XR Safety Initiative
www.xrsi.org

THE XRSI PRIVACY FRAMEWORK

version 1.0

September, 2020

Liaison Organizations

OPEN AR CLOUD

CENTER FOR ACADEMIC INNOVATION
UNIVERSITY OF MICHIGAN

Georgia Tech

Abstract

The XR Safety Initiative (XRSI) develops and promotes a fundamental understanding the impact of accessibility, inclusion and trust on privacy in XR environments by providing technical leadership in the XR and spatial computing domain. XRSI develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and responsible use of immersive technology.

XRSI's responsibilities include the development of technical, physical, administrative, safety and privacy standards, framework and guidelines for the human-centric privacy by design and development in XR and Spatial Computing environments. This Novel XRSI Privacy Framework provides a baseline approach to research, guidance, design, development, and thought leadership for privacy.

The ultimate goal is to create transparency, inclusion and awareness to enhance accountability and trust in spatial computing and XR ecosystems by providing concrete guidance to public-private industries, governments, and academic organizations. Based on the available information curated, the current understanding of these topics will continue to refine and evolve.

Acknowledgments

The founder of The XR Safety Initiative, Kavya Pearlman, would like to thank the many experts in the industry, governments, and academia who contributed their thoughts to the creation and review of this document. We especially acknowledge our liaison organizations (Open AR Cloud, University of Michigan - Center for Academic Innovation, and Georgia Institute of Technology), for the technical insight and active contribution in this effort.

- Kavya Pearlman | *Founder & CEO – XR Safety Initiative (XRSI)*
- Marco Magnano | *Journalist; Exec. Director of Communications – XR Safety Initiative (XRSI)*
- April Boyd-Noronha | *Global D&I Advisor – XR Safety Initiative (XRSI); Exec. Lead – The Cyber XR Coalition*
- Alina Kadlubsky | *Director of Communication – Open AR Cloud (OARC); Chair – The Cyber XR Coalition*
- Dr. Ryan Wegner | *Founder at Cyntient Inc., Advisor – XR Safety Initiative (XRSI)*
- David Clarke | *EU-GDPR Strategy Advisor – XR Safety Initiative (XRSI)*
- Tamas Henning | *Trust and Safety Advisor – XR Safety Initiative (XRSI)*
- Maria Tamellini | *Co-founder & COO – GamerSafer; Child Safety Advisor – XR Safety Initiative (XRSI)*
- Steve Peters | *Immersive Experience/Game Designer; Geoprivacy & Spatial Computing Advisor – XR Safety Initiative (XRSI)*
- Brian D. Wassom | *Partner, Warner Norcross + Judd LLP; Advisor – XR Safety Initiative (XRSI)*
- Joel Scharlat | *Director of Operations – Cyber Bytes Foundation; Advisor – XR Safety Initiative (XRSI)*
- Ross Newman | *Global AI Advisor – XR Safety Initiative (XRSI)*
- Ibrahim "Abe" Baggili, Ph.D. | *Co-Founder – XR Safety Initiative (XRSI)*
- Dennis Bonilla | *Co-Founder – Baltu Technologies Inc; Advisor – XR Safety Initiative (XRSI)*
- Muki Kulhan | *Media Consultant; Founding Member – The Cyber XR Coalition*
- Vandana Verma Sehgal | *President – InfosecGirls; Founding Member – The Cyber XR Coalition*
- Jeremy Nelson | *Director, XR Initiative (XRI) – Center for Academic Innovation, University of Michigan*
- Richard LaFosse | *Compliance and Policy Lead – Center for Academic Innovation, University of Michigan*
- Macey Miller | *Compliance Fellow – Center for Academic Innovation, University of Michigan*
- Didier Contis | *Interim Associate Vice President for Data Strategy and Analytics – Georgia Institute of Technology*
- Noble Ackerson | *Senior Product Manager – Ventera Corporation*
- Jan-Erik Vinje | *Managing Director – Open AR Cloud (OARC)*
- Colin Steinmann | *Director of Operations – Open AR Cloud (OARC)*
- Marco Tillmann | *Product Manager, Spatial Computing, 2D/3D Visuals – HERE Technologies*
- Luis Bravo Martins | *Head of Marketing – NEXT Reality*
- Ben Erwin | *Director - Silicon Harlem XR Programs and Annual Conference; Owner – PowerSimple LLC*
- Christiane Lesch | *Managing Director – XR World Academy*
- Debbie Reynolds "The Data Diva" | *Founder, CEO, and Chief Data Privacy Officer – Debbie Reynolds Consulting, LLC*
- Joseph Jerome | *Lawyer and Privacy Consultant*
- Zoe Braiterman | *Consultant/Researcher*
- Alexandria Heston | *UX Designer – Niantic Inc.*

Credits
Illustrations: Leonora Camusso - www.leonoracamusso.it
Editing: Kelly J. Cooper - www.kjcedits.com

Table of contents

Executive Summary

Spatial Computing and Extended Reality technologies provide a bridge that combines hardware, software, people, places, and information via head-mounted display (HMD), from digital contact lenses to haptic wearables, IoT devices, sensors, robots, autonomous vehicles, and beyond. If we think that Web 2.0 took the world by storm, emerging technologies such as XR and Spatial Computing will transform the way humans connect, create, do commerce, and heal. While this technological shift expands our capabilities and increases our potential, impacting every aspect of the economy, our culture, and our lives, it also creates deeper societal and privacy concerns.

Spatial Computing versus Extended Reality (XR)

Spatial Computing is an umbrella term that refers to the type of interaction we have with reality more than to a specific technology. The expression puts function over form, related to the use of the space around us as a medium to interact with technology. Spatial Computing defines a human-machine interaction in which the machine retains and manipulates referents to real objects and spaces. Spatial Computing differs from related fields such as 3D modeling and digital design as it requires the forms and spaces it deals with to pre-exist and have real-world valence. It is not enough that the screen represents a virtual space—it must be meaningfully related to an actual physical place.

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 broad spectrum of hardware and software, including sensory interfaces, applications, and infrastructures. XR is often referred to as immersive video content, enhanced media experiences, and interactive and multi-dimensional human experiences.

