org/10.3390/su151310116

De Back, T. T., Tinga, A. M., & Louwerse, M. M. (2024). Natural- and redirected walking in virtual reality: Spatial performance and user experience. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-024-19879-1

Deflem, M. (2000). Bureaucratization and Social Control: Historical Foundations of International Police Cooperation. *Law & Society Review*, *34*(3), 739. https://doi.org/10.2307/3115142

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Easterbrook, F. H. (1996). Cyberspace and the Law of the Horse. *THE UNIVERSITY OF CHICAGO LEGAL FORUM*, 207–216.

Ehrett, J. S. (2016). E-judiciaries: A model for community policing in cyberspace. *Information & Communications Technology Law*, *25*(3), 272–291. https://doi.org/10.1080/13600834.2016.1236428

European Commission. (2020). *IMPACT ASSESSMENT Accompanying the document* PROPOSAL FOR *A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.* https://doi.org/10.5040/9781782258674

European Commission. (2022). *Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and the Council laying down rules to prevent and combat child sexual abuse*.

European Commission. (2023). *Virtual Worlds fit for people*. https://digital-strategy.ec.europa.eu/en/policies/virtual-worlds

European Roma Rights Centre. (2023, February 14). *New Research Points to Institutional Racism Against Roma in North Macedonia's Criminal Justice System*. www.errc.org/press-releases/new-research-points-to-institutional-racism-against-roma-in-north-macedonias-criminal-justice-system

EUROPOL. (2022). *Policing in the metaverse: What law enforcement needs to know : an observatory report from the Europol innovation lab*. Publications Office. https://data.europa.eu/doi/10.2813/81062

Falchuk, B., Loeb, S., & Neff, R. (2018). The Social Metaverse: Battle for Privacy. *IEEE Technology and Society Magazine*, *37*(2), 52–61. https://doi.org/10.1109/MTS.2018.2826060

Farrant, T. (2024, January 4). *UK police launch first investigation into virtual rape in metaverse*. Euronews. https://www.euronews.com/next/2024/01/04/british-police-launch-first-investigation-into-virtual-rape-in-metaverse

Floridi, L. (2008). The Method of Levels of Abstraction. *Minds and Machines*, *18*(3), 303–329. https://doi.org/10.1007/s11023-008-9113-7

Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, *33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Floridi, L. (2021). The European Legislation on AI: A Brief Analysis of its Philosophical Approach. *Philosophy & Technology*, *34*(2), 215–222. https://doi.org/10.1007/s13347-021-00460-9

Floridi, L. (2022). Metaverse: A Matter of Experience. *Philosophy & Technology*, *35*(3), 73, s13347-022-00568–6. https://doi.org/10.1007/s13347-022-00568-6

Fortis, S. (2023, November 10). *China declares stealing digital collections like NFTs liable for criminal theft sentence*. Cointelegraph. https://cointelegraph.com/news/china-declares-stealing-digital-collections-like-nfts-liable-for-criminal-theft-sentence

France-Presse, A. (2022, February 10). Russian teenager jailed over 'Minecraft plot to blow up virtual spy HQ.' *The Guardian*. https://www.theguardian.com/world/2022/feb/10/russian-teenager-nikita-uvarov-jailed-over-minecraft-plot-to-blow-up-virtual-spy-hq

Garner, B. A. (2014). Arrest. In *Black's Law Dictionary* (10th edition).

Garon, J. M. (2022). Legal Implications of a Ubiquitous Metaverse and a Web3 Future. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4002551

Gómez-Quintero, J., Johnson, S. D., Borrion, H., & Lundrigan, S. (2024). A scoping study of crime facilitated by the metaverse. *Futures*, *157*, 103338. https://doi.org/10.1016/j.futures.2024.103338

Goujard, C. (2024, February 8). Meta, TikTok take EU to court over online content rulebook. *POLITICO*. https://www.politico.eu/article/tiktok-joins-meta-in-suing-eu-over-online-content-rulebook/

Gray, J. E., Carter, M., & Egliston, B. (2024). Trust and Safety in Social VR: Current Industry Practices. In J. E. Gray, M. Carter, & B. Egliston (Eds.), *Governing Social Virtual Reality: Preparing for the Content, Conduct and Design Challenges of Immersive Social Media* (pp. 61–75). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-61831-4_6

