Digital Society (2024) 3:33
https://doi.org/10.1007/s44206-024-00114-1

ORIGINAL PAPER

Safety and Privacy in Immersive Extended Reality: An Analysis and Policy Recommendations

Emmie Hine[1] · Isadora Neroni Rezende[1] · Huw Roberts[2] · David Wong[3] · Mariarosaria Taddeo[2,5] · Luciano Floridi[4,1]

Received: 28 September 2023 / Accepted: 14 May 2024

Abstract

Extended reality (XR) technologies have experienced cycles of development—"summers" and "winters"—for decades, but their overall trajectory is one of increasing uptake. In recent years, immersive extended reality (IXR) applications, a kind of XR that encompasses immersive virtual reality (VR) and augmented reality (AR) environments, have become especially prevalent. The European Union (EU) is exploring regulating this type of technology, and this article seeks to support this endeavor. It outlines safety and privacy harms associated with IXR, analyzes to what extent the existing EU framework for digital governance—including the General Data Protection Regulation, Product Safety Legislation, ePrivacy Directive, Digital Markets Act, Digital Services Act, and AI Act—addresses these harms, and offers some recommendations to EU legislators on how to fill regulatory gaps and improve current approaches to the governance of IXR.

Keywords Digital ethics · Extended reality · Virtual reality · Metaverse · Governance · EU law

✉ Emmie Hine
emma.hine@studio.unibo.it

[1] Department of Legal Studies, University of Bologna, Via Zamboni, 27/29, Bologna 40121, Italy

[2] Oxford Internet Institute, University of Oxford, 1. St. Giles', Oxford OX1 3JS, UK

[3] Yale Law School, Yale University, 127 Wall St., New Haven, CT 06520, USA

[4] Digital Ethics Center, Yale University, 85 Trumbull St., New Haven, CT 06511, USA

[5] The Alan Turing Institute, British Library, 96 Euston Rd, London NW1 2DB, UK

Published online: 03 July 2024

1 Introduction

Emerging technologies often experience cycles of "summer" and "winter." 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, 2020). Extended reality (XR) recently experienced a very hot summer, 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 (Lü, 2023; Miller, 2023; Thorbecke, 2023; Whelan & Flint, 2023). However, XR technologies promise new, different, and better experiences across many domains (Floridi, 2022), and development continues. Regardless of market conditions, XR technologies significantly threaten fundamental rights. The current lull in hype provides a time window to assess risks and consider early regulation. In this article, we intend to aid ongoing regulatory efforts by analyzing risks to *safety* and *privacy* posed by a subset of emerging XR technologies—immersive extended reality (IXR), which encompasses immersive VR and MR environments—and by formulating some policy recommendations addressed to European Union (EU) legislators on how to regulate these technologies effectively. This objective requires three clarifications.

First, we 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, 2020). This approach mitigates the risk that regulation would quickly become outdated. It informs our broad focus on aspects of extended reality, rather than specific XR technologies. 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) (Milgram & Kishino, 1994). Within this spectrum, IXR includes experiences such as social "metaverse" platforms, VR games, and work environments, but excludes non-immersive experiences such as "desktop" VR. It also comprises aspects of MR/AR where users are "immersed" in a context wholly mediated by a device, such as using glasses that overlay information onto the user's field of vision.[1] The term IXR goes beyond the EU's definition of "virtual worlds" as "persistent, immersive environments," which covers non-persistent and AR contexts (European Commission, 2023), to include also standalone spaces, such as virtual offices. However, it excludes applications such as the overlay of information on television sports broadcasts or smartphone AR, as these only mediate part of a user's world and thus are not immersive. Inevitably, many of our policy recommendations will also apply to other XR applications, including non-immersive social metaverse platforms. 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 paper overbroad. We focus on immersive technologies because they pose novel threats to funda-

[1] We use "IXR" as a generic term throughout or when referring to concerns across IXR, and "VR" or "AR" when referring to aspects of those specific areas.

mental rights, 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.

Second, many issues in IXR governance demand attention, like competition, liabilities, financial transactions, cybersecurity, health, accessibility, and inclusiveness (Madiega et al., 2022). Here, we focus exclusively on safety and privacy because they are among the most critical aspects implicating the protection of fundamental rights and the quality of experiences in IXR and must be addressed early. 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 addressed now. The importance of safety and privacy is reflected in several EU policy documents that foreground these rights, as well as the Charter of Fundamental Rights of the European Union ("the Charter") and the European Convention on Human Rights (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.[2] 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, 2023).

Third, although we provide recommendations to EU policymakers, our map of safety and privacy risks and some of our recommendations may also apply to other jurisdictions. Because IXR is a global and pan-jurisdictional phenomenon, we hope this article will contribute to a more extensive discussion of how safety and privacy protections can be harmonized in other contexts. Still, we address this article 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 (AI 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, 2023). 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,

[2] *European Declaration on Digital Rights and Principles for the Digital Decade OJ C 23, 23.1.2023, pp. 1–7.*

2023) and the European Commission Joint Research Centre published a report on the challenges of "next generation virtual worlds" (Hupont et al., 2023).

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.[3] 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 we hope that IXR companies anticipating our 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, 2011) and avoid potentially disruptive adaptations when legislation is passed.

Let us turn now to the structure of the article. Section 2 explains our methodological approach. Section 3 outlines the theoretical conception of safety and privacy grounding the rest of the article. Sections 4 and 5 use historical VR literature and the most recent wave of XR research to discuss safety and privacy risks in IXR. Section 6 discusses how some extant EU legislation succeeds or fails in mitigating those threats. Section 7 outlines our recommendations to legislators; Section 8 concludes the article.

2 Methodology

This article aims to map the landscape of XR risks to inform policymakers, rather than comprehensively classifying or ranking the likelihood of all possible risks. To achieve this, we employ an iterative narrative literature review (Jahan et al., 2016). The initial search phase 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

We read the titles and abstracts of returned articles and filtered them for relevance based on whether they substantively discussed privacy or safety related to IXR. Our inclusion criteria for risks are those that have manifested in the physical world or existing Internet and are technologically plausible considering the current technolog-

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

ical trajectory of IXR, as well as novel risks that are technologically plausible. 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 paper. Where appropriate, additional articles and documents were added ad hoc to provide further context to the examples identified in the literature search.

3 Conceptualizing Safety and Privacy

Safety has been a concern since the early days of VR development, when studies focused mainly on the physical effects of VR. This made sense when headsets weighed four kilograms and often caused severe discomfort (Costello, 1997; Wilson, 1996). Now, additional risks are emerging regarding mental safety and social stability. We use a three-part definition of "safety" encompassing physical, mental, and social elements, which is informed by the EU's conceptualization of the term.[4] 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,[5] 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; proposed updates to the Product Liability Directive would allow individuals to claim damages for psychological harm (De Luca, 2023). The Digital Services Act (DSA)[6] 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 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.