The benefits of extending realities and building mirror worlds are fueled by massive amounts of data that flow through a complex ecosystem. Individuals and organizations are currently not fully aware of the irreversible and unintended consequences of XR on the digital and physical world. With the mass adoption of emerging technologies, it is imperative to understand the privacy and safety concerns and proactively address them.

This framework by the XR Safety Initiative (XRSI) provides a baseline approach to enable better engineering practices that support privacy by design concepts and help organizations protect individuals' privacy. The framework is the work of several interdisciplinary experts and serves as a tool for improving privacy through human-centric design, pragmatic decision making, and proactive risk management.

This privacy framework's foundation is based on the goals The Cyber XR Coalition adopted and outlined in the "Immersive Standards for Accessibility Ethics, Inclusion and Safety 1.0,"[1] which are:

1. **Leave no one behind**
2. **Be accessible**
   Everyone must be able to participate in the digital society
3. **Protect identities**
   Users must be able to participate in the digital society no matter their gender, ethnicity, birthplace, or cultural and political beliefs, ensuring discrimination and biases are mitigated and not further reinforced
4. **Keep everyone safe and secure**
   Shape rules and practices to enable a secure and resilient immersive environment
5. **Build new rules to promote trust**
   Develop new, flexible, participatory governance mechanisms to complement traditional policy and regulation in a domain that's in constant evolution

Addressing privacy in the uncharted territories of emerging technologies allows us to drive critical benefits from the data while simultaneously building trust that will ultimately define these emerging domains' success. When it comes to individual privacy in Spatial Computing and XR, the industry is in dire need of clear and specific guidance, which this framework provides. This framework supports individual privacy rights, choices, and expectations by taking a conservative baseline approach to layout and design choices and relying on a well-engineered foundation.

The **XRSI Privacy Framework** is flexible and addresses diverse privacy needs. It enables more innovative and effective solutions that can lead to better outcomes for individuals and organizations. It also incorporates the impact and cross-section of other emerging technologies, such as artificial intelligence (AI), 5G, 6G, and Brain-Computer Interface (BCI).

In the past decade, we have seen an increase in data privacy laws. The news headlines are full of companies and governments misusing data and losing trust because of it. In the post-COVID world, where extending realities via virtual and augmented technologies is the new normal, organizations must take privacy and compliance much more seriously. Massive amounts of data fuel humanity's journey into the uncharted territories of Spatial Computing and XR. In order to make this journey safe both in terms of our embodied self and our interaction with other humans, extreme caution must be taken while handling personal and sensitive data. Compared to the personal data already collected by large technology organizations, XR datasets contain much more personal and sensitive information about individuals and impact communities in far greater depth.

Spatial Computing and XR technologies empower us to enjoy experiences and applications never before possible by collecting precise data about the environment and how the user interacts with it, using sensors and on-device tracking mechanisms. However, the most significant challenge lies in addressing how that data is collected, processed, stored, and destroyed safely and ethically.

Achieving privacy in Spatial Computing and XR is challenging because the technology itself is rendered useless without the appropriate data collection. The privacy laws are ever-evolving, although still catching up to the exponential growth in the immersive technology domain. While privacy itself is a human rights challenge that can help safeguard essential values such as human autonomy and dignity, immersive technologies require us to understand and manage risks in a manner that prevents harm to individual values and society.

1 *http://www.cyberxr.org/xr-standards*

The **XRSI Privacy Framework** is the necessary component that empowers individuals and organizations with a common language and a practical tool that is flexible enough to address diverse privacy needs and is understood by technical and non-technical audiences. This framework draws a baseline, offering solution-based controls that have principles like "privacy by design" and "privacy by default" baked in, driven by trust, transparency, accountability, and human-centric design.

1.0 The XRSI Privacy Framework

1.1 Overview

1.1.2 What is The XRSI Privacy Framework?

The XRSI Privacy Framework is a free, globally-accessible baseline rulebook curated by the XR Safety Initiative (XRSI). It has a layered structure that outlines the focus areas that act as a set of functions within a system and how they interrelate to achieve privacy. It includes standardized subcategories and a corresponding set of privacy controls for the Spatial Computing and XR domain. The framework creates a baseline set of standards, guidelines, and best practices that are regulation-agnostic. It includes privacy requirements drawn from the General Data Protection Regulations (GDPR), National Institute of Standards and Technology (NIST) guidance, Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy Protection Rule (COPPA)[1], and a few other evolving laws. But it is designed to adapt to include new requirements as new regulations come into effect. The XRSI Privacy Framework helps organizations define their privacy goals, identify privacy risks, and optimize the use of personal and sensitive information while limiting privacy violations. The framework is not a law or standard; it is a free tool that is continuously evolving.

1.1.3 Components of the the XRSI Privacy Framework

As shown in *Figure 1*, the Privacy Framework is composed of three parts: Focus Areas, Set of Function, and granular controls. Each component reinforces how organizations achieve privacy goals through aligning business strategy, roles and responsibilities, and activities to prevent harm to humans in Spatial Computing and XR environments.