Greenberg, A. (2022, April 7). *Inside the Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site*.

https://www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth/

Gromer, D., Reinke, M., Christner, I., & Pauli, P. (2019). Causal Interactive Links Between Presence and Fear in Virtual Reality Height Exposure. *Frontiers in Psychology*, *10*, 141. https://doi.org/10.3389/fpsyg.2019.00141

Haber, E. (2024). The Criminal Metaverse. *Indiana Law Journal*, *99*(3). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4400281

Habermas, J. (1991). *The Structural Transformation of the Public Sphere* (1st ed.). MIT Press.

Headleand, C. J., Free, J., Farndale, S., & Hall, M. (2020). Virtual Community Support Officers: Community Policing in the Digital Space. *2020 International Conference on Cyberworlds (CW)*, 121–124. https://doi.org/10.1109/CW49994.2020.00025

Hillyard, P., & Tombs, S. (2007). From 'crime' to social harm? *Crime, Law and Social Change*, *48*(1–2), 9–25. https://doi.org/10.1007/s10611-007-9079-z

Hillyard, P., & Tombs, S. (2021). Beyond Criminology? In P. Davies, P. Leighton, & T. Wyatt (Eds.), *The Palgrave Handbook of Social Harm* (pp. 11–36). Springer International Publishing. https://doi.org/10.1007/978-3-030-72408-5_2

Hine, E. (2023). *Content Moderation in the Metaverse Could Be a New Frontier to Attack Freedom of Expression*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4458433

Hine, E., Rezende, I. N., Roberts, H., Wong, D., Taddeo, M., & Floridi, L. (2024). Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations. *Digital Society*, *3*(2), 33. https://doi.org/10.1007/s44206-024-00114-1

Horwitz, J., & Blunt, K. (2023, June 7). Instagram Connects Vast Pedophile Network. *The Wall Street Journal*. https://www.wsj.com/articles/instagram-vast-pedophile-network-4ab7189

INTERPOL. (2024). *Metaverse: A law enforcerment perspective*.

Jackson, J., McKay, T., Cheliotis, L., Bradford, B., Fine, A., & Trinkner, R. (2023). Centering Race in Procedural Justice Theory: Structural Racism and the Under- and Overpolicing of Black Communities. *Law and Human Behaviour*, *47*(1), 68–82.

Keiler, J., & Roef, D. (2019). Principles of Criminalization and the Limits of Criminal Law. In *Comparative Concepts of Criminal Law* (3rd ed., pp. 35–83). Intersentia.

Knight, W. (2005, August 8). *Computer characters mugged in virtual crime spree*. New Scientist. https://web.archive.org/web/20231108210055/https://www.newscientist.com/article/dn7865-computer-characters-mugged-in-virtual-crime-spree/

Laue, C. (2011). Crime Potential of Metaverses. In K. Cornelius & D. Hermann (Eds.), *Virtual Worlds and Criminality* (pp. 19–29). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-20823-2_2

Leenes, R. (2008). Privacy in the Metaverse. In S. Fischer-Hübner, P. Duquenoy, A. Zuccato, & L. Martucci (Eds.), *The Future of Identity in the Information Society* (pp. 95–112). Springer US. https://doi.org/10.1007/978-0-387-79026-8_7

Lemley, M. A., & Volokh, E. (2017). Law, Virtual Reality, and Augmented Reality. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2933867

Lessig, L. (1999). The Law of the Horse: What Cyberlaw Might Teach. *Harvard Law Review*, *113*(2), 501. https://doi.org/10.2307/1342331

Mackenzie, S. (2022). Criminology Towards the Metaverse: Cryptocurrency Scams, Grey Economy and the Technosocial. *The British Journal of Criminology*, *62*(6), 1537–1552. https://doi.org/10.1093/bjc/azab118

Madiega, T., Car, P., Niestadt, Maria, & Van de Pol, L. (2022, June). *Metaverse: Opportunities, risks and policy implications*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf

Makransky, G., & Mayer, R. E. (2022). Benefits of Taking a Virtual Field Trip in Immersive Virtual Reality: Evidence for the Immersion Principle in Multimedia Learning. *Educational Psychology Review*, *34*(3), 1771–1798. https://doi.org/10.1007/s10648-022-09675-4

Maresca, T. (2023, January 16). Seoul launches ambitious metaverse platform for city services, tourism. *UPI*. https://www.upi.com/Top_News/World-News/2023/01/16/Seoul-Metaverse-virtual-platform-launched/6531673859297/

Martens, M. A., Antley, A., Freeman, D., Slater, M., Harrison, P. J., & Tunbridge, E. M. (2019). It feels real: Physiological responses to a stressful virtual reality environment and its impact on working memory. *Journal of Psychopharmacology (Oxford, England)*, *33*(10), 1264–1273. https://doi.org/10.1177/0269881119860156

Marthews, A., & Tucker, C. (2017). The Impact of Online Surveillance on Behavior. In D. Gray & S. E. Henderson (Eds.), *The Cambridge Handbook of Surveillance Law* (1st ed., pp. 437–454). Cambridge University Press. https://doi.org/10.1017/9781316481127.019

Meta. (2024). *Moderators and Community Guides in Meta Horizon Worlds*. https://www.meta.com/help/quest/articles/horizon/safety-and-privacy-in-horizon-worlds/community-guides-in-horizon/

Meta Horizon Worlds Frequently Asked Questions | Quest help | Meta Store. (n.d.). Retrieved January 28, 2025, from https://www.meta.com/en-gb/help/quest/articles/horizon/explore-horizon-worlds/horizon-frequently-asked-questions/

Michalowski, R. J. (2016). What is Crime? *Critical Criminology*, *24*(2), 181–199. https://doi.org/10.1007/s10612-015-9303-6

Milgram, P., & Kishino, F. (1994). A TAXONOMY OF MIXED REALITY VISUAL DISPLAYS. *IEICE Transactions on Information Systems*, *E77-D*(12).

Murray, C. D., & Sixsmith, J. (1999). The Corporeal Body in Virtual Reality. *Ethos*, *27*(3), 315–343.

Mütterlein, J. (2018). The Three Pillars of Virtual Reality? Investigating the Roles of Immersion, Presence, and Interactivity. *Proceedings of the 51st Hawaii International Conference on System Sciences*, 1407–1415. http://hdl.handle.net/10125/50061

Nabben, K. (2021). Building the Metaverse: 'Crypto States' and Corporates Compete, Down to the Hardware. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3981345

Nichols, S. (2022). *Metaverse rollout brings new security risks, challenges | TechTarget*. TechTarget. https://www.techtarget.com/searchsecurity/news/252513072/Metaverse-rollout-brings-new-security-risks-challenges

Oppenheim, M. (2022, February 3). Woman reveals 'nightmare' of being 'gang raped' in virtual reality. *The Independent*. https://www.independent.co.uk/news/uk/home-news/metaverse-gang-rape-virtual-world-b2005959.html

Outlaw, J. (2018, April 4). Virtual Harassment: The Social Experience of 600+ Regular Virtual Reality (VR) Users. *VirtualRealityPop*. https://virtualrealitypop.com/virtual-harassment-the-social-experience-of-600-regular-virtual-reality-vr-users-23b1b4ef884e

Oxman, B. H. (2007). Jurisdiction of States. In *Max Planck Encyclopedia of Public International Law*. Oxford University Press.

Pemberton, S. (2007). Social harm future(s): Exploring the potential of the social harm approach. *Crime, Law and Social Change*, *48*(1–2), 27–41. https://doi.org/10.1007/s10611-007-9078-0

Qin, H. X., Wang, Y., & Hui, P. (2025). Identity, crimes, and law enforcement in the Metaverse. *Humanities and Social Sciences Communications*, *12*(1), 194. https://doi.org/10.1057/s41599-024-04266-w

Qiwei, L., Zhang, S., Kasper, A. T., Ashkinaze, J., Eaton, A. A., Schoenebeck, S., & Gilbert, E. (2024). *Reporting Non-Consensual Intimate Media: An Audit Study of Deepfakes* (arXiv:2409.12138). arXiv. https://doi.org/10.48550/arXiv.2409.12138

Regan, P. M. (2015). Privacy and the common good: Revisited. In B. Roessler & D. Mokrosinska (Eds.), *Social Dimensions of Privacy* (1st ed., pp. 50–70). Cambridge University Press. https://doi.org/10.1017/CBO9781107280557.004

Riis, T., & Schwemer, S. F. (2018). Leaving the European Safe Harbor, Sailing Towards Algorithmic Content Regulation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3300159

Robinson, C. D., & Scaglion, R. (1987). The Origin and Evolution of the Police Function in Society: Notes toward a Theory. *Law & Society Review*, *21*(1), 109. https://doi.org/10.2307/3053387

Ruppert, E. S. (2006). Rights to Public Space: Regulatory Reconfigurations of Liberty. *Urban Geography*, *27*(3), 271–292. https://doi.org/10.2747/0272-3638.27.3.271

Sales, N. J. (2024). A girl was allegedly raped in the metaverse. Is this the beginning of a dark new future? *The Guardian*.

Santana, C., & Albareda, L. (2022). Blockchain and the emergence of Decentralized Autonomous Organizations (DAOs): An integrative model and research agenda. *Technological Forecasting and Social Change*, *182*, 121806. https://doi.org/10.1016/j.techfore.2022.121806

Schabas, W. (2015). *European Convention on human rights: A commentary* (1st ed.). Oxford University Press.

Schmitt, M. N. (Ed.). (2017). Jurisdiction. In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed., pp. 51–78). Cambridge University Press. https://doi.org/10.1017/9781316822524.009

Schulenberg, K., Li, L., Freeman, G., Zamanifard, S., & McNeese, N. J. (2023). Towards Leveraging AI-based Moderation to Address Emergent Harassment in Social Virtual Reality. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–17. https://doi.org/10.1145/3544548.3581090

Sethi, A. (2022). *Security and Privacy in Metaverse: Issues, Challenges, and Future Opportunities. 2.*

Singapore Ministry of Home Affairs. (2023, February 21). *Issuance of Orders Under the Internal Security Act Against Two Self-Radicalised Singaporean Youths*. Ministry of Home Affairs. http://www.mha.gov.sg/mediaroom/press-releases/issuance-of-orders-under-the-internal-security-act-against-two-self-radicalised-singaporean-youths/

Stevenson, A. (Ed.). (2010). *Oxford dictionary of English* (3rd ed). Oxford University Press.

SumOfUs. (2022). *Metaverse: Another cesspool of toxic content*. https://www.eko.org/images/Metaverse_report_May_2022.pdf

Taylor, P. M. (2020). *A Commentary on the International Covenant on Civil and Political Rights: The UN Human Rights Committee's Monitoring of ICCPR Rights* (1st ed.). Cambridge University Press.

https://doi.org/10.1017/9781108689458

Toolkit: Cross-Border Content Moderation. (2021). Internet & Jurisdiction Policy Network. www.internetjurisdiction.net/content/toolkit

Tseng, W.-J., Bonnail, E., McGill, M., Khamis, M., Lecolinet, E., Huron, S., & Gugenheimer, J. (2022). The Dark Side of Perceptual Manipulations in Virtual Reality. *CHI Conference on Human Factors in Computing Systems*, 1–15. https://doi.org/10.1145/3491102.3517728

Urban, J. M., Karaganis, J., & Schofield, B. L. (2017). *NOTICE AND TAKEDOWN IN EVERYDAY PRACTICE*. Berkeley Law.

Wang, H. (2023). How to deal with virtual property crime: Judicial dilemma and a theoretical solution from China. *Computer Law & Security Review*, *49*, 105808. https://doi.org/10.1016/j.clsr.2023.105808

Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys & Tutorials*, 1–1. https://doi.org/10.1109/COMST.2022.3202047

World Economic Forum. (2023a). *Metaverse: What are the economic benefits? | World Economic Forum*. https://www.weforum.org/agenda/2023/06/what-will-be-the-economic-benefits-of-the-metaverse/

World Economic Forum, J. U. (2023b). *Metaverse Privacy and Safety*.

Zallio, M., & Clarkson, P. J. (2022). Designing the metaverse: A study on inclusion, diversity, equity, accessibility and safety for digital immersive environments. *Telematics and Informatics*, *75*, 101909. https://doi.org/10.1016/j.tele.2022.101909