VIRTUAL WORLDS
REAL RISKS AND CHALLENGES

1st XR Data Classification Roundtable Report
XR Safety Week 2021 – December 10th, 2021

www.dc.xrsi.org

Hosted by

Supported by

Executive Summary

Today, most people understand that internet technologies generate data with each click, like, and share. Humans have relied on data collection and sharing to record and propagate historical facts, ideas, and opinions across timelines. In the past few decades, the creation, processing, and sharing of data have become so common that most people have stopped paying attention to the amount of data they give away every day.

People relinquish their data without realizing the risks or consequences. While this is not new, the difference today is we are moving towards an era of constant reality capture, especially with the increased adoption of immersive technologies and a strong push to build the next iteration of the Internet, also known as the Metaverse[1].

Immersive technologies, including Extended Reality (XR)[2] and Internet of Things (IoT), bring a new set of privacy, cybersecurity, and safety concerns, at a time when we have not fully addressed the challenges of the Internet era. XR technologies currently being used to create virtual worlds introduce real-world risks to humans, amplified as we evolve towards the Metaverse. Kavya Pearlman, founder and CEO of the XR Safety Initiative (XRSI), recognized the coming wave of technology challenges in 2018 and started research into the massive data collection associated with virtual worlds and the real risks that come with them[3]. Most privacy laws and data protection principles of our times are going to be inadequate because they do not fully address the risks related to the processing of XR data, giving way to undermining human rights.

1 XRSI defines the Metaverse as "the convergence of several enabling technologies and experiences: AR, VR, 5G, AI, edge networks, improved graphics and computer hardware, and improved mobile device capabilities."

2 Extended Reality (XR) is a fusion of all the realities – including Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR) – which consists of technology-mediated experiences enabled via a wide spectrum of hardware and software, including sensory interfaces, applications, and infrastructures.

3 Pearlman, K. (2018, September). Virtual Worlds - Real Risks. Cybersecurity Quarterly; Center for Internet Security (CIS). https://issuu.com/cybersecurityquarterly/docs/csq_volume_2_issue_3/14

XRSI commenced its mission in early 2019 and immediately started researching and investigating these matters launching an XR Data Classification Public Working Group[4] to pursue the following goals:

- Establish a "standards-based" workflow to manage access and use of XR data and computing resources.
- Develop a standard approach to communicating any data/resource.
- Establish reporting to and coordination with funding agencies.
- Develop "community-based" contracts to streamline the acquisition of services.
- Encourage commercial providers to research the emerging Metaverse and cyberspace consistent with community-generated requirements and compliant with relevant policies.
- Analyze stewardship, policy-based, regulatory, contractual, and financial obligations related to the access to and use of XR technologies;

The XR Data Classification Roundtable is a series of gatherings hosted by XRSI to address the issues that stem from the massive collection of data. This report recognizes that while the Metaverse may be an interconnected network of Virtual Worlds, the risks associated with it are very real and could lead to human rights violations if not addressed proactively.

4 "XR Data Classification Working Group – XR Data Classification." XR Data Classification Roundtable, Framework, Working Group for a Safer XR, dc.xrsi.org/working-group/. Accessed 4 Feb. 2022.

Table of Contents

Introduction

On December 10, 1948, the UN General Assembly adopted the Universal Declaration of Human Rights (UDHR). This milestone document proclaims the inalienable rights of every human being, regardless of race, color, religion, sex, language, political or other opinions, national or social origin, property, birth, or different statuses. To mark the 73rd International Human Rights Day, XRSI organized the second annual XR Safety Week, which took place December 6-10, 2021. The week presented individuals and privately held companies opportunities to come together, educate, learn, and raise awareness of the opportunities and risks XR presents to individuals and society.

The fifth and final day of XR Safety Week began with an affirmation of participants and represented organizations to the Universal Declaration of Human Rights. An XR Data Classification Roundtable spearheaded the day's formal activities, fostering dialogue to create awareness around the impact of XR data collection on human rights. While the discussions focused on XR data, the specific context of data collections and uses was the Metaverse. The debate involved XR stakeholders, technologists, human rights experts, philanthropic foundations, and civil liberties organizations, along with a handful of influential technology companies. The roundtable discussion was rooted in the following objectives:

- Discuss the potential impact of massive data collection through XR and related Emerging Technologies.
- Discuss and establish a common understanding around the various contexts in which data can help or hurt humans and potentially undermine Human Rights.
- Focus on three contexts as a starting point: Education, Work, and Healthcare.

The roundtable discussion marks a critical step forward for XR data rights by establishing and mapping the classification contexts and schemes that enable and drive the adoption of the XR technologies and various intersections while ensuring not undermining human rights. The roundtable was a significant milestone in the broader work undertaken by XRSI's XR Data Classification Public Woking Group since 2019[5].

5 "XR Data Classification Working Group – XR Data Classification." XR Data Classification Roundtable, Framework, Working Group for a Safer XR, dc.xrsi.org/working-group/. Accessed 4 Feb. 2022.

WHAT WE KNOW

XR Data can undermine Human Rights

In the past few years, we have learned that massive data collection in virtual worlds brings with it real risks[6]. As we rapidly evolve towards the Metaverse, the door is closing on the opportunity to weigh and consider the risks and opportunities that such data collection will introduce, mostly as development is underway. To mitigate these risks, we need to understand the context of data collection and processing. These contexts of data collection and processing are guided by certain "informational norms"[7] which need to be established for XR in order to ensure human autonomy.