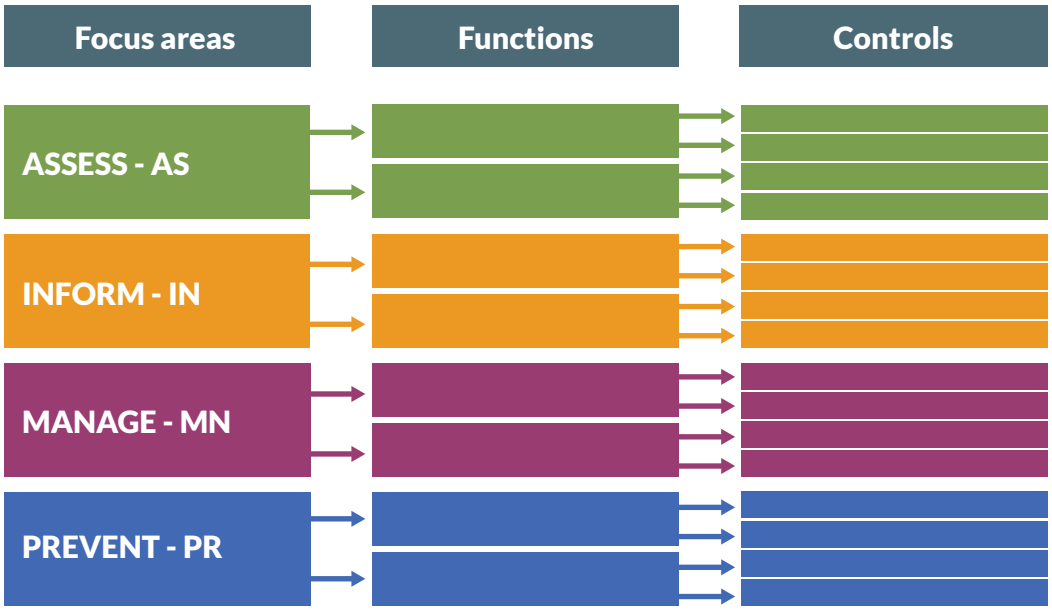

Figure 1: Components of the XRSI Privacy Framework

1 *For more details, see Section 3.0*

Focus Areas
The Focus Areas provide a foundation for outlining the scope of work that enables Spatial Computing and XR organizations to incorporate privacy by design and default into their business practices and development.

Functions
Functions are the subcategories for outlining groups of privacy-focused activities tied to Focus Areas and the subsequent granular controls.

Controls
Controls are the activities that are carried out to achieve specific privacy outcomes about business operations. They provide a set of results and help support the achievement of the intended outcome in each of the Focus Areas.
Within the XRSI Privacy Framework , four areas of work have been identified to achieve the goals described above. The first area of work—**assess**—is one of the four foundational focus areas for assessing privacy risks to build inclusive, safe, and private XR systems for all. The second and third areas—**inform** and **manage**—collectively address organizations' capacity to build trust by informing individuals and managing privacy risks within the ecosystems. The fourth focus area—**prevent**—enhances safety by outlining preventative controls needed for safety and privacy within the Spatial Computing and XR ecosystems. The four areas of work identified here will inevitably intersect with each other and therefore remain interdependent. For example, we cannot prevent or manage risks that we have not yet assessed. Likewise, we can only inform individuals about privacy-related information and risks once they are understood, requiring a risk assessment.

1.2 Privacy Expectations and the XRSI Privacy Framework

While understanding user privacy expectations is challenging, it is significantly more critical in immersive technologies. The expectations in immersive environments can serve as the basis for a layered approach to privacy in creating a safe and trustworthy experience. Inspired by the Consumer Satisfaction/ Dissatisfaction (CS/D) and service quality domains, and based on individual expectations, information and data privacy information are a multi-level construct. The three levels of privacy expectations outlined within the XRSI Privacy Framework are:

Minimum: The Minimum level is what people would tolerate if something must happen; something is essential to fulfilling a need, and there is not much choice. Here "must" indicates a more substantial obligation than "should" or "ought." The Minimum level is determined by a lack of options and driven by legal compliance mandates.

Desired: Compared to the other levels, the Desired level has an affective dimension that focuses on feelings. The Desired level is what people feel should or ought to happen, given their investment. Here, the investment can be in terms of time, effort, money, loyalty, etc.

Ideal: The Ideal level is what people ideally want to happen. It is similar to the desired level of privacy. The desired level of privacy is an ideal internal state at any moment, and people evaluate the achieved level of privacy against the desired level of privacy.[2]

2 *https://www.frontiersin.org/articles/10.3389/fdata.2020.00007/full*

1.3 How to Use the XRSI Privacy Framework

The XRSI Privacy Framework—a voluntary tool for managing privacy risks in Spatial Computing and XR—is intended to serve organizations of all sizes conducting business in those domains. The XRSI Privacy Framework was inspired by the NIST privacy framework's approach and was strategically designed to be compatible with existing U.S.-based and international legal and regulatory regimes and usable by any type of organization to enable widespread adoption. It explicitly considers key regulations such as GDPR, CCPA, COPPA, FERPA, and a few others, as previously mentioned.

The XRSI Privacy Framework's purpose is to help Spatial Computing and XR organizations manage privacy risks by:

- Making privacy a priority and outlining how to consider it during planning, designing, building, deploying, operating, decommissioning, and deploying the systems, products, services, and XR experiences affecting an individual's privacy.
- Communicating both internally and externally about the privacy risks and overall practices via cross-organizational collaboration.

When used as a risk management tool, the XRSI Privacy Framework can help an organization build trust, achieve transparency, and create accountability during development and innovation while minimizing unintended consequences for individuals. The XRSI Privacy Framework can help Spatial Computing, and XR organizations assess the scope of their impact on individual privacy rights, facilitate those rights, and potentially comply with various international and state regulations.
While addressing a Spatial Computing and XR organization's privacy needs, the XRSI Privacy Framework remains flexible, complements existing business models, and leaves its application decision to the organization itself. For example, a large organization may already have a robust privacy program and sound risk management processes. Still, it may use the framework to analyze novel privacy and safety risks that the introduction of Spatial Computing and XR may create. Likewise, a small-to-medium organization without a privacy program can use the Focus Areas and Functions as a reference to understand and communicate privacy needs and expectations to its stakeholders. Organizations can also use the XRSI Privacy Framework to understand their responsibility toward individual privacy while building an experience, application, or platform.

There are many ways organizations can use the XRSI Privacy Framework. Caution must be taken when using it as a compliance tool because that is not its function. There is no inherent expectation for companies to "comply with the XRSI Privacy Framework." Instead, they should use it as the baseline measure to optimize privacy efforts in minimizing risks within the Spatial Computing and XR data processing ecosystem. At its best, the XRSI Privacy Framework intends to create accountability in the immersive domain.

1.4 ASSESS (AS) – Privacy Risk Assessment

By their nature, XR applications are very multi-modal and often use the full suite of sensors available on a given XR-enabled device. For instance, AR frameworks often use data from a mobile device's camera, analyzed together with the data from the gyroscope and the acceleration sensor to determine the device's position in space. Each data set a company collects comes with complications. First, it's essential to assess what data is required to facilitate the experience and then evaluate what data needs to be stored.