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

[5] *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* OB L 210, 7.8.1985, pp. 29.

[6] *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)* OJ L 277, 27.10.2022, pp. 1–102.

In digital contexts, privacy (enshrined as a fundamental right in 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 (who coined the term "virtual reality") 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 & 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 (Abraham et al., 2022; Bagheri, 2017; Bavana, 2021; Falchuk et al., 2018; Huang et al., 2022; Martin, 2022; Sethi, 2022; Spiegel, 2018). We 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)[7] offers a framework for data protection. However, privacy concerns in IXR extend beyond data protection. Thus, we 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, which 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 our taxonomy while hewing close to the EU context.

[7] *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, pp. 1–88.

4 Threats to Safety

In this section, we outline the main threats to safety posed by IXR as identified by our narrative literature review. We consider amplifications of existing harms and those novel and unique to IXR.

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. We 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 (Stephen 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 & 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 & Rodriguez, 2022). IXR devices also often contain electronics close to users' heads, which could cause serious bodily injury or brain damage if malfunctional (Bagheri, 2017), although product safety standards seem to have prevented this so far.

Intentional physical harm may follow if devices are hacked to cause malfunction (Yuntao 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[8] (Lemley & Volokh, 2018). Hacking is already illegal according to laws implemented under Directive 2013/40/EU,[9] but these malicious user actions are an additional avenue in technology-facilitated physical assault.

[8] In the US, an author with epilepsy was targeted with a strobing GIF on Twitter 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).

[9] *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* OJ L 2018, 14.8.2013, p. 8–14.

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. We 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 we 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 & 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[10]—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 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 & Joseff, 2022).

The subsequent three concerns are more speculative, but grounded in plausibility. IXR offers a new avenue for cyberstalking (Canbay et al., 2022; Falchuk et al., 2018; Sethi, 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

[10] Some 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.

al., 2018) and other kinds of phishing.[11] Avatar identity theft could enable impersonation and fraud (Yuntao et al., 2022), but also inflict emotional trauma if users identify with their avatars (Michael & Metzinger, 2016).

Concerningly, deepfake avatars or characters in immersive experiences may be used as "non-consensual virtual sexbots" (Kalpokas & 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 (ibid., 105). Exploiting "body-to-avatar rendering data"—or simply clever design—could create deepfake avatars for an even more violating kind of revenge pornography (ibid., 100). 98% of all deepfake videos online are nonconsensual pornography, 99% of which is 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.

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 (Jacob et al., 2017; Turner & Lefevre, 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 (Ghiță & 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

[11] 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.

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 & 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"[12] and depersonalization and derealization dissociative disorders are associated with 2D gaming (De Pasquale et al., 2018; WHO Team, 2020) 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 (Michael & Metzinger, 2016; Spiegel, 2018). 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 (Michael & 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 & 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 & 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).[13] Future research should investigate whether IXR could lead to harmful, parasocial relationships and how that could affect

[12] 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).

[13] 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 psychological implications of human-AI relationships should be studied (Kalpokas & Kalpokienė, 2023, 66).

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., 2023), informed consent cannot be obtained via a clause buried deep in the terms of service (Koops, 2014), which would significantly violate user autonomy.

4.3 Threats to Social Stability

Threats to social stability can be split into several categories: threats to social order, security, and democracy. Though further study is required, 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 it 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 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 (Doctor et al., 2022; O'Brolcháin et al., 2016), training (Yuntao et al., 2022), and indoctrination (Michael & 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 have 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 & John 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 even what AI-powered avatars ("Artificial Avatars") you encounter, whether in a virtual context or augmenting the physical world. These interactions could be continuously adjusted based on the users' micro-reactions, offering a potent tool of persuasion (Rosenberg, 2022b). 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.

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 vulnerable 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 Sect. 7.

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, we 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.

5.1 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, 138–139). 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 we 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 & Schroeder, 2023). 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 & Kalpokienė, 2023, 21–22). Biometric data can be aggregated to create an individual "kinematic fingerprint" (Spiegel, 2018). While much of these data are generally considered non-identifiable, as Schroeder (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.

Besides revealing an individual's identity, biometric data and other XR data can infer sensitive or protected characteristics (Abraham et al., 2022; Bagheri, 2017), 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 (Logan, 2018; Rupp & Wallen, 2007), 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).[14] This empirical evidence shows that individuals need to be aware of 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 IXR 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 & 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).

[14] Issues related to biometric data straddle the line between informational and decisional privacy, but we 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.

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 & 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.

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, 2022b). 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 & Gebru, 2018), and thus they may have worse outcomes in these assessments (Pahi & Schroeder, 2023). 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.

5.3 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 lack of such spaces

could render the entire IXR 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 & Schroeder, 2023).[15] Just as inferences can be made about individuals based on their online data footprints (Wachter & 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 by 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.

5.4 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 physical and virtual worlds, and our recommendations for addressing them are in Sect. 7.

6 Applicability of Current EU Legislation

Existing EU legislation may mitigate some of the safety and privacy concerns outlined above. We consider the applicability to IXR of six areas of relevant legislation. While other areas of sectoral legislation may apply to specific IXR applications, we focus here on more broadly pertinent legislation based on our analysis of the specific risks inherent to IXR. In the field of consumer protection, we primarily examine the

[15] 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).

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 (Maciejewski, 2023; Madiega et al., 2022); future work should investigate whether and how they may be implicated.

6.1 Product Safety Legislation

Existing and new product safety legislation will apply to IXR equipment, like headsets. The General Product Safety Directive[16] ensures that products placed on the market are safe and traceable and that consumers are informed of associated risks. A 2021 revision, set to take effect in 2024, updates the Directive to address sales in online marketplaces and the product safety challenges of new technologies, requiring actors to consider the cybersecurity requirements and learning abilities of products when assessing their safety.[17] The Directive notes that "the development of new technologies might bring new health risks to consumers, such as psychological risk, development risks, in particular for children, mental risks, depression, loss of sleep, or altered brain function" (Recital 21), meaning that the Directive could be interpreted to address the physical, mental, and even some social safety impacts of IXR technology. The 2022 Network and Information Security Directive 2 (NIS 2 Directive) will support this.[18] When implemented, the NIS 2 Directive will require Member States to include cybersecurity training in their national cybersecurity strategy (Article 7(2)(f)). "Essential 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 upcoming legislation, a proposal[19] to revise the 1985 Product Liability Directive would protect user safety by addressing liability for software (including AI systems) and digital services, including those provided by online platforms. Although currently untested, it would allow individuals to claim damages not just for physical injury, but also for "medically [recognized] harm to psychological health,"

[16] *Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on General Product Safety (Text with EEA Relevance)* OJ L 11, 15.1.2002, pp. 4–17.

[17] *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)* OJ L 135, 23.5.2023, pp. 1–51.