So far, we have learned the following lessons through the Working Group:

- XR Data can be defined as what's collected, inferred, processed, and shared from both consumers and bystanders to create and facilitate immersive experiences. XR Data includes Personally Identifiable Information (PII) and Personal Data, Biometrically-Inferred Data (BID), and Sensor Data to enable 6 degrees of freedom[8], presence, persistence, and immersion.
- Legal protections related to Personally Identifiable Information (PII) do not currently protect human rights from being undermined due to massive data collection in play for the development of XR ecosystems.
- Personal data, a subset of data that relates to individuals, is likely the only legal basis for addressing the issues stemming from the massive data collection to develop immersive technologies such as XR. EU General Data Protection Regulation (GDPR) defines personal data[9] as "any information relating to an identified or identifiable natural person ("data subject"); an

6 Pearlman, K. (2018, September). Virtual Worlds - Real Risks. Cybersecurity Quarterly; Center for Internet Security (CIS). https://issuu.com/cybersecurityquarterly/docs/csq_volume_2_issue_3/14

7 Nissenbaum, H. (2019). Contextual Integrity Up and Down the Data Food Chain. Theoretical Inquiries in Law, 20(1), 221–256. https://doi.org/10.1515/til-2019-0008

8 XR Safety Initiative. (2020, February). Degrees of Freedom (DoF) definition. XR Safety Initiative (XRSI). https://xrsi.org/definition/degrees-of-freedom-dof

9 European Commission. (2018a, November 14). Art. 4 GDPR - Definitions. GDPR.eu. https://gdpr.eu/article-4-definitions/

identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

- Although often erroneously used interchangeably, Personally Identifiable Information (PII) and Personal Data are not the same. Personal Data encompasses information that can be attributed indirectly to an individual; however, PII, a term primarily used in the U.S., has a much narrower scope and attributes directly to an individual. PII can be considered personal data, but not vice versa.
- When it comes to the processing and protection of personal data from a GDPR perspective, it does not explicitly include BID disclosure and misuse, etc., which may undermine human rights. However, a contextualized AI[10] could perform "automated processing of personal data" and can be attributed as "profiling"[11] in the XR context. This aspect of data processing can potentially place obligations on data controllers and contribute to data subject rights acting as an existing baseline for the immersive technologies.
- Organizations all around the globe continue to evade ethical and moral responsibility for protecting BID by declaring their product development work as "research."
- Unlike personal data, Article 9 of the GDPR[12] clearly defines special category data in a prescriptive manner, consisting of Racial or ethnic origin, Political opinions, Religious or philosophical beliefs, Trade union membership, Health data, Sex life or sexual orientation, Genetic data, Biometric data.
  The consequences of not protecting PII or personal data[13], which as we have seen requires knowledge of where the data is and what it is, could be severe and can be framed as follows: Operational risk, Legal/regulatory risk, Financial risk, Reputational risk, and Psychological or physical damages.

In case an event should occur, a security incident involving personal data constitutes a data breach. It may mandate notification and reporting to supervisory authorities and data subjects, depending on the extent of the violation. Currently, there are no laws or regulations that address and protect the risks stemming from the collection and processing of BID. It largely depends on understanding the context in which the data is collected and processed.

10 Brdiczka, O. (2019, September 4). Contextual AI: The next frontier of artificial intelligence. Adobe Experience Cloud Blog; Adobe. https://business.adobe.com/blog/perspectives/contextual-ai-the-next-frontier-of-artificial-intelligence

11 European Commission. (2018a, November 14). Art. 4 GDPR - Definitions. GDPR.eu. https://gdpr.eu/article-4-definitions

12 European Commission. (2018, November 14). Art. 9 GDPR - Processing of special categories of personal data. GDPR.eu. https://gdpr.eu/article-9-processing-special-categories-of-personal-data-prohibited

13 VentureBeat. (2021, November 10). Report: 58M Americans were victims of fraud in the past year. VentureBeat. https://venturebeat.com/2021/11/10/report-58m-americans-were-victims-of-fraud-in-the-past-year

Neuro Rights

A new level of protection for Digital Humans

With on-market XR hardware that can read EEG, ECG, and galvanic skin responses, there is a disappointing lack of established regulations and guidelines to develop these technologies further to uphold the individual's privacy rights.

While the biosignals captured by medical devices for medical and therapeutic use must adhere to stringent governance and regulatory guidelines, XR technologies on the consumer market do not abide by medical device regulations despite capturing the same biosignals.

As these technologies evolve, the capability to read mood and emotions with mental imagery and language is already possible or in an advanced stage of development. It is clear that these devices are capturing the personal data of a data subject. This is so as the "mental identity" of a person qualifies as "personal data" under Article 4(1) of the GDPR. Therefore, protecting the mental identity of a person is paramount, and the data subject ought to have an option to decide if it may or may not wish to share this personal data. As with any personal data being collected under GDPR, personal data of this nature should only be collected and shared following a completed opt-in process by the data subject, with a clear definition of what the data subjects are agreeing to share.

Furthermore, the capability to influence users moods, emotions, mental imagery, and language centers, whether this be via a direct neural interface, electromagnetic wave, temporal interference, visual, auditory, or chemical stimulation, requires the explicit and timely permission of the participant at the commencement of any XR session where it may be implemented, with the mechanisms, potential outcomes and hazards made clear to them immediately before their opportunity to permit or refuse these manners of influence.

As this is a nascent technology, the ongoing use of direct brain interfaces as listed above should be monitored for emergent addiction, habit formation, mental and physical health pathologies related to its use, with recommended use (both by end participants and technology developers) modified regularly and accordingly.