1.4.1 Assessment and Mapping

Data processing by systems, products, and/or services is understood and informs the management of privacy risk.

While scanning the environment and mapping, organizations should assess and understand how the XR device/platform/service collects and uses mapping information.

- Shared mapping functionality should be opt-in.
- Users should be able to designate private maps and have the option to delete them, e.g., inside private residences.
- The mapping data should be interoperable. Individuals should be able to download and export mapping information to other XR platforms.

Under article 25 of the GDPR, as part of the principles of privacy by default and by design, products/services must be designed and developed to protect user's personal data by default. In particular, given "the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing" (GDPR, article 25(1)[3]) of a large scale of biometric data due to the use of XR, XR providers shall:

- Both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization and/or data minimization, to meet the GDPR's requirements and protect the rights of data subjects, and to ensure that only personal data that are necessary for each specific purpose of the processing are processed;
- Before the processing, assess the impact of the envisaged processing operations on the protection of personal data, under article 35 of GDPR[4] (Data protection impact assessment—"DPIA").

3 *https://gdpr-text.com/read/article-25/*
4 *https://gdpr-info.eu/art-35-gdpr/*

1.4.2 Risk Assessment

Privacy risks related to individuals are assessed to determine the impact on organizational operations, mission, and functions while taking into account other risk factors, including human, societal, informational, and financial risks.

While performing a risk assessment for Spatial Computing and XR ecosystems, the following questions can help organizations assess their privacy data exposure vulnerabilities.

- What are the various types of data required by the XR platform, service, or app?
- What are the various types of data being collected, processed, and shared?
- What is the legal basis for storing personal and sensitive XR data?
- Which third parties will the data be shared with and how will they be processing the data?
- What processes are in place to communicate to customers, collaborators, and regulators what data is being collected and why?
- What processes are in place to ensure the data is stored securely?
- What processes are in place for responding to a data breach or any privacy incident in a timely manner?
- What is the data collection pipeline?
    - What is collected by the device?
    - What is stored locally on the device?
    - What data is shared with:
    - Other users?
    - Third-party applications?
    - Other companies?
- What data is stored?
    - On-device?
    - Distributed to other users?
    - On an edge cloud?
    - On a remote cloud?
    - How long will the data be retained?
    - Will the personal and sensitive XR data be encrypted, de-identified, obfuscated, and/or aggregated when storing or processing?

1.5 INFORM (IN) – Informing Users about Privacy Risks

Informing individuals and organizations about privacy risks should begin by first understanding their privacy needs and expectations. Privacy needs can be derived from individuals' legal privacy rights, whereas the context and choice can be communicated by understanding privacy expectations.

1.5.1 Privacy Policies

Privacy disclosures are essential to XR, providing insight and transparency into what information is being collected by XR devices and how this information is being used. The organizations should recognize that legally-mandated "privacy policies" are not sufficient to inform users about (1) how do the organizations affirmatively protect privacy and (2) how do the organizations use (or may use at a later stage) personal and sensitive XR data, including biometrically-inferred data.

Minimum Expectation: The organizations should have legally-compliant privacy policies.

- Design privacy policies to provide individuals with information about what information is collected from them, how it is collected and used, who it is shared with, how it is protected, and what control they have over this information.
- Provide disclosures that satisfy CCPA and GDPR requirements.
- Provide disclosures and records of processing that satisfy sectoral privacy laws.

Desired Expectation: Organizations should include layered, just-in-time, and other contextual privacy communications.

- Provide just-in-time disclosures to individuals and obtain their affirmatively expressed consent before allowing systems and applications to access personal and sensitive data.
- Provide just-in-time disclosures and obtain affirmative express consent where biometrically-inferred data is being processed and could put individual safety at risk.
- Develop a one-stop "dashboard" approach to allow individuals to review the types of content accessed by their applications.
- Use standard icons and visuals to depict the transmission of user data.
- Promote privacy best practices internally. For example, an organization can reasonably enforce privacy requirements by educating application developers.
- Provide individuals with clear disclosures about the extent to which an organization reviews applications prior to making them available for use and conduct compliance checks, audit, and review once the application is in use.

Ideal Expectations: Organizations should provide clear indications to bystanders or other XR users through visual or audio indicators when data is being collected and recorded.

- If a Spatial Computing or XR session is being recorded, organizations should ensure the individuals impacted are aware of it and the communication of the risks is clear.
- If information in Spatial Computing or XR environment is being recorded, organizations should ensure this information can be communicated to bystanders or otherwise detectable by third parties. Similar examples exist in other technology domains, such as:
- Requiring Unmanned Aerial Vehicles (UAVs) to "broadcast" a license plate that can be viewed and monitored by third parties, so they know who is operating UAVs in their immediate vicinity.
- Developing IoT personal assistants that inform individuals about the surrounding technologies and the kind of personal and sensitive data they collect as well as the risks associated with it[5].

5 *https://cylab.cmu.edu/news/2020/02/19-privacy-assistant.html*

1.5.2 Consent

Consent is generally considered as a valid legal basis for the processing of biometric data. In order to ensure that valid permission has been granted, it is necessary to assess whether it was freely given. In this respect, consent could be considered as not freely given where a valid alternative to the processing of biometric data and biometrically inferred data is not provided. In this regard, it is noteworthy that a data subject may have a different perception of privacy in a XR context (so-called "virtual privacy") than in a non-XR context, and that such "lower" privacy perception could also cause a reliance on less sustainable consent propositions. Consent might not be considered as freely given if the provision of an XR service:

1. …is strictly bound to the processing of biometric and biometrically-inferred data (without any valid alternative for the data subjects);
2. …is conditional on consent to the processing of personal data that is not necessary for the performance of that service (see Article 7(4) GDPR).[6]

Most of the abovementioned biometric data certainly appear to be required for enabling the use and availability of XR services, but there might be a question over whether subjects have a "real choice" to refuse the processing and whether it is possible to draw the line between necessary and unnecessary data.

1.5.3 Context

Communicate clearly, transparently, and effectively to empower individuals in making informed decisions about how their data is processed as well as what kind of risks may be associated with such data processing.