[18] *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)* OJ L 333, 27.12.2022, pp. 80–150.

[19] *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Liability for Defective Products*, 28.9.2022.

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 would eliminate the €500 threshold for claimable property damage, it would not provide a remedy for social harms or damages to mental health that do not rise to the threshold of "medically recognized." Another piece of relevant upcoming legislation is the AI Liability Directive.[20] This Directive would protect 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 also create 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 will ensure that individuals are not harmed further by data exclusion that would impede their case and enable just outcomes when safety has been violated. However, the "information gap" must be addressed so that individuals actually know when they have been harmed by an automated system (Ziosi, 2023).

6.2 ePrivacy Directive

IXR equipment may qualify as "terminal equipment" under the Privacy and Electronic Communications Directive[21] (ePrivacy Directive) because it connects to the Internet (Vale & Berrick, 2023). These 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 they leave the device. In this case, data could be transmitted to another entity for non-essential (i.e., commercial) purposes, although this is a questionable practice.

These 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.[22] Fighting other serious crimes only justifies retaining

[20] *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*), 28.9.2022.

[21] *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, pp. 37.

[22] 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.

data with a specific link to public security threats.[23] 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,[24] especially considering the aforementioned possibility of using IXR to facilitate terrorism.

The proposal for an ePrivacy Regulation[25] would expand 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, 2022). 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 negotiations are currently deadlocked (Bertuzzi, 2023).

6.3 General Data Protection Regulation

It is unclear how effectively the GDPR will apply to IXR. The GDPR deals with "personal data," defined as "any information relating to an identified or identifiable natural person" (Article 4(1)). 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 for

[23] Id., §144.

[24] 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.

[25] *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)*, 10.1.2017.

such,[26] prompting Meta to shift to the "legitimate interests" clause. However, TikTok was warned that its "legitimate interests" were not sufficient to justify processing for targeted advertising (Lomas, 2023). If it does end up being used, however, the "legitimate interests" basis requires users to be able to opt out of the processing (Bryant, 2023), providing additional protection to users should it be implemented effectively. Although seemingly a highly legitimate justification for processing, issues have emerged with the GDPR's consent regime, with consent dialogues often using deceptive presentation of information and fatiguing users with their quantity (Utz et al., 2019). Thus, even when presented with an ostensibly valid consent choice, users could end up consenting to more or different data collection than they intended to.

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 biometric data can be aggregated to uniquely identify a person, so this article likely applies. It could protect bystanders from having their data collected and used to create "shadow profiles," but this should 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 & 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 an invasion of privacy.

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

[26] 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).

and NFTs, because although transaction data may qualify as personal data, the digital items themselves likely would not.

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*,[27] 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) (Maynard et al., 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 promising 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,[28] which ruled that using proctoring software to monitor students via browser, camera, and facial analysis violated their privacy rights. This holds 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.

6.4 Digital Services Act

The DSA, which entered into force in November of 2022, will impact how IXR platforms deal with illegal content and targeted advertisements. 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"),[29] terrorist content must be removed within one hour. However, due to the pan-jurisdictional nature of

[27] Judgement of 1 August 2022, OT v Vyriausioji tarnybinės etikos komisija (2022).

[28] Deliberação/2021/622 (2021).

[29] *Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online* OJ L 172, 17.5.2021, pp. 79–109.

IXR, determining the audience for which content must be removed could be difficult (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 the advertiser and sponsor in real time and show 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. However, if implemented effectively, Article 26, combined with the requirement that "very large online platforms" (VLOPs) and search engines 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,[30] 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.

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. 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.

6.5 Digital Markets Act

The Digital Markets Act (DMA)[31] also went into effect in November of 2022, with full compliance expected as of March 2024 ("Digital Markets Act", 2022). It is intended to manage the power of entrenched, large online "gatekeepers" that provide "core platform services" such as social networks, search engines, operating systems, web browsers, and online advertising (Article 2). In terms of user privacy, 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,

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

[31] *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)* OJ L 265, 12.10.2022, pp. 1–66.

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.

Other provisions prevent IXR platforms from prioritizing their own events over those of creators on the platform (which Horizon Worlds users report Meta is currently doing (Peters, 2023)). There are also messaging, software, and hardware interoperability requirements (Articles 6–7), and IXR hardware providers will have to allow third-party app stores on their devices (Article 6(4)). However, as these issues are not directly relevant to user safety and privacy, we leave their fuller exploration to future work.

6.6 Artificial Intelligence Act

The AI Act will impact how AI systems can be used in IXR since the definition of an "AI system" includes those that influence "virtual environments" (Article 3). According to the final text,[32] platforms will be obligated to notify users when they are interacting with AI systems (including Artificial Avatars (Petrányi et al., 2023)), and synthetic content must be labeled in machine-readable format and disclosed (Article 50(2), (4)), which could reduce deception and manipulation. Notification requirements also apply to emotion recognition and biometric categorization systems (Article 50(3)), which is beneficial for transparency but would not address the potential exploitative purposes of those systems. Furthermore, this would not apply to systems "permitted by law to detect, prevent, investigate, and prosecute criminal offences" (Article 50(3)), which opens a potential loophole for platforms working with law enforcement.

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, biometric identification could still be done in virtual environments with similar effects. However, other clauses may offer more 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, profiling individuals based on biometric data to infer protected characteristics will be banned, which could limit profiling using IXR biometric data, although it does not apply to "lawfully acquired biometric datasets" in law enforcement (Article 5(1)(g)). 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)), raising the question of what kinds of systems will actually be banned. Recital 16

[32] *European Parliament Legislative Resolution of 13 March 2024 on the Proposal for a Regulation of the European Parliament and of the Council on Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts* (COM(2021)0206–C9-0146/2021– 2021/0106(COD)).

sheds some light on the issue, saying that the AI Act is not concerned with "biometric categorization systems that are a purely ancillary feature intrinsically linked to another commercial service, meaning that the feature cannot, for objective technical reasons, be used without the principal service." This would include filters that categorize facial or body features on online marketplaces by allowing consumers to preview the display of the product on themselves and make purchase decisions, or filters used on online social network services that categorize facial or body features to allow users to add or modify pictures or videos, which may thus include categorization to enable AR features.

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 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.

In the next section, we make recommendations to EU legislators to address some of the regulatory gaps noted and to anticipate future challenges posed by IXR.

7 Recommendations to the EU Legislator

This section details our 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, we 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. Within each area of safety or privacy, recommendations for new policies are first, followed by proposals to modify current legislation, and finally regulatory and non-legislative recommendations.

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.
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, 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. This threshold time should be further studied. Every 30 min, 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, although Meta lowered the minimum age for its Quest headsets to 10 years old (Duffy, 2023), but regardless, age minimums are 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[33] for access to age-restricted content ("Access Age-Restricted Content & Features," 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

[33] *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) (Codified Version) (Text with EEA Relevance)* OJ L 95, 15.4.2010, pp. 1–24.