Along with monitoring this technology, legal frameworks should explore the concept of neuro rights. According to The NeuroRights Foundation, a New York-based organization who works at a global level to promote this concepts, neuro rights "give a user the freedom to decide who is allowed to monitor, read or alter your brain such as right to personal identity, right to free-will, right to mental privacy, the right to equal access to mental augmentation, the right to protection from algorithmic bias.[14]" In September 2021, Chile became the first country in the world to recognize mental integrity

14 Mission. The NeuroRights Foundation. Retrieved February 7, 2022, from https://neurorightsfoundation.org/mission

as a right of all citizens by amending its Constitution[15]. Other efforts, especially in Europe, are underway to connect neuro rights to the existing legislation and the principles stated in the EU Charter of Fundamental Rights[16]. In 2017, France updated the Loi Travail, the law regulating jobs, workspace, and workers' rights, introducing measures to protect mental integrity[17]. The Italian Data Protection Authority is currently examining the legal impacts of neuroscience and AI on the current regulations[18]. Finally, as these regimes develop, entities that follow GDPR must acknowledge that mental identity is recognized as personal data under GDPR. In the meantime, the obligations on data controllers in GDPR to protect mental identity must be fulfilled ensue.

Protecting PII and personal data has reduced the risks an organization can face in light of a data breach. Still, there are gaps in the legal understanding and concepts that lead to tremendous harm and danger regarding human rights. This can only be addressed by introducing new concepts considering BID and health inferences and taking approaches such as "prevention of harm[19]" and "safety by design[20]" principles. Such an understanding could become the foundation for protecting BID such as gaze, pose, gait, and other inferences about humans or an entire segment of society and cultures. On the other hand, a lack of safeguards around health inferences and BID could lead to potential human rights violations.

The Universal Declaration of Human Rights, adopted in 1948 by the United Nations, has led to fundamental advancements in addressing crucial topics such as torture, discrimination, gender inequality, religious and political freedom, inclusion, and accessibility. Current innovations and development require additional rights to maintain human agency, autonomy and free will. The transformations we face today and the growing complexity of the captured, stored, inferred, and transmitted data demand adopting a global framework for protecting mental well-being and neuro rights as a foundation for the Metaverse.

15 Constitución Política de la República de Chile, Article 19, section 1 (2021). https://www.bcn.cl/leychile/navegar?idNorma=242302&idParte=10085339

16 Article 3 - Right to integrity of the person. (2015b, April 25). European Union Agency for Fundamental Rights. https://fra.europa.eu/en/eu-charter/article/3-right-integrity-person

17 Droit du travail. Ministère du travail, de l'emploi et de l'insertion, République Française. Retrieved February 7, 2022, from https://travail-emploi.gouv.fr/droit-du-travail

18 La privacy e i nuovi scenari posti dalle neuroscienze nel convegno organizzato dal Garante in occasione della Giornata europea della protezione dati. (2021, January 28). Garante per La Protezione Dei Dati Personali (GPDP). https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9527139

19 XR Safety Initiative (XRSI). The XRSI Privacy and Safety Framework. https://xrsi.org/publication/the-xrsi-privacy-framework

20 Safety by Design. eSafety Commissioner. https://www.esafety.gov.au/industry/safety-by-design

OPENING SESSION OVERVIEW

The Roundtable discussion was opened by the co-chairs

- ***Kavya Pearlman***
  XRSI's founder & CEO and Founding Member of the Metaverse Reality Check
- ***Kristina Podnar***
  XRSI's Global Policy Advisor and Lead of the Metaverse Reality Check

Welcome to the 1st XR Data Classification Roundtable

On 73rd Human Rights Day – December 10th, 2021

Kavya Pearlman
Founder and CEO – XR Safety Initiative (XRSI)
Chair - Human Rights Day – XR Safety Week
Founding Member - Metaverse Reality Check (The MRC)

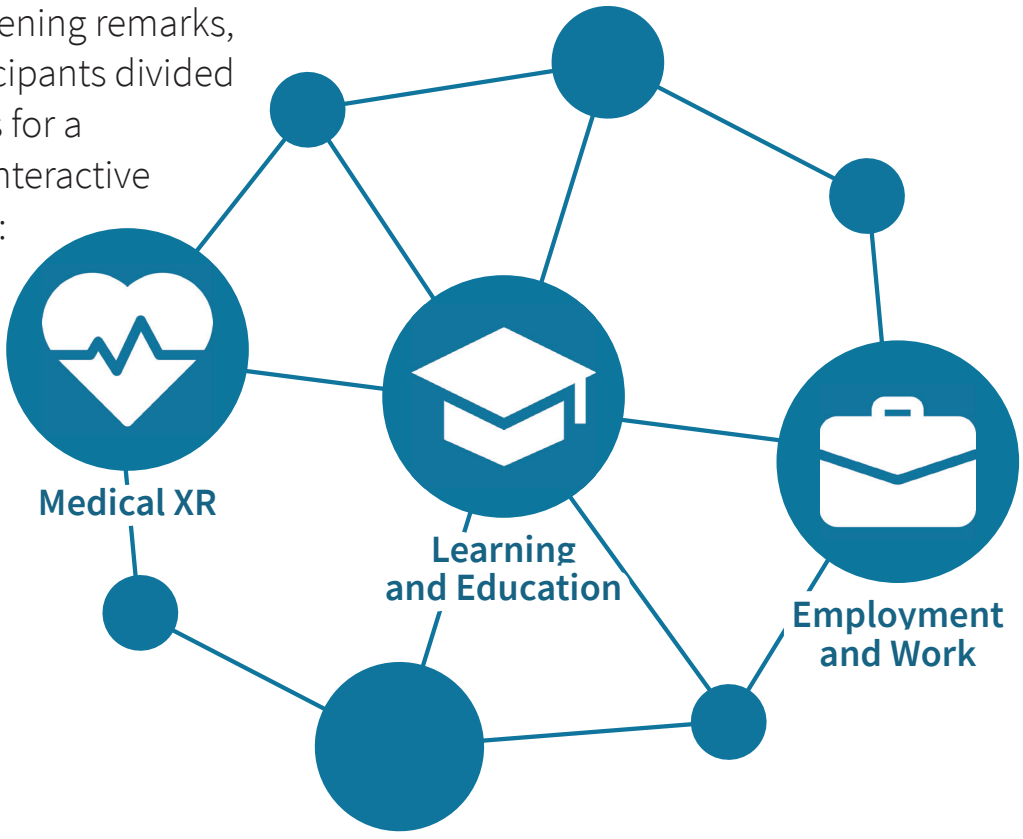
Kristina Podnar
Global Digital Policy Advisor – XRSI
Co-chair - Human Rights Day – XR Safety Week
Executive Lead – Metaverse Reality Check (The MRC)