1. Responsibility lies in the hands of the organizations and the end-user individual.
2. Cognitive load for users: Users bear the responsibility of understanding how their data will be used so that they can have the choice to provide their consent without confusion. Due to the cognitive load, end-users tend to ignore reading terms of use that are often verbose and stand in the way of using the tool.
3. Organizations, when designing for context about what data you intend to use—along with why, when, how, with whom, and where you intend to use it so that your individuals are informed and empowered—should be able to make informed decisions about how their data are processed. The organization must present information that is clear, accessible, accurate, and timely.

1.5.4 Choice

Establish mechanisms to facilitate individual privacy rights in a manner that offers multiple avenues to make risk-based and informed decisions around the collection and processing of data.
Spatial Computing and XR organizations gather more personally identifiable information about an individual than any other prior technology. Being more immersive, the justifiable gathering of an individual's data means you offer the user timely and relevant information as they engage and offer a choice mechanism (such as progressive disclosure, an interaction design pattern that sequences information and actions across several steps, helping users manage the complexity) to allow the user to provide additional consent or revoke access without breaking the experience;

1.5.5 Control

Build accessible and intuitive mechanisms to allow individuals the ability to own data rights and management.

- Individuals have been subject to dark patterns[7] through the user experience of traditional applications.
- Understanding an individual's desired outcomes should be considered a success measure.
- Measuring the effectiveness of your individuals' desired outcomes in protecting their data is essential to achieve the trust of your users.

6 *https://gdpr-info.eu/art-7-gdpr/*
7 *https://arxiv.org/pdf/1907.07032.pdf*

1.5.6 Child Safety

Policies and procedures must account for additional requirements and facilitate controls when processing and/or collecting data associated with minors.

XR providers must implement adequate procedures and security measures to protect children's data (minors constitute a wide portion of increasingly sophisticated and tech-savvy gamers). Children need particular protection when data controllers are collecting and processing their personal data because they are traditionally less aware of the risks involved in the processing of their data. XR providers should protect minors from the very beginning of their use of XR technologies, designing and implementing such technologies in compliance with the strict privacy by design and by default principles. From a practical standpoint, it is often difficult to ascertain whether an XR user is a child and, for instance, valid parental consent has been given. XR providers should accordingly review the steps they are taking to protect children's data on a regular basis and consider whether they can implement more effective verification mechanisms, other than relying upon simple consent mechanisms.

Age-Appropriate Design

Our recommendations for child privacy and safety in XR experiences were based on the Age Appropriate Design Code (AADC) published by the UK Information Commissioner's Office (ICO).[8] Considering the maturity levels and needs of child users are key elements to safeguard them. This also applies to processing their personal data. According to AADC recommendations, the focus for this guide is to protect children under the age of 18 years old. The correlation between children's overall development and attitudes toward risks is a critical factor to safeguarding them in immersive or augmented worlds.

Age recommendation for immersive experiences

Recommendation for parents: follow headset manufacturers recommendations.

The lack of data about long-term exposure consequences of continuous use of devices for younger children naturally raises concerns about this audience. It's important always to observe the headset manufacturer usage recommendations (most of them position their products for 12 or 13+ audiences). Key areas of concern are the content nature (of both content itself and its intensity) and the user exposure (duration and frequency).

8 *Age appropriate Design: A code of practice for online services (2020), https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/*

1.6 MANAGE (MN) – Privacy Risk Management

Organizations should manage privacy risk by establishing mitigating controls such as reasonable data security protections; taking into account the costs of available security controls and tools; the sophistication and size of the company; and sensitivity of the associated personal and XR data.

1.6.1 Awareness and Training

The organization's workforce and third parties engaged in data processing should be provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, agreements, and organizational privacy values.

1.6.2 Monitoring and Review

The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.

1.6.3 Data Disclosures (Breach Notification)

Data breach notification requirements were designed to empower consumers and shame companies into improving their data security practices. The precise contours of when/where/how users must be informed varies widely based on jurisdiction.

- **Minimum Expectations:** Organizations should review what their jurisdiction's laws are. Most jurisdictions have laws and regulations in place that apply to "personal data breaches" or other security incidents.
    - California's evolving breach notification rules may serve as a baseline of what notification is required.[9]
    - The UK ICO has guidance on the GDPR's breach notification rules.[10]
- **Desired Expectations:** Organizations should put in place processes and procedures for managing breaches and vulnerabilities. Organizations should establish mechanisms/procedures/policies to address:
    1. Steps to take;
    2. Parties to contact in the event of a breach.[11]
- **Ideal Expectations:** Organizations should communicate the details of the incident, remediation steps, and how it intends to improve privacy and security moving forward.
    1. Provide disclosures and explain to individuals impacted what procedures and technologies are used to secure their information.
    2. Consider undertaking independent security audits and releasing this information to the public.

1.6.4 Data Processing Ecosystem Risk Management

The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, manage, and protect individuals' privacy, increase manageability, and implement privacy principles (e.g., individual participation, data quality, and data minimization).

9 *https://oag.ca.gov/privacy/databreach/reporting*
10 *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/*
11 *FTC Data Breach Guidance: https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business*

1.6.5 Special Data Type Consideration

The organization has established and implemented the processes to identify, assess, and manage privacy risks related to special data types. The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support risk decisions associated with sensitive data that may put humans at risk.

Biometrically-inferred data (BID) are a collection of datasets that are the result of information inferred from behavioral, physical, and psychological biometric identification techniques and other nonverbal communication methods. Prime examples of biometric identification techniques that potentially contribute to BID are:

- Facial recognition;
- Dactyloscopic data (fingerprint verification);
- Iris scanning;
- Retinal analysis;
- Voice recognition;
- Ear shape recognition;
- Keystroke analysis;
- Handwritten signature analysis;
- Gait analysis;
- Gaze analysis (eye-tracking).