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) 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 ("Face ID & Privacy," 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[34] 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. We 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.
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

[34] *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, 2.12.2016.

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. Under EU data protection law, competent authorities 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. The EDPB should clarify what dark patterns look like in IXR, and a mechanism for reporting them should be established.

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.

8 Conclusion

IXR offers great potential to augment the physical world and open up new experiences, but its accompanying risks must be addressed. In this article, we have outlined the risks to safety and privacy in IXR and offered policy suggestions for EU legislators. Some of these risks already exist in the physical or digital worlds, but IXR could exacerbate them, while others are novel. Many will disproportionately impact marginalized and disabled users, who should receive particular consideration. We do not presume to have covered all risks, but we hope our proposed policies may provide a flexible basis to address emergent risks.

Governance of IXR will require harmonization because it involves companies and users from across the globe. 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" (Michael & Metzinger, 2016); the rights to experiential authenticity, emotional privacy, and behavioral privacy (Rosenberg, 2022a); "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). Some have instead suggested 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. Regardless of the ultimate approach, some tensions are inevitable when contemplating how to safeguard fundamental rights, such as trade-offs between safety and freedom of expression or privacy. Good regulation will have to carefully consider how to balance conflicting rights. We hope this work will support global, cross-sectoral discussions, in industry, academia, government, civil society, and other sectors. Our new extended reality depends on it.

Acknowledgements The authors would like to thank Patrick Grady and two other individuals for commenting on a previous version of the paper.

Author Contributions E.H. and L.F. conceptualized the article. E.H. prepared the first draft of the manuscript. All authors contributed to subsequent versions of the manuscript, and all authors read and approved the final manuscript.

Funding The authors have no relevant financial or non-financial interests to disclose.
Open access funding provided by Alma Mater Studiorum - Università di Bologna within the CRUI-CARE Agreement.

Data Availability Not applicable.

Declarations

Ethical Approval Not applicable.

Consent Not applicable.

Competing Interests The authors have no relevant financial or non-financial interests to disclose.

References

Abraham, M., Saeghe, P., Mcgill, M., & Khamis, M. (2022). Implications of XR on privacy, security and behaviour: Insights from experts. In *Nordic human-computer interaction conference, 1–12. NordiCHI '22*. Association for Computing Machinery. https://doi.org/10.1145/3546155.3546691

Access Age-Restricted Content & Features. (n.d.). Google Account Help. Retrieved February 13, 2023, from https://support.google.com/accounts/answer/10071085?visit_id=638118830802650744-3756593632&p=age-verify&rd=1

Aguiar, L., Peukert, C., Schäfer, M., & Ullrich, H. (2022). Facebook shadow profiles. arXiv. https://doi.org/10.48550/arXiv.2202.04131

Alsop, T. 2022. Topic: XR: AR, VR, and the metaverse. Statista. Retrieved October 20, 2022, from https://www.statista.com/topics/6072/extended-reality-xr/

Ang, S., & Quarles, J. (2023). Reduction of cybersickness in head mounted displays use: A systematic review and taxonomy of current strategies. *Frontiers in Virtual Reality*, *4*, 1027552. https://www.frontiersin.org/articles/10.3389/frvir.2023.1027552

Artzt, M. (2022). Metaverse and privacy. Retrieved August 23, 2022, from https://iapp.org/news/a/metaverse-and-privacy-2/.

Awan, I. (2017). Cyber-extremism: ISIS and the power of social media. *Society*, *54*(2), 138–149. https://doi.org/10.1007/s12115-017-0114-0

Axelsson, A.-S. (2002). The digital divide: Status differences in virtual environments. In R. Schroeder (Ed.), *The social life of avatars* (pp. 188–204). Computer Supported Cooperative Work. Springer. https://doi.org/10.1007/978-1-4471-0277-9_11

Bagheri, R. (2017). Virtual reality: The real life consequences. *UC Davis Business Law Journal*, *17* (March), 102–120.

Bailey, J. O., Bailenson, J. N., Obradović, J., & Aguiar, N. R. (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

Bardhan, A. (2022). Men are creating AI girlfriends and then verbally abusing them. Futurism. Retrieved January 18, 2022, from. https://futurism.com/chatbot-abuse

Barreda-Ángeles, M., & Hartmann, T. (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, T. (2021). The metaverse has a groping problem already. MIT Technology Review. Retrieved December 21, 2021, from 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.

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. In *Proceedings of the 2021 CHI conference on human factors in computing systems, 1–15. CHI '21*. Association for Computing Machinery. https://doi.org/10.1145/3411764.3445157

Bertuzzi, L. (2022) Leading lawmakers pitch extending scope of AI rulebook to the metaverse. *Euractiv*. Retrieved September 29, 2022, from https://www.euractiv.com/section/digital/news/leading-lawmakers-pitch-extending-scope-of-ai-rulebook-to-the-metaverse/

Bertuzzi, L. (2023) EU consumer department to present voluntary pledge over 'Cookie Fatigue'. *Euractiv*. Retrieved March 23, 2023, from. https://www.euractiv.com/section/data-privacy/news/eu-consumer-department-to-present-voluntary-pledge-over-cookie-fatigue/

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). Retrieved December 5, 2022, from https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-32022-dispute-submitted_en

Blackwell, L., Ellison, N., Elliott-Deflo, N., & Schwartz, R. (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

Bradford, A. (2020). *The brussels effect: How the European union rules the world*. Oxford University Press.

Bryant, J. (2023). Irish DPC, EDPB Meta decisions raise complex, fundamental questions. Retrieved January 13 2023, from https://iapp.org/news/a/irelands-meta-decisions-raise-complex-fundamental-questions/

Bublitz, J. C. (2022). Novel neurorights: From nonsense to substance. *Neuroethics*, *15*(1), 7. https://doi.org/10.1007/s12152-022-09481-3

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Proceedings of the 1st conference on fairness, accountability and transparency* (pp. 77–91). PMLR. https://proceedings.mlr.press/v81/buolamwini18a.html

Bylieva, D., Bekirogullari, Z., Lobatyuk, V., & Nam, T. (2021). How virtual personal assistants influence children's communication. In D. Bylieva, A. Nordmann, O. Shipunova, & V. Volkova (Eds.), *Knowledge in the information society* (pp. 112–124). Lecture notes in networks and systems. Springer International Publishing. https://doi.org/10.1007/978-3-030-65857-1_12

Campoamor, D. (2022). New report reveals the dangers of virtual reality for young children. *TODAY*. Retrieved March 24, 2022, from https://www.today.com/parents/parents/dangers-virtual-reality-young-children-rcna21278

Canales, K. (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 Llaw. Business Insider. Retrieved January 14, 2022, from https://www.businessinsider.com/why-you-must-be-13-facebook-instagram-problematic-law-coppa-2022-1

Canbay, Y., Utku, A., & Canbay, P. (2022). Privacy concerns and measures in metaverse: A review. In *2022 15th International Conference on Information Security and Cryptography (ISCTURKEY)* (pp. 80–85). https://doi.org/10.1109/ISCTURKEY56345.2022.9931866

Chang, P. (2018). U.S. Navy enlists virtual and augmented reality for cutting-edge training and recruitment. Retrieved October 12, 2018, from https://arpost.co/2018/10/12/us-navy-virtual-augmented-reality-cutting-edge-training-recruitment/

Chan, J., Ghose, A., & Seamans, R. (2016). The internet and racial hate crime: Offline spillovers from online access. *MIS Quarterly*, *40*(2).