XR SAFETY WEEK

Key messages of the Roundtable opening statement

- The magnitude and scale of XR data make it challenging to categorize in a simplified manner, especially when considering a broad context such as the Metaverse. Regardless, an attempt must be made to look through and analyze such a large amount of data with filters of information security, privacy and safety principles.
- XR has the potential to record various novel types of user information (from eye movements and emotions to the movement of a user's entire body through space); ensuring that this data is managed responsibly has become paramount for XR researchers and commercial entities alike. XR creates a complex convolution in which the biological mind and its technological niche influence each other in ways we are just beginning to understand. This complex convolution makes it essential to think about XR's Security, Privacy, and Ethics in a critical, evidence-based, and rational manner. The development of Data Classification guidance, standard vocabularies, and Data sets will undoubtedly contribute to understanding potential risks associated with XR data.
- XRSI has a technology leadership role consistent with its mission to inspire and catalyze the safe use of Extended Reality (XR) and help build a safe and inclusive Metaverse. As part of this, XRSI intends to create baseline standards and secure and effective adoption of XR technologies. Clear guidance and good practices could further aid organizations and stakeholders in planning the responsible adoption of XR technologies. During this process, we must consider the potential dangers of unintended data disclosures, data breaches, privacy, and Terms of Service (ToS) violations that could eventually impact their mission and objectives and cause Human Rights violations.

Following the opening remarks, roundtable participants divided into three groups for a workshop-style interactive thematic session:



The remainder of this document outlines the focus of each thematic session.

XR DATA AND IMPACT ON HUMANS

THEMATIC SESSION 1

Medical XR and Healthcare

Medical XR Subgroup Challenge Statement

The subgroup intended to classify biometric data, inferences, Personally Identifiable Information (PII), and non-PII data for various contexts within the medical and healthcare domain (such as clinical visits, diagnostics, etc.) while focusing on patient safety and autonomy as the prime objective.

XR in healthcare offers a bold promise to create a more precise, more accessible, and more effective assessment, treatment, diagnosis, and therapy. The COVID-19 pandemic has fueled the use of XR in healthcare as providers accelerated their digital transformation journeys and adopted novel and innovative solutions to navigate the impact of the pandemic. Soon, the remote communities that previously had no choice will be able to choose the services they need using immersive technologies or avail medical care remotely. However, some healthcare workers and patients could not be technologically savvy and skilled enough to understand and mitigate the risks that come with these innovations.

Additionally, the techniques developed to manage pain and provide physiotherapy and psychotherapy could potentially manipulate or cause trauma if not accompanied by appropriate education, guidance, and standards. A detailed assessment of cybersecurity, privacy, and safety-related risks to the system across the entire healthcare ecosystem is necessary. In this case, understanding the data is the first step to understanding the risks associated with various medical use cases of XR technologies.

Medical XR offers the opportunity to collect an extensive range of unprecedented data types. Some of these are not well understood and are traditionally limited to highly controlled laboratory contexts, but now will be widely available on all consumer devices and in the hands of developers with skills ranging from novice to expert, and ethical consideration left to personal experience of individuals.

Examples of data unique to XR applications include cameras and sensors that continuously capture a patient's gaze, body movements, video, and audio recordings. The collected data can be used to

derive methods for identifying an individual, health inferences, predictive algorithms, behavior data, room data, mood, gender presentation, sexual orientation, and unique physical attributes not traditionally captured during clinical interactions. If not handled carefully, health inferences or Biometrically-Inferred Data (BID)[21] can be manipulative tools or cause harm to any individual.

There remains a gap in the governance of sophisticated data collected by XR devices and processed with Artificial Intelligence (AI) algorithms. The EU Commission has proposed the first-ever legal framework on A[22]I, which addresses the risks of AI and positions Europe to play a leading role globally.

Regulatory oversight and privacy law alignment are needed to reduce the risks and realize the benefits of Medical XR globally. Therefore, current regulatory definitions of Personally Identifiable Information (PII) and Personal Health Information (PHI) need to be updated and expanded to incorporate and govern the unique types of data created and used by XR applications.

More extensive and further research is warranted in this area, and XRSI and many research partners will continue to interface directly with regulatory agencies as stakeholders to provide adequate guidance on the subject matter.

Key Messages

- With the promise of inexpensive and effective XR-based treatments, patients may be presented with an XR device as the first line of treatment, sometimes without a proper understanding of the associated risks.
- XR devices can generate and process large amounts of highly personal data, including metadata and health inferences across various geolocations. XR expands the definition of personal information that must be protected, including Biometrically-Inferred Data (BID), which is especially prevalent in XR data pipelines.
- Biometrically-Inferred Data (BID) can amplify biases. In some countries, citizens may be denied health insurance coverage based on the data attributing to pre-existing or emerging health conditions that patients may not even be aware of yet.

21 XR Safety Initiative (XRSI). (2020a, February). Biometrically-Inferred Data (BID). XRSI – XR Safety Initiative. https://xrsi.org/definition/biometrically-inferred-data-bid

22 Regulatory framework on AI | Shaping Europe's digital future. (n.d.). Digital-Strategy.ec.europa.eu. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

THEMATIC SESSION 2

Learning and Education

Education Subgroup Challenge Statement

The subgroup intended to classify biometric data, inferences, Personally Identifiable Information (PII), and non-PII data for various contexts within the practice of the education domain, such as K-12, College/University, remote training, etc., while focusing on learner safety, agency, privacy, and autonomy as the prime directive.

XR in education is emblematic of the prize and peril presented by emerging technologies. A lynchpin of defining new generations of technological adoption and acceptance - education is often seen as the model or forerunner to adopt, integrate, and explain new paradigms such as XR. Yet, it is clear that educators, students, administrations, and learning communities could face significant obstacles if they fully embrace XR consistent with privacy and security expectations while maintaining agency and autonomy in the learning process.

The pandemic and a necessity to adjust globally to remote-learning and online asynchronous communications and engagement platforms has only hastened the need for reform and magnified existing complexity in the education space by adding a layer of technical complication. However, the consensus is that, within the education domain, these issues are a potential opportunity. XR technology can be used to establish new norms and privacy frameworks that will benefit traditional "bricks and mortar" learning environments and emerging distributed classrooms or future immersive virtual learning models.

Biometrically-Inferred Data (BID) is abundant and readily available within the learning space. It is complex to determine ownership, useability, transferability, control, and data authority. Without a clear understanding, students' and teachers' rights within the education system could be undermined. Such issues are further complicated in K-12 areas where legally defined minors are involved.

Education in XR can flourish and help expedite the adoption of user populations if efforts are first made to define the guardrails necessary to classify data appropriately in this space.

Regulators must operate on policy and procedures that deliberately make accommodations that respect children's (defined as those under the age of 13) and adults' local, regional, national, and global privacy needs while also leaving room for cross-pollination and collaboration of ideas.

Key Messages

- Education in XR should first focus on the challenges of working with children - i.e., the unique difficulties in ensuring the rights of minors within the learning context.
- The adoption of immersive technologies raises moral and ethical concerns regarding human rights, access to technology, and quality of education, with a special focus on those who can't easily access these technologies. This is a fundamental issue that widens the technologic and the learning achievement gaps, and socio-economic disparities globally.
- In the U.S. educational system, Children's Online Privacy Protection Act (COPPA)[23] is over-arching and omnipresent as a consideration due to the nature of the roles and responsibilities and involvement of minors in K-12. COPPA Reform is taking place in the United States, and Metaverse-related technologies need to be part of the review and consideration as these laws are updated. Similar processes are happening in different countries.
- There is a disconnect with various ruling doctrines at different levels including state (CCPA[24], CPRA[25], VCDPA[26], CPA[27], etc.), federal (e.g., COPPA, FERPA[28]), and international (e.g., GDPR[29], PIPL[30], etc.). There is an urgent need for a global framework or a unified set of basic rules in education that align with broader policy goals.
- Data Sovereignty is a significant issue. Ownership within education is usually negotiated between parties (school and vendor, school and partner institutions, tech platform and school, etc.), assuming that the end-user has minimal rights.
- Despite regulations intended to protect students' data and educational records, existing laws (e.g., FERPA) does not say that a student – or even the academic institution – "owns" their personal data. Most big tech companies position the education institution as a processor or a data steward, responsible for data storage, security, and protection. The terms of "ownership" of other student-generated content and data are mostly spelled out between individual schools and the databases and software they buy or license. As such, there is little protection or autonomy for the individual student.

23 Federal Trade Commission. (2018, October 4). Children's Online Privacy Protection Rule ("COPPA"). Federal Trade Commission. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

24 Becerra, X. (2018, October 15). California Consumer Privacy Act (CCPA). State of California - Department of Justice - Office of the Attorney General. https://oag.ca.gov/privacy/ccpa

25 The California Privacy Rights Act. (2020). Thecpra.org. https://thecpra.org/

26 Rippy, S. (2021, March 3). Virginia passes the Consumer Data Protection Act. International Association of Privacy Professionals (IAPP). https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/

27 Consumer Privacy Act (CPA). Consumer Privacy Act. https://www.consumerprivacyact.com/

28 Family Educational Rights and Privacy Act (FERPA). (1974). https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

29 General Data Protection Regulation (GDPR). (2016). https://gdpr.eu/

30 Personal Information Protection Law of the People's Republic of China. (2021). http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm

- XRSI's program, Metaverse Reality Check (The MRC)[31], has advised Senator Ed Markey and 89 House Members on the Children and Media Research Advancement (CAMRA) Act, H.R. 1367[32], which would commission research on children's technology use and particular health outcomes, including addiction, bullying, and depression. The CAMRA Act is the first law that focuses on learning the impact of XR and emerging technologies on children. It authorizes the National Institutes of Health (NIH) to lead a research program on technology and media's effects on infants, children, and adolescents in core areas of cognitive, physical, and socio-emotional development. The law needs to be enacted as soon as possible to address the risks proactively and establish a granular understanding of data classification and age-appropriate design considerations for immersive technologies.

31 The Metaverse Reality Check (MRC): A global oversight board for and by the citizens, was established on Human Rights Day, December 10, 2021. For more information, please reference https://metaverserealitycheck.org.

32 Raskin, J. (2019, February 27). H.R.1367 - 116th Congress (2019-2020): CAMRA Act. Congress.gov. https://www.congress.gov/bill/116th-congress/house-bill/1367

THEMATIC SESSION 3

Employment and Work

Employment Subgroup Challenge statement

With the increased utility of immersive technology in the work environment, XR could provide practical solutions to many issues precipitated by the global pandemic. Organizations need to comprehend the benefits and respond to the potential threats.

Businesses are adjusting to pandemic reality and emerging market trends by accelerating their digital transformation, which includes the adoption of XR to engage employees in new and effective ways. Immersive experiences allow workers to interact in new ways that offer efficiencies. Still, businesses struggle to translate privacy and safety into the XR arena and face compounding challenges from lagging employee technical skills and the speed at which the emerging technologies paradigm unfolds, most notably the evolution to the Metaverse.

While companies benefit from improved worker communication and collaboration, streamlined training environments, reduced training costs, and higher engagement and knowledge retention, more personal data collection points may present risks and introduce ethical dilemmas. Adopting XR-related technologies has increased the dangers of massive data collection on remote workers worldwide.

Due to the more significant number of persons working from home, the employment environment expands exponentially into employee personal space (e.g., kitchen, living room, bedroom). In this context, the definition of corporate data ownership may shift beyond the employee and extend to family members, roommates, and unassuming houseguests and bystanders whose data (e.g., temperature, mood, voice, facial image, and expressions) is collected without consent or awareness.

Privacy risks are significant not only using consumer-level XR devices but also for industry-grade devices. The latest enterprise devices capture gaze, gait, and various other forms of BID via on-device

cameras and combine these data points with data collected via the Internet of Things (IoT) sensors. The challenge of protecting data becomes even more enormous when employees utilize haptics and Brain-Computer Interfaces (BCI) to perform job functions. The balance of power over employee personal data and rights could shift further in employers' favor due to XR's introduction. We need a new framework for the workplace that defines privacy and safety for employers and employees alike.

Key messages

- Privacy and security in the workplace have always been an issue. With XR, the data is highly personal and sensitive, potentially including our most intimate behaviors and thoughts. It is unlikely that employees would willingly share such data. Still, legacy laws and regulations will automatically skew in favor of organizations and likely deprive employees of rights or even the opportunity to discuss their potential rights.
- As with other technologies before XR, the legal system is far behind and playing catch up. Without clear laws on what is and is not acceptable in the virtual work environment, organizations may be asserting more rights over employee data than what is appropriate or ethical.
- Organizations should start immediately defining and communicating the type of employee data collected and how they use it. An initial step in this process is data classification to adopt and practice awareness and safe practices.
- XR is likely to widen the gap between persons with or without disabilities and perpetuate historical bias and lack of inclusivity. As XR is developed and adopted into the workplace, entities and individuals must account for these issues since it is likely impossible or complicated to adapt XR retroactively. Organizations need to hire people with disabilities and effectively support them in the workplace as doing so can contribute to a diverse workplace and improve an organization's bottom line.

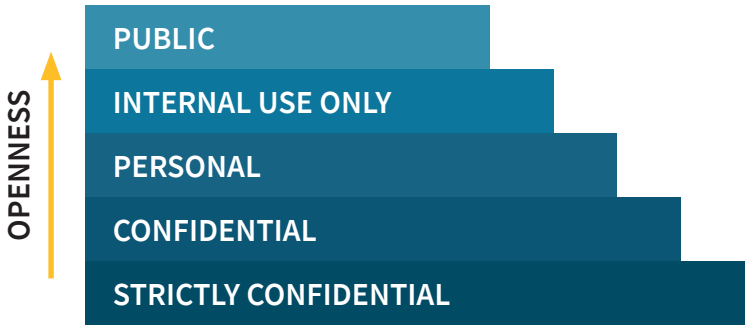
Knowing thy data

The importance of data mapping and classification

It is critical to know the organization's data and map how XR data is handled, stored, processed, transmitted, and ultimately deleted. Unlike traditional internet technologies, the next iteration of the internet, the Metaverse, can not realize its full potential without appropriate data collection. This prerequisite demands a much more thorough understanding of the contexts in which the data is collected and shared. This contextual understanding will help an entity adopt organizational and technical measures to protect personal data according to its associated and prioritized risks.

In addition to XR Data classification, the December 10 Roundtable session underlined the need to categorize data. Traditionally, a typical classification scheme for commercial organizations is composed of a hierarchy of data categories organized by their openness.

Sensitive personal information is generally afforded a higher level of protection under data protection and privacy laws. The possibility to process such data is narrower than in the case of ordinary personal data, and inappropriate handling of sensitive data can have adverse consequences for individuals or those associated with the individual.



However, this does not mean that personal data will always be less 'sensitive' than the defined categories of sensitive data. Depending on the context, personal information may be highly sensitive to an individual or capable of causing harm[33].

The traditional classification does not transfer into XR since it does not accompany sufficient context and does not provide adequate guidance and protections for the data collection and processing needed for the Metaverse. For this reason, each data point and data set needs to accompany a specific context, and appropriate guidelines need to be established globally.

The XR Data Classification Working Group will continue to host similar sessions in the future. Individuals interested in participating in the next roundtable or taking part in the XR Data Classification Working Group are encouraged to visit the website **dc.xrsi.org**.

33 Review of the Privacy Act 1988. Attorney-General's Department. https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988

Industry is starting to make strides in improving overall levels of platform safety by adopting and applying core Safety by Design principles.

We want this proactive change to be applied in the context of the Metaverse – and this time, we can also change the design ethos from moving fast and breaking things to moving thoughtfully; and moving from profits at all costs, to practices that place the safety of the user at the centre of the development process. Investments and innovation in both physical and online safety should be paramount for this new technology frontier, with governance frameworks designed to prevent and minimise potential harms.

Julie Inman Grant

Australia's eSafety Commissioner

Conclusion

Today, data collection is happening on an industrial scale. Governments, individuals, and in particular businesses hold remarkably detailed and robust information about us. With each passing day, more and more aspects of our lives are being digitally tracked, stored, used, and misused.
We demand that organizations innovating in the emerging technology domain proactively address safety and inclusivity and promote business and development models and technologies that do not undermine human rights. Knowing that emerging technologies are unfolding, including the evolution to the Metaverse, and the vast data collection will only increase and compromise our human rights and dignity, we must take action. We recommend the organizations do not trade off privacy in the name of safety such as client-side scanning on applications and devices or encryption backdoors. Instead **we recommend organization adopt privacy preserving technologies such as fully homomorphic encryption and differential privacy.**

We live in an era where regulations, policies, and standards do not adequately address privacy, safety, and inclusivity in digital and emerging technologies. We know that they will not address the Metaverse nor protect the individual or society in the era of emerging technologies. The lack of guaranteed protection in the metaverse is a global concern, just as preventing harms and ensuring the wellbeing of humans is an international and shared responsibility. **We encourage every regulatory body and government entity to follow the lead of the eSafety commissioner of Australia that has set an example and leveraged XRSI's Immersive Technology Standards[34] in creating an immersive technology positioning statement[35] to address safety and Human Rights related risks.**

We cannot express it more strongly than this. As a global community and as individuals, we have a role and responsibility to ensure human rights are embedded and protected in the metaverse. A lot of our attention is rightly focused on today's digital challenges, but we must understand and engage in that which is yet to come and is more threatening than what we have evidenced to date. **We encourage each and every individual around the globe to educate themselves and the children on potential risks and dangers associated with the immersive and emerging technologies.** Everyone has a role to play in preventing the potentially grave violations of human rights and ensuring that everyone has the opportunity to partake in this new digital age safely. We hope you will join us.

Kavya Pearlman
Founder and CEO – XR Safety Initiative (XRSI)
Chair - Human Rights Day – XR Safety Week
Founding Member - Metaverse Reality Check (The MRC)

Kristina Podnar
Global Digital Policy Advisor – XRSI
Co-chair - Human Rights Day – XR Safety Week
Executive Lead – Metaverse Reality Check (The MRC)

34 XR Safety Initiative (XRSI). (2020a, May). Immersive Technology Standards. XRSI – XR Safety Initiative. https://xrsi.org/publication/immersive-technology-standards

35 eSafety Commissioner. Government of Australia. Immersive technologies – position statement. https://www.esafety.gov.au/industry/tech-trends-and-challenges/immersive-tech

About XR Safety Initiative (XRSI)

XR Safety Initiative (XRSI) is a 501(c)(3) worldwide not-for-profit **Standards Developing Organization (SDO)** that promotes privacy, security, and ethics in immersive environments. XRSI's mission is to help build safe and inclusive experiences so that XR stakeholders can make informed and pragmatic decisions. XRSI does this by discovering novel cybersecurity, privacy, and ethical risks and proposing potential new solutions to mitigate them.

XRSI, being the first such global effort, is uniquely positioned to provide impartial, practical information about XR and Metaverse-related risks and opportunities to individuals, corporations, universities, government agencies, and other organizations worldwide.

XRSI launched the first novel **XRSI Privacy Framework for the XR domain** to address the impact of Biometric Inferences via Special Data Type consideration. The framework has been well received and has been a point of discussion among XR stakeholders and many regulatory entities worldwide. XRSI is currently working on Medical XR and Child Safety frameworks for addressing Privacy and Safety Issues in the Metaverse.

Since 2019, XRSI has created various programs focusing on the most critical aspects of the immersive domain, such as **Medical XR** (Medical XR Advisory Council), **Child Safety** (Child Safety Initiative), **Diversity and Inclusion** (CyberXR Coalition), **Storytelling and Awareness** (Ready Hacker One), and recently launched the **Metaverse Reality Check** (The MRC), an oversight board by and for the citizens.

XRSI's PRINCIPLES

HUMAN RIGHTS
SUPPORT STATEMENTS

Digital Rights are human rights and we will uphold them for all digital ecosystems while helping guide global citizens to safely navigate these emerging digital ecosystems.

Kavya Pearlman
Founder and CEO – XR Safety Initiative (XRSI)

Digital technologies already deliver many benefits and their value to citizens and society is enormous. But we cannot ignore the risks and the dark side. The digital revolution is already a major global human rights issue, immersive realities will only highlight challenges further, and the unquestionable benefits that we are starting to see do not cancel out its unmistakable risks. We will foster dialogue around the risks and opportunities that digital represents, advise citizens, entities, and governments to ensure that we can safely navigate this new era in a way that is sustainable for all.

Kristina Podnar
Global Digital Policy Advisor – XRSI
Co-chair - Human Rights Day – XR Safety Week
Executive Lead – Metaverse Reality Check (The MRC)

Digital Patient safety, right to privacy, autonomy, and inclusion are critical to healthcare and we will uphold these rights as human rights for all in reality and XR.

Ryan Cameron
CEO, Electric Puppets
Co-Chair, Medical XR Council by XRSI

Like human rights, digital rights must be universal, inalienable, and guaranteed across all present and future digital ecosystems. Digital privacy, safety, and control over one's data are fundamental rights that no human can be deprived of upon accessing a digital world or platform.

Didier Contis

We stand with XRSI and the international community in declaring our pledge to be a standards barrier for responsible innovation, safety, privacy, inclusivity, and acceptance for all who wish to be denizens of a better tomorrow.

Matthew Price, PhD
Reality Science, LLC

This Human Rights Day it has never been more important to protect our human rights as we see see those who seek to erode them. The metaverse offers a chance to build new human rights but we must remain vigilant to uphold those fragile, precious rights in the digital realm.