XR technologies collect body-tracking data (which are part of our deep-seated identity data) by means of eye-tracking systems, facial recognition systems, and advanced sensors (e.g., fingerprints, voiceprints, hand and face geometry detection, electrical muscle activity, heart rate, skin response, eye movement detection, head position, etc.) to provide an immersive and comfortable experience for users. Such data are identifiable as biometric data, i.e., under article 4(14) of the GDPR[12], "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data." According to article 9 of GDPR[13], their processing requires special attention as they are considered a special category of personal data. In particular the GDPR provides that the processing of biometric data (for the purpose of uniquely identifying a natural person)—except for some limited purposes, such as employment and social security law, vital and substantial public interests, purposes of preventive or occupational medicine, etc.—shall be prohibited unless the data subject has given explicit consent to the processing.

In this regard, the Italian Data Protection Authority's General Application Order Concerning Biometric Data[14] reiterated that: (i) the processing of biometric data requires the provision of an information notice; (ii) the processing requires the data subject's consent; (iii) biometric data must be protected by adequate security measures (e.g., encryption); (iv) access to databases containing biometric data must be tracked; and (v) data must be retained as long as necessary for the processing purpose.

12 *https://gdpr-info.eu/art-4-gdpr/*
13 *https://gdpr-info.eu/art-9-gdpr/*
14 *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3590114*

1.7 PREVENT (PR) – Prevent Privacy Incidents

1.7.1 Data Protection Policies, Processes, and Procedures

Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to prevent harm.

1.7.2 Identity Management, Authentication, and Access Control (PR.AC)

Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access.

1.7.3 Data Security

Data is managed consistent with the organization's risk strategy to protect individuals' privacy and to maintain data confidentiality, integrity, and availability.

Given the context, the nature, and the purposes of the processing of users' data (and the amount of personal data processed), XR providers should minimize any potential data/information exposure. Some XR providers do not ensure the adoption of certain data security measures, such as encryption or pseudonymization (standard practice in more traditional digital communication means such as instant messaging apps). Furthermore, certain XR systems also rely on third-party services or apps which do not appear to implement suitable security standards. It is essential for XR providers to implement adequate policies and security measures (e.g., physical security of data, physical security of facilities/personnel, network security, system hardening, password security, endpoint protection, patch management, remote access, etc.) to satisfy legal requirements. Many commentators are currently pushing for the identification by governments (or even XR providers' self-regulation bodies) of specific XR minimum security standards (e.g., SANS[15], NIST[16], ISO[17], CIS). Such standards would help XR operators to provide more secure products and services, thus fostering a wider deployment of XR solutions. Moreover, XR providers must ensure restoration of systems to ordinary operation as soon as possible; adequate business-continuity and disaster-recovery plans should be in place that are also able to address incident response and security breaches.

1.7.4 Online Harm Prevention (PR.HP)

Deterrent activities to prevent and mitigate harm consistent with clear policies, processes, procedures, and agreements.

15 *https://www.cisecurity.org/controls/cis-controls-list/*
16 *https://nvd.nist.gov/800-53*
17 *https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained*

1.7.5 Content Moderation Policies

Content moderation policies detail how platforms and services will treat user-generated content. Certain jurisdictions have stricter rules regarding violent/extremist content, hate speech, or other unlawful content.

Minimum Expectations:

- Organizations should include details of the content moderation practices as a part of the acceptable use policy and make it easily accessible to individuals.
- Organizations should Implement regular reporting requirements that include disaggregated statistics on content that has been removed or deprioritized.

Desired Expectations:

- Organizations should adopt policies that provide detail on how to handle inappropriate, unlawful, or harassment-related content. For instance, Canadian hate speech laws prohibit advocating genocide, publicly inciting hatred, or promoting hatred against "identifiable groups."
- Organizations should maintain a complaint management system that processes reports and notifies impacted individuals within a reasonable time frame and allows users to appeal decisions.
- Organizations should consider automated tools to filter/block clearly identified content and permit geofences where XR content can be privately/closely managed.
    - Caution must be taken while implementing such controls because aggressive monitoring requirements can potentially undermine anonymity and free expression.

Ideal Expectations

- Organizations should provide researchers and other qualified independent third parties with access to data to conduct scientific, historical, statistical, and other relevant research, including removed, demonetized, or deprioritized content.

2.0 Human-Centric Privacy by Design

2.1 Overview

While we would like to enjoy the benefits of innovation in the Spatial Computing and XR domain, we must also preserve our freedom of choice and control over our data processing. As we re-think privacy in the era of constant reality capture, one of the pre-existing concepts that comes in handy is "Privacy by Design." Ann Cavoukian, Ph.D., author of *Privacy by Design: The 7 Foundational Principles*[18], wrote that privacy should be "integral to the system, without diminishing functionality." The approach implies that the product or system is designed with privacy as a priority, along with whatever other purposes the product or system serves. Cavoukian's "Seven Privacy by Design" principles are as follows:

1. **Proactive not Reactive; Preventative not Remedial**
   Anticipate and prevent privacy incidents before they happen, to protect organizations from privacy issues that could potentially hurt their reputation.
2. **Privacy as the Default**
   Ensure that personal and sensitive data are automatically protected so that individuals don't have to take steps to secure their data, making privacy the default.
3. **Privacy Embedded into Design**
   Embed privacy into the design, rather than trying to add it on later. Making user-experiences worse for the sake of privacy cannot be an option.
4. **Full Functionality—Positive-Sum, not Zero-Sum**
   Do not make trade-offs to accommodate either privacy or functionality.
5. **End-to-End Security—Lifecycle Protection**
   Considering security (safety) from start to finish to ensure information is secure and protected when it enters the system, is retained safely, and then properly destroyed.
6. **Visibility and Transparency**
   Allow users and other involved parties to see how information moves through the system. Promote trust via accountability, openness, and compliance by being clear about the level of security (safety) provided.
7. **Respect for User Privacy**
   Make user privacy the number one concern and optimize the system or application to meet all the human privacy needs.