Chemaly, S. (2014). When it comes to harassment and stalking, the virtual world IS real. HuffPost. Retrieved January 10, 2014, from. https://www.huffpost.com/entry/when-it-comes-to-harassme_b_4577719.

Chen, Z., Jiayang, W., Gan, W., & Zhenlian, Q. (2022, November). Metaverse security and privacy: An overview. https://doi.org/10.48550/arXiv.2211.14948

Committee on the Internal Market and Consumer Protection. (2023). Draft report: Virtual worlds - Opportunities, risks and policy implications for the single market. European Parliament. https://www.europarl.europa.eu/doceo/document/IMCO-PR-751902_EN.pdf

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. (1999). *OB L* Vol. *210*. http://data.europa.eu/eli/dir/1985/374/1999-06-04/eng

Crawford, A., & Smith, T. (2022). Metaverse app allows kids into virtual strip clubs. *BBC News*, Retrieved February 23, 2022, from sec. Technology. https://www.bbc.com/news/technology-60415317

Deliberação/2021/622. (2021). Comissão Nacional de Proteção de Dados. https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121887.

De Luca, S. (2023). New product liability directive. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739341/EPRS_BRI(2023)739341_EN.pdf

Del Vicario, M., Vivaldo, G., Bessi, A., Zollo, F., Scala, A., Caldarelli, G., & Quattrociocchi, W. (2016). Echo chambers: Emotional contagion and group polarization on facebook. *Scientific Reports*, *6*(1), 37825. https://doi.org/10.1038/srep37825

De Pasquale, C., Dinaro, C., & Sciacca, F. (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

de Ridder, D. D., Kroese, F., & van Gestel, L. (2022). Nudgeability: Mapping conditions of susceptibility to nudge influence. *Perspectives on Psychological Science*, *17*(2), 346–359. https://doi.org/10.1177/1745691621995183

Digital, Culture, Media and Sport Committee. (2019). Psychosocial harms of immersive technologies. UK Parliament. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1846/184605.htm.

Digital Markets Act. (2022). Text. *European Commission - European Commission*. Retrieved October 31, 2022, from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6423

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on General Product Safety. (2001). *OJ L* Vol. *011*. 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). (2002). *OJ L 201* Vol. *201*. http://data.europa.eu/eli/dir/2002/58/oj/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). (2010). *OJ L* Vol. *095*. 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. (2013). *OJ L* Vol. *218*. 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. (2016). L 327/1. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32016L2102

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). OJ L *333*. https://eur-lex.europa.eu/eli/dir/2022/2555

Doctor, A. C., Elson, J. S., & Hunter, S. (2022). The metaverse offers a future full of potential– For terrorists and extremists, too. *The Conversation*. Retrieved January 7, 2022, from http://theconversation.com/the-metaverse-offers-a-future-full-of-potential-for-terrorists-and-extremists-too-173622

Dove, E. S., & Chen, J. (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), 107–124. https://doi.org/10.1093/idpl/ipab005

Duffy, C. (2023). Meta lowers the minimum age for its quest headsets from 13 to 10. *CNN Business*. June 16, 2023. https://www.cnn.com/2023/06/16/tech/meta-quest-headsets-lowering-minimum-age/index.html

Eskens, S. (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), 143–155.

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. (2021). Shaping Europe's digital future. Retrieved September 15, 2021, from. https://digital-strategy.ec.europa.eu/en/policies

European Commission. (2022). Proposal for an ePrivacy regulation. European Commission. Retrieved June 7, 2022, from. https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation.

European Commission. (2023). *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*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0442.

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. Retrieved August 31, 2022, from. https://www.echr.coe.int/documents/guide_art_8_eng.pdf.

European Declaration on Digital Rights and Principles for the Digital Decade. (2023). *OJ C*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001

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. *European Parliament*. https://www.europarl.europa.eu/doceo/document/A-9-2023-0442_EN.html

European Parliament Legislative Resolution of 13 March 2024 on the Proposal for a Regulation of the European Parliament and of the Council on Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021)0206–C9-0146/2021– 2021/0106(COD)). (2024). https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf

Face ID & Privacy. (n.d.). Apple legal. Retrieved February 13, 2023, from. https://www.apple.com/legal/privacy/data/en/face-id/

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

Fernandez, M. (2019). Epilepsy foundation was targeted in mass strobe cyberattack. *The New York Times*, Retrieved December 16, 2019, from sec. U.S. https://www.nytimes.com/2019/12/16/us/strobe-attack-epilepsy.html.

Floridi, L. (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, L. (2017). Group privacy: A defence and an interpretation. In *Group privacy: New challenges of data technologies*. Taylor, L., Floridi, L., & Van der Sloot, B. (Eds.). Philosophical Studies Series. Cham: Springer International Publishing. 83–100. https://doi.org/10.1007/978-3-319-46608-8_5

Floridi, L. (2020). 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, L. (2022). Metaverse: A matter of experience. *Philosophy & Technology*, *35*(3), 73. https://doi.org/10.1007/s13347-022-00568-6

Franklin, M., Ashton, H., Gorman, R., & Armstrong, S. (2022, May). Missing mechanisms of manipulation in the EU AI Act. In *The international FLAIRS conference proceedings* (Vol. 35). https://doi.org/10.32473/flairs.v35i.130723

French, K. (2017). First they got sick, then they moved into a virtual utopia. *Wired*, Retrieved February 13, 2017, from https://www.wired.com/2017/02/first-they-got-sick-then-they-moved-into-a-virtual-utopia/

Frenkel, S., & Browning, K. (2021). The metaverse's dark side: Here come harassment and assaults. *The New York Times*, Retrieved December 30, 2021, from sec. Technology https://www.nytimes.com/2021/12/30/technology/metaverse-harassment-assaults.html.

Friedman, D. (1996). A world of strong privacy: Promises and perils of encryption. *Social Philosophy and Policy*, *13*(2), 212–228. https://doi.org/10.1017/S0265052500003526

Fristed, E., Skirrow, C., Meszaros, M., Lenain, R., Meepegama, U., Cappa, S., Aarsland, D., & Weston, J. (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

Ghiță, A., & Gutiérrez-Maldonado, J. (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

Grady, P. (2023). [Document] IMCO's draft report on virtual worlds. Retrieved July 14, 2023, from https://www.metaversepolicy.eu/p/document-imcos-draft-report-on-virtual

Granero, R., Fernández-Aranda, F., Mestre-Bach, G., Steward, T., Baño, M., Del Pino-gutiérrez, A., Moragas, L., Mallorquí-Bagué, N., Aymamí, N., Gómez-Peña, M., Tárrega, S., Menchón, J. M., & Jiménez-Murcia, S. (2016). Compulsive buying behavior: Clinical comparison with other behavioral addictions. *Frontiers in Psychology*, *7*(June), 914. https://doi.org/10.3389/fpsyg.2016.00914

Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognise and avoid them. (2022). European Data Protection Board. https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

Hayles, N. K. (1996). Embodied virtuality: Or how to put bodies back into the picture. In M. A. Moser & D. MacLeod (Eds.), *Immersed in technology: Art and virtual environments* (pp. 1–28). MIT Press. https://ieeexplore.ieee.org/document/6300716

Heller, B. (2020). Reimagining reality: Human rights and immersive technology. Carr Center Discussion Paper Series. https://carrcenter.hks.harvard.edu/publications/reimagining-reality-human-rights-and-immersive-technology

Hertz, N. (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

Hill, K. (2022). This is life in the metaverse. *The New York Times*, Retrieved October 7, 2022, from, sec. Technology. https://www.nytimes.com/2022/10/07/technology/metaverse-facebook-horizon-worlds.html

Hine, E. (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

Home Security Heroes. (2024). 2023 State of deepfakes: Realities, threats, and impact. *Home security heroes*. https://www.homesecurityheroes.com/state-of-deepfakes

Huang, Y., Li, Y., & Cai, Z. (2022, November). Security and privacy in metaverse: A comprehensive survey. *Big Data Mining and Analytics*. https://doi.org/10.26599/BDMA.2022.9020047

Hupont, T. I., Charisi, V., de Prato, G., Pogorzelska, K., Schade, S., Kotsev, A., Sobolewski, M., Duch, B. N., Calza, E., Dunker, C., Di Girolamo, F., Bellia, M., Hledik, J., Fovino, I. N., & Vespe, M. (2023). *Next generation virtual worlds: Societal, technological, economic and policy challenges for the EU*. European Commission. https://doi.org/10.2760/51579

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.

Jacob, N., Evans, R., & Scourfield, J. (2017). The influence of online images on self-harm: A qualitative study of young people aged 16–24. *Journal of Adolescence*, *60* (October), 140–147. https://doi.org/10.1016/j.adolescence.2017.08.001

Jahan, N., Naveed, S., Zeshan, M., & Tahir, M. A. (2016). How to conduct a systematic review: A narrative literature review. *Cureus*, *8*(11), e864. https://doi.org/10.7759/cureus.864

Jasper, A., Cone, N., Meusel, C., Curtis, M., Dorneich, M. C., & Gilbert, S. B. (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

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%26utm_medium=email%26utm_campaign=29-541%26pnespid=6bhqDSobLqlCxOmRqjnvSZnUphCwV55zPbGmyO5toAdmNnl0ntCzVQTVlh6t6v.npd2W8zZNCg

Kalpokas, I., & Kalpokienė, J. (2023). *Regulating the metaverse: A critical assessment*. Routledge. https://doi.org/10.4324/9781003355861

Kelly, J. W., Gilbert, S. B., Dorneich, M. C., & Costabile, K. A. (2023). Gender differences in cybersickness: Clarifying confusion and identifying paths forward. In *2023 IEEE conference on virtual reality and 3D user interfaces abstracts and workshops (VRW)* (pp. 283–288). https://doi.org/10.1109/VRW58643.2023.00067

Kleinman, Z. (2019). My son spent £3,160 in one game. *BBC News*, Retrieved July 15, 2019, from, sec. Technology. https://www.bbc.com/news/technology-48925623

Koops, B.-J. (2014). The trouble with European data protection law. *International Data Privacy Law*, *4*(4), 250–261. https://doi.org/10.1093/idpl/ipu023

Kröger, J. L., Hans-Martin Lutz, O., & Müller, F. (2020). What does your gaze reveal about you? On the privacy implications of eye tracking. In M. Friedewald, M. Önen, E. Lievens, S. Krenn, & S. Fricker (Eds.), *Privacy and identity management. Data for better living: AI and privacy. Privacy and identity 2019* (Vol. 576, pp. 226–241). IFIP advances in information and communication technology. Springer. https://doi.org/10.1007/978-3-030-42504-3_15

Kulal, S., Zhigang, L., & Tian, X. (2022). Security and privacy in virtual reality: A literature review. *Issues In Information Systems*, *23*(2), 185–192. https://doi.org/10.48009/2_iis_2022_125

Lanier, J., & Biocca, F. (1992). An insider's view of the future of virtual reality. *Journal of Communication*, *42*(4), 150–172. https://doi.org/10.1111/j.1460-2466.1992.tb00816.x

La Quadrature du Net and Others v Premier ministre and Others. (2020). ECJ.

Lauri, M. A., & Farrugia, L. (2020). Identity exploration in anonymous online spaces. In L. Green, D. Holloway, K. Stevenson, T. Leaver, & L. Haddon (Eds.), *The Routledge companion to digital media and children* (pp. 173–184). Routledge. https://doi.org/10.4324/9781351004107-16

Laux, J., Wachter, S., & Mittelstadt, B. (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

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.

Legacy Verification Policy. (n.d.). Retrieved February 13, 2023, from https://help.twitter.com/en/managing-your-account/legacy-verification-policy.

Lemley, M., and Volokh, E. (2018). Law, virtual reality, and augmented reality. *University of Pennsylvania Law Review*, 166(5), 1051. https://scholarship.law.upenn.edu/penn_law_review/vol166/iss5/1

LfD Lower Saxony. (2021). LfD lower Saxony imposes a fine of 10.4 million Euros on Notebooksbilliger.De. Retrieved January 8, 2021, from. https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-verhangt-bussgeld-uber-10-4-millionen-euro-gegen-notebooksbilliger-de-196019.html

Lin, W.-H., Liu, C.-H., & Yi, C.-C. (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, I. T. (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.

Lomas, N. (2023). Meta tries to keep denying EU users a free choice over tracking– But change is coming. *TechCrunch* (blog). Retrieved March 30, 2023, from https://techcrunch.com/2023/03/30/meta-facebook-gdpr-ads-tracking/

Lovato, S. B., Marie Piper, A., & Wartella, E. A. (2019, June). Hey Google, do unicorns exist? In *Proceedings of the 18th ACM international conference on interaction design and children* (pp. 301–312). https://doi.org/10.1145/3311927.3323150

Lü, Q. (2023). Tencent disbands XR team, ByteDance's Pico lays off staff as metaverse fever fades. Yicai Global. Retrieved February 17, 2023, from https://www.yicaiglobal.com/news/tencent-dissolves-xr-team-bytedance-pico-lays-off-staff-as-metaverse-hype-fades?mc_cid=6001f1b13c%26mc_eid=c29ab63a8f

Maciejewski, M. (2023). Metaverse. European Parliament Policy Department for Citizens' Rights and Constitutional Affairs. https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU(2023)751222_EN.pdf

Madiega, T., Car, P., Niestadt, M., & Pol, L. V. D. (2022). *Metaverse: Opportunities, risks and policy implications*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf

Malik, A. (2023). Instagram starts testing its age verification tools in more countries. *TechCrunch* (blog). Retrieved March 2, 2023, from https://techcrunch.com/2023/03/02/instagram-starts-testing-its-age-verification-tools-in-more-countries/

Marinotti, J. (2022). Can you truly own anything in the metaverse? A law professor explains how blockchains and NFTs don't protect virtual property. The Conversation. Retrieved April 21, 2022, from http://theconversation.com/can-you-truly-own-anything-in-the-metaverse-a-law-professor-explains-how-blockchains-and-nfts-dont-protect-virtual-property-179067.

Martin, B. (2022). Privacy in a programmed platform: How the general data protection regulation applies to the metaverse. *Harvard Journal of Law & Technology*, *36*(1).

Maynard, P., Cooper, D., & O'Shea, S. (2022). Special category data by inference: CJEU significantly expands the scope of Article 9 GDPR. Inside Privacy. Retrieved August 10, 2022, from https://www.insideprivacy.com/eu-data-protection/special-category-data-by-inference-cjeu-significantly-expands-the-scope-of-article-9-gdpr/

McCay, A. (2022, March). Neurorights: The Chilean constitutional change. *AI and Society*. https://doi.org/10.1007/s00146-022-01396-0

McStay, A. (2023). The metaverse: Surveillant physics, virtual realist governance, and the missing commons. *Philosophy and Technology*, *36*(1), 13. https://doi.org/10.1007/s13347-023-00613-y

Merritt, A. L. (1989). Damages for emotional distress in fraud litigation: Dignitary torts in a commercial society. *Vanderbilt Law Review*, *42*(1), 1–38.

Meta Accessibility. (2022). Meta Accessibility. *Facebook*. https://www.facebook.com/accessibility/photos/a.544973158879747/4925712904139062/

Michael, M., & Metzinger, T. K. (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.

Miehlbradt, J., Cuturi, L. F., Zanchi, S., Gori, M., & Micera, S. (2021). Immersive virtual reality interferes with default head–trunk coordination strategies in young children. *Scientific Reports*, *11*(1), 17959. https://doi.org/10.1038/s41598-021-96866-8

Milgram, P., & Kishino, F. (1994). A taxonomy of mixed reality visual displays. *IEICE Transactions on Information and Systems*, *E77-D*(12), 1321–1329.

Miller, R. (2023). Microsoft's industrial metaverse aspirations can wait. *Forbes*. https://www.forbes.com/sites/rosemariemiller/2023/02/14/microsofts-industrial-metaverse-aspirations-can-wait/

Mitsilegas, V., Guild, E., Kuskonmaz, E., & Vavoula, N. (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

Nair, V., Guo, W., Mattern, J., Wang, R., O'Brien, J. F., Rosenberg, L., & Song, D. (2023). Unique identification of 50,000+ virtual reality users from head & hand motion data. arXiv. http://arxiv.org/abs/2302.08927

Needleman, S. E., & Rodriguez, S. (2022). VR to the ER: Metaverse early adopters prove accident-prone. *Wall Street Journal*, Retrieved February 1, 2022, from sec. Page One. https://www.wsj.com/articles/metaverse-virtual-reality-vr-accident-prone-meta-11643730489

O'Brolcháin, F., Jacquemard, T., Monaghan, D., O'Connor, N., Novitzky, P., & Gordijn, B. (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

Oliva, T. D., Marcelo Antonialli, D., & Gomes, A. (2021). Fighting hate speech, silencing drag queens? Artificial intelligence in content moderation and risks to LGBTQ voices online. *Sexuality & Culture*, *25*(2), 700–733.

OT v Vyriausioji tarnybinės etikos komisija. (2022). ECJ.

Outlaw, J. (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%26usp=embed_facebook

Pahi, S., and Schroeder, C. (2023). Extended privacy for extended reality: XR technology has 99 problems and privacy is several of them. *Notre Dame Journal on Emerging Technologies*, *4*(1), 1. https://scholarship.law.nd.edu/ndlsjet/vol4/iss1/1/

Parsons, T. D., Courtney, C., Cosand, L., Iyer, A., Rizzo, A. A., & Oie, K. (2009). Assessment of psychophysiological differences of west point cadets and civilian controls immersed within a virtual environment. In D. D. Schmorrow, I. V. Estabrooke, & M. Grootjen (Eds.), *Foundations of augmented cognition. Neuroergonomics and operational neuroscience* (pp. 514–523). Lecture Notes in Computer Science. Springer. https://doi.org/10.1007/978-3-642-02812-0_60

Patchin, J. W. (2019). Cyberbullying data 2019. *Cyberbullying Research Center* (blog). Retrieved July 9, 2019, from https://cyberbullying.org/2019-cyberbullying-data.

Penney, J. W. (2016). Chilling Effects: Online surveillance and wikipedia use. *Berkeley Technology Law Journal*, *31*(1), 117–182.

Perez, S. (2022). Meta to allow horizon worlds users to turn their avatar's personal safety boundary off. TechCrunch. Retrieved March 14, 2022, from 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/

Peters, J. (2023). Comedians are trying to make the metaverse cool, but it won't let them. The Verge. Retrieved March 21, 2023, from https://www.theverge.com/2023/3/21/23645512/meta-horizon-worlds-metaverse-comedians

Petrányi, D., Horváth, K., & Domokos, M. (2023). Part 4| Expected impact of the EU artificial intelligence regulation, the metaverse as a workplace. CMS. https://cms.law/en/int/publication/legal-issues-in-the-metaverse/part-4-expected-impact-of-the-eu-artificial-intelligence-regulation-the-metaverse-as-a-workplace

Polonioli, A., Ghioni, R., Greco, C., Juneja, P., Tagliabue, J., & Floridi, L. (2023). The ethics of online controlled experiments (A/B Testing). *Minds and Machines*. https://doi.org/10.1007/s11023-023-09644-y

Pozharliev, R., De Angelis, M., & Rossi, D. (2022). The effect of augmented reality versus traditional advertising: A comparison between neurophysiological and self-reported measures. *Marketing Letters*, *33*(1), 113–128. https://doi.org/10.1007/s11002-021-09573-9

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). https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Liability for Defective Products. (2022). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495

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

PwC Digital Ethics for Responsible Metaverse. (2022).

Reed, N., & Joseff, K. (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). (2016). *OJ L* Vol. *119*. 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. (2021). *OJ L* Vol. *172*. 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). (2022). *OJ L* Vol. *265*. 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). (2022). *OJ L* Vol. *277*. 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. (2023). *OJ L* Vol. *135*. http://data.europa.eu/eli/reg/2023/988/oj/eng

Renieris, E. M. (2023). *Beyond data: Reclaiming human rights at the dawn of the metaverse*. MIT Press. https://mitpress.mit.edu/9780262047821/beyond-data/

Roberts, H. (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

Robertson, A. (2022). Meta is adding a 'Personal Boundary' to VR avatars to stop harassment. The Verge. Retrieved February 4, 2022, from https://www.theverge.com/2022/2/4/22917722/meta-horizon-worlds-venues-metaverse-harassment-groping-personal-boundary-feature

Roessler, B. (2005). *The Value of Privacy*. Polity.

Roessler, B. (2018). Three dimensions of privacy. In *Handbook of privacy studies: An interdisciplinary introduction* (pp. 137–142). Amsterdam University Press. https://www-cambridge-org.ezproxy.unibo.it/core/books/abs/handbook-of-privacy-studies/three-dimensions-of-privacy/F759F4050608495A318D894AEBBCD672

Rosenberg, L. (2022a). Migration to the metaverse: We need guaranteed basic immersive rights. *VentureBeat* (blog). Retrieved September 11, 2022, from https://venturebeat.com/virtual/metaverse-we-need-guaranteed-basic-immersive-rights/

Rosenberg, L. (2022b). Mind control: The metaverse may be the ultimate tool of persuasion. *VentureBeat* (blog). Retrieved October 22, 2022, from https://venturebeat.com/virtual/mind-control-the-metaverse-may-be-the-ultimate-tool-of-persuasion/

Rupp, H. A., & Wallen, K. (2007). Sex differences in viewing sexual stimuli: An eye-tracking study in men and women. *Hormones and Behavior*, *51*(4), 524–533. https://doi.org/10.1016/j.yhbeh.2007.01.008

Schmitz, M., Burghardt, K., & Muric, G. (2022). Quantifying how hateful communities radicalize online users. In *2022 IEEE/ACM international conference on advances in social networks analysis and mining (ASONAM)* (pp. 139–146). https://doi.org/10.1109/ASONAM55673.2022.10068644

Schroeder, R. (2010). *Being there together: Social interaction in shared virtual environments*. Oxford University Press.

Segovia, K. Y., & Bailenson, J. N. (2009). Virtually true: Children's acquisition of false memories in virtual reality. *Media Psychology*, *12*(4), 371–393. https://doi.org/10.1080/15213260903287267

Sethi, A. (2022). Security and privacy in metaverse: Issues, challenges, and future opportunities. *Cyber Security Insights Magazine*, 2022.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477. https://doi.org/10.2307/40041279

Spiegel, J. S. (2018). The ethics of virtual reality technology: Social hazards and public policy recommendations. *Science and Engineering Ethics*, *24*(5), 1537–1550. https://doi.org/10.1007/s11948-017-9979-y

Stanford HAI dir, (2022). *Jeremy Bailenson: Your mind on the metaverse*https://www.youtube.com/watch?v=idD1rZ7UqT0

Stephen, P., Allison, R. S., & Kim, J. (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

Stoner, G. (2022). VR is here to stay. It's time to make it accessible. Retrieved January 3, 2022, from https://www.wired.com/story/virtual-reality-accessibility-disabilities/

The Virtual Reality Show, dir. (2022). *VRChat's MAJOR drinking problem*. https://www.youtube.com/watch?v=XS99QBGTS7E

Thorbecke, C. (2023). What metaverse? Meta says its single largest investment is now in 'Advancing AI'. CNN. Retrieved March 15, 2023, from https://www.cnn.com/2023/03/15/tech/meta-ai-investment-priority/index.html

Tucker, J., Guess, A., Barbera, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D., & Nyhan, B. (2018). Social media, political polarization, and political disinformation: A review of the scientific literature. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3144139

Turner, P. G., & Lefevre, C. E. (2017). Instagram use is linked to increased symptoms of orthorexia nervosa. *Eating and Weight Disorders - Studies on Anorexia, Bulimia and Obesity*, *22*(2), 277–284. https://doi.org/10.1007/s40519-017-0364-2

United Nations Human Rights Office of the High Commissioner. (2011). 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

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)Informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 973–990). ACM. https://doi.org/10.1145/3319535.3354212

Vale, S. B., & Berrick, D. (2023). Reality check: How is the EU ensuring data protection in XR technologies? — The digital constitutionalist. Retrieved January 25, 2023, from https://digi-con.org/reality-check-how-is-the-eu-ensuring-data-protection-in-xr-technologies/

Visual Venture, dir. (2023). *The dark world of VRChat (Ft. iamLucid)*. https://www.youtube.com/watch?v=exLtUH2bO6M

Wachter, S., & Mittelstadt, B. (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), 494–620. https://doi.org/10.7916/cblr.v2019i2.3424

Wells, G., Horwitz, J., & Seetharaman, D. (2021). Facebook knows instagram is toxic for teen girls, company documents show. *The Wall Street Journal*, Retrieved September 14, 2021, from https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739

Whelan, R., & Flint, J. (2023). Disney eliminates its metaverse division as part of company's layoffs plan. The Wall Street Journal. Retrieved March 28, 2023, from https://www.wsj.com/articles/disney-eliminates-its-metaverse-division-as-part-of-companys-layoffs-plan-94b03650?mod=djemalertNEWS%26utm_source=substack%26utm_medium=email

WHO Team. (2020). Addictive behaviours: Gaming disorder. Retrieved October 22, 2020, from. https://www.who.int/news-room/questions-and-answers/item/addictive-behaviours-gaming-disorder

Wilson, J. 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

World Economic Forum. (2022). *Shaping the future of media, entertainment and sport: Defining and building the metaverse*.

Yoti. (2023). Yoti facial age estimation white paper. https://www.yoti.com/wp-content/uploads/Yoti-Age-Estimation-White-Paper-March-2023.pdf

Yuntao, W., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. In *IEEE communications surveys & tutorials* (pp. 1–1). https://doi.org/10.1109/COMST.2022.3202047

Zallio, M., & John Clarkson, P. (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

Ziosi, M., Mökander, J., Novelli, C., Casolari, F., Taddeo, M., & Floridi, L. (2023). The EU AI liability directive: Shifting the burden from proof to evidence. *SSRN Scholarly Paper*. Rochester, NY. https://doi.org/10.2139/ssrn.4470725