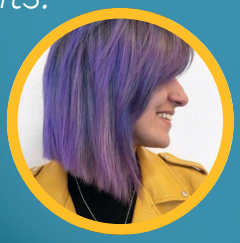
Richard Price
Global Health Education Technology Advisor , Health Education England (NHS)

As it stands, the technological innovation over the last half century has collectively and systematically reinforced existing wealth distributions and restricted opportunities for social mobility.
The autonomous and intelligent infrastructure that supports spatial computing brings deeply unexamined avenues for the collection, analysis, and exploitation of user generated data; as well as raising ethical and responsibility questions around the ownership of biometric data.
As scientists, engineers, and creators; we are, ultimately, not just handling a technology; but people. And as such, it is important to contextualize all that we do inside a responsible research and innovation framework. Users are people; and it is important to uphold that all people have the right to autonomy, expression, privacy, and safety so that we may to move from an understanding of human-computer interaction to humane innovation that supports each individual's right to prosperity.

Sophia Batchelor
Post Graduate Researcher, Center for Immersive Technologies

When we talk about digital rights in XR and the Metaverse(s) as a new domain, we risk losing the lessons learned from Internet governance and artificial intelligence ethics research, as well as the rights conquered along the way. Immersive reality is more of a problem of magnitude and convergence, amplifying already existing bias, mental privacy, lack of inclusion and self-determination challenges in our digital society.

Augmented reality demands augmented human rights.



Micaela Mantegna
Affiliate. Video games and XR policy,
Berkman Klein Center for Technology & Society, Harvard University.

It is vital that we consider digital rights as a human rights issue since too many in the world still lack the capabilities to have digital access and data agency. Immersive environments create many opportunities if everyone can benefit. This is issue of our time, and how we respond to it now, will shape our future.

Debbie Reynold
CEO and Chief Data Privacy Officer
Debbie Reynolds Consulting LLC

Privacy is one such human right, and relinquishing it should not be a requirement to use technology or enter an immersive ecosystem.

Brendan David-John
Ph.D. Candidate

Human rights in the Metaverse will be recognized only when individuals are able to safely & securely maintain autonomy, privacy, and a right to informational transparency & knowledge sharing in all matters that would impact or impede the pursuit of their own well-being. Meta-social codes of conduct will determine behavioral incentives that motivate the pursuit of safe, welcoming environments as well as hostile, risk-seeking ones. Professional ethics of designers, developers, moderators and platform providers will eclipse the scope of responsibility & impact of today's public safety officers, educators, and healthcare providers. It is within their duty to inform the public, collaborate with reality-based stakeholders, and maintain cultures of iterative improvement that protect the physical rights of human beings in their pursuit of dignity, safety, education & health, both in the physical & virtual realm.

Laura E. Brown
Education Policy, Research & Design Consultant

Naturally, human rights exist in all domains. The metaverse has the potential to infringe on rights that are not in the typically foremost in the minds of product developers.
Specifically, the connection and awareness of ourselves as bodies is vital to our physical and mental well-being. The cost of persistent alienation from our physical selves should be acknowledged as technology is developed.
The freedom to develop our worldview without others holding a monetary interest in that process.
The right to mental well-being.
There is a duty of care to develop products with the overall well-being of users in mind from the outset.

Jonathan Lewis
Purpose Loves Company

As the metaverse expands, the line separating the 'real world' and the digital one become increasingly blurred, and one day may cease to exist altogether. Harms occurred in the digital space are not confined to that space, but may echo and bleed into the 'real' world. Thus, it is of utmost importance to uphold human rights in this digital domain, so as to ensure people are safe and can thrive in these ecosystems.

Abraham Mhaidli
Ph.D. Candidate

As we seek to create a set of interconnected parallel worlds with all and more of the capabilities for human interaction we enjoy in the physical world, we must also consider and safeguard those human rights we enjoy here. These must be locked in and protected from the outset and for as long as we choose to inhabit these digital worlds.

David W. Sime
Riiot Digital Ltd.

Human rights must be foundational to everyone's access and use of digital technologies. The Metaverse brings a new set of challenges to ensure these rights are sustained - and expand - to ensure safety in this rapidly evolving space.

Damien Weldon
Founder & President, The Molybdenum

This report was edited and published by the XR Safety Initiative (XRSI), based on the **1st XR Data Classification Roundtable** that happened during the XR Safety Week 2021 on **73rd Human Rights Day – December 10th, 2021**

www.dc.xrsi.org

Organizations Represented

US Department of Veterans Affairs, Meta Inc., HP Inc., Microsoft, EFF, Access Now, Office of the eSafety Commissioner, IEEE, Mozilla, AARP, NHSX, National Institutes of Health, Health Education England, European Research Executive Agency established by the European Commission, Bipartisan Policy Center, Stanford University, Arizona State University, Trinity College Dublin, Georgia Institute of Technology (Georgia Tech), University of Canterbury, Dartmouth College, Goethe University Frankfurt, University of Leeds, University of Michigan, University of California, Irvine, University of Florida, University of New Haven, University of Washington, UC San Diego / Design Lab, Slingshot Simulations Ltd., Glocal Studios, The Molybdenum, Cognitive3D, Purpose Loves Company, Bowmara, YouTheData.com, Valo Health, Inc., Noboxes/SSH, RealityScience, LLC, Between Five And Nine LLC, BehaVR LLC, Realities Centre, MedVR Bootcamp and Incubator, Debbie Reynolds Consulting LLC, OviSquare, PNI Therapeutics, XRSI / NativeTrust Consulting, LLC / The Cantellus Group, Berkman Klein Center // Women in Games Argentina, Chaos Computer Club, Identity Woman & HumanFirst.Tech, Brookings, MKAI – The inclusive AI Community, Luxsonic Technologies Inc., Games4Change.

Hosted by

Supported by