18 *http://dataprotection.industries/wp-content/uploads/2017/10/privacy-by-design.pdf*

The **XRSI Privacy Framework** uses this approach with a **heavy emphasis on the seventh principle. Combining the seven privacy by design principles with the Human-Centric design principles, first outlined by the Cyber XR Coalition, the Privacy XRSI Framework helps achieve a much-needed outcome: Human-Centric Privacy By Design (*Figure 2*).**

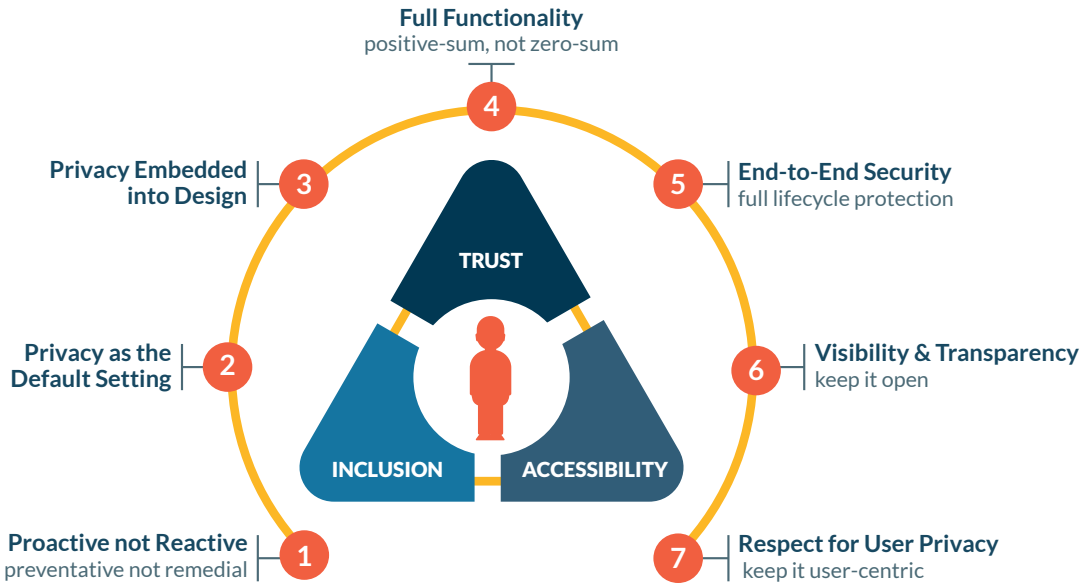

Figure 2: Human-Centric Privacy by Design

2.2 Transparency, Awareness, Accountability, and Trust

Transparency and awareness are essential to establishing accountability and trust in Spatial Computing and XR ecosystems. Privacy risks can be managed by creating awareness. One of the key areas that require transparency in Spatial Computing and XR is content moderation. One hallmark of XR will be a higher degree of interactivity between participants. While not feasible in the short term, future Spatial Computing and XR environments will certainly include haptic feedback-based interaction. Avatar customization and hyper-realistic self-representation will play a role in how individuals not only interact but also express themselves.

Some open questions remain because it is unclear to what extent XR-based environments will necessitate additional controls/safeguards to monitor or prevent sexual harassment and discrimination. How will an inappropriate virtual interaction involving haptic feedback in a classroom setting be litigated? Will inappropriate comments on someone's avatar carry the same consequences that in reality? What would be the consequences of defacing a virtual avatar in a way that could be interpreted as gender stereotype-related discrimination?

2.2.1 Section 230 of the Communications Decency Act

Tucked inside the Communications Decency Act (CDA) of 1996 is one of the most valuable tools for protecting freedom of expression and innovation on the Internet: 47 U.S.C. § 230, a Provision of the Communication Decency Act -.

Section 230 says that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" (47 U.S.C. § 230). In other words, online intermediaries that host or republish speech are protected against a range of laws that might otherwise be used to hold them legally responsible for what others say and do. The protected intermediaries include not only regular Internet Service Providers (ISPs), but also a range of "interactive computer service providers," including basically any online service that publishes third-party content. Although there are important exceptions for specific criminal and intellectual property-based claims, CDA 230 creates a broad protection that has allowed innovation and free speech to flourish online.

2.3 Accessibility, Inclusion, and Trust

A human-centric design and development approach for immersive technologies is built on three pillars—Trust, Inclusion, and Accessibility. This approach fuels the creation of products that resonate more deeply with an audience, ultimately driving engagement and growth.

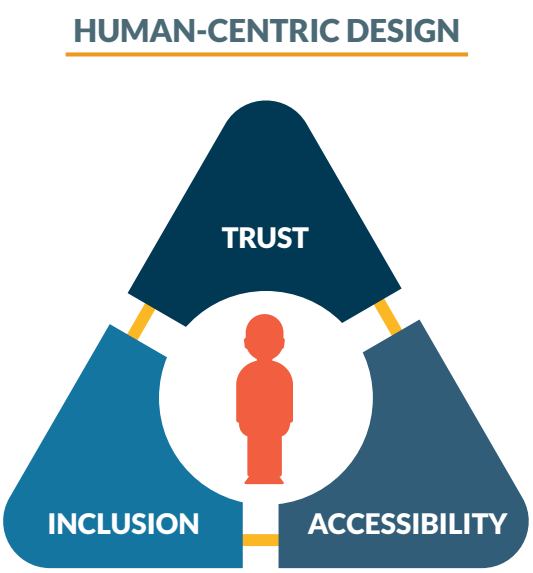

Figure 3: Trust, Inclusion, and Accessibility. The TIA Triad for Human-Centric Privacy by design in XR and Spatial Computing

Trust: The standard definition of "trust" includes the "assured reliance on the character, ability, strength, or truth of someone or something";[19] There is no single recipe for building trust in every system. However, a particular mindset can be established to build systems and applications to promote trust from the ground up. Trust will ultimately define the success of immersive technologies and therefore is a foundational concept to approaching human-centric design and the development of immersive technologies.

Inclusion: The standard definition of "inclusion" includes "the act or practice of including and accommodating people who have historically been excluded."[20] Immersive technologies provide us with an opportunity to create the future. Therefore, attention must be paid to include all forms of diversity while building these technologies. We must build and foster immersive environments where everyone feels welcome.

Accessibility: The standard definition of "inclusion" includes the qualities of "being reached" and "of being used or seen."[21] Current digital frameworks were not designed with accessibility as their foundation. Therefore, a post-production movement emerged to make digital systems accessible to all. With immersive technologies, both the hardware and software of XR should be customizable for all users and, specifically, for those with disabilities or special needs. Only then can we hope for an extended reality design and development that is genuinely human-centric and accounts for human limitations, whether temporary or permanent.

19 *https://www.merriam-webster.com/dictionary/trust*
20 *https://www.merriam-webster.com/dictionary/inclusion*
21 *https://www.merriam-webster.com/dictionary/accessibility*

2.3.1 Importance of Inclusion and its Impact on Privacy

We are at a crossroads between emerging technologies, data sciences, and cybersecurity—fueled by the renewed global necessity of inclusion and accessibility in each domain. Technology jobs are still facing high levels of inequality when it comes to gender and ethnicity. With the rise of Artificial Intelligence-based solutions, the gender and ethnicity exclusion issues are becoming even more relevant. The over-representation of white men in designing these technologies could undo decades of advances in gender and racial equality.

Emerging technologies will not solve this issue if we're not going to change the input. If that data carries stereotypical concepts, the resulting application of the technology will perpetuate that bias. The models and systems we create and train are a reflection of ourselves.

By their nature, XR and Spatial Computing ecosystems process vast quantities of data and have the potential to put minorities, persons of color, and marginalized communities at risk. The XRSI Privacy Framework takes into consideration the principles of inclusion and accessibility. We outline actionable steps to provide data protection for all, weaving equity and accountability in the very fabric of these technologies. We offer mitigation measures to avoid biases while processing personal, sensitive data that can potentially reveal racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, biometrically-inferred data, and more.

These principles were first identified by the CyberXR Coalition in May 2020 and continue to serve as the basis for building safer and more inclusive ecosystems within Spatial Computing and XR.

2.3.2 Accessibility and Privacy via the XRSI Privacy Framework

Accessibility is an ongoing commitment to building technologies that include everyone. Incorporating it as a foundational aspect of building immersive technologies benefits everyone.

Aligning privacy with principles of inclusion and accessibility helps build a culture of care via inclusive hardware and software design; development and coding; appropriate testing; and training. The underpinning reason for infusing accessibility into the privacy landscape is not only because it's the right thing to do, but also because it leads to better, more inclusive digital environments and a culture where everyone feels welcomed.

Privacy considerations for accessibility are not just about how the data is processed but also how risk is assessed, managed, communicated, and prevented. The set of controls and privacy measures defined in the XRSI Privacy Framework provide a comprehensive approach to ensure these considerations are part of the design and developmental process.

ASSESS: Assessment of privacy risks is fundamental to building a privacy-focused technology ecosystem due to the impact these technologies can have on human beings. When developing a comprehensive understanding of the organizations' privacy risks associated with data collection, processing, analysis, and its impact on the users, one has to consider all humans, especially those who need special considerations. These special considerations and controls help organizations prioritize mitigation of the risks while conducting privacy risk assessments and ultimately build a culture of care.

INFORM: When informing individuals and organizations of the risks to enable open and transparent communication to understanding accessibility, a variety of languages, formats, and mediums must be considered (e.g., multi-sensory, multilingual, close-captioned). It is also important to inform individuals anytime they are impacted by automated decision making, profiling (e.g., targeted ads, marginalized communities), and third-party data processing activities.

MANAGE: Spatial Computing and XR technologies have the potential to influence human behavior and can put people's lives at risk. It is imperative to establish and implement the organizational governance structure to manage privacy risk priorities. While this function focuses on organizational-level activities to prioritize its efforts, the privacy burden on individuals must be reduced. Privacy risks for individuals arising from data processing activities have the potential to ignore accessibility considerations. The framework has avoided leaving that to chance by baking them in.

PREVENT: To create safe and inclusive ecosystems, where everyone feels welcomed, safeguards have to be placed to prevent harm arising from existing and novel privacy, safety, and health risks. This is only possible by building equitable tools for privacy management and facilitating controls that consider human abilities and special needs.

2.3.3 Sections 504 and 508 of the Rehabilitation Act and the Americans with Disabilities Act

Section 504 of the Rehabilitation Act of 1973 and the Americans with Disabilities Act (ADA) prohibits discrimination based on disability. An individual with a disability under these statutes is construed broadly as a person who has a physical or mental impairment that substantially limits one or more major life activities, a person who has a history or record of such an impairment, or a person who is perceived by others as having such an impairment. The Office of Civil Rights (OCR) and the U.S. Department of Justice (DOJ) administer implementing regulations for these statutes and interpret their application to extend to technological advancements used in educational settings, including in the delivery of online and remote learning. While these agencies have yet to issue guidance specifically on XR environments, the protections promised by these anti-discrimination statutes would nevertheless apply as has been the case with any emerging technology offering educational benefits since the ADA's passage in 1990.

While compliance with Section 504 and the ADA depends in large part upon providing accommodations to individuals when requested, Section 508 of the Rehabilitation Act of 1973 assigns proactive requirements to institutions receiving federal funding concerning certain information and communication technologies (ICT). Section 508's ICT standards are updated periodically to conform with the World Wide Web Consortium's Web Content Accessibility Guidelines (WCAG) (globally recognized technical standards to improve accessibility). They are administered by the U.S. Access Board. These guidelines are organized under four principles—perceivable, operable, understandable, and robust—and for each, information is provided for testable success criteria at three levels: A, AA, and AAA.

2.3.4 European Accessibility Act

The European Accessibility Act[22] aims to improve the functioning of the internal market for accessible products and services by removing barriers created by divergent rules in the Member States. The benefits to the business range from cost reduction by following common rules on accessibility in the EU to easier cross-border trading, as well as more market opportunities for accessible products and services. Likewise, persons with disabilities and older people can benefit from more accessible products and services in the market; accessible products and services at more competitive prices; fewer barriers when accessing transport; education; the open labor market; and more jobs available where accessibility expertise is needed. The European Accessibility Act covers products and services that have been identified as being most important for persons with disabilities while being most likely to have diverging accessibility requirements across EU countries. Still, it does not explicitly include Spatial Computing and XR devices in those services. Some gaps exist in the accessibility laws, potentially impacting the privacy of individuals with special needs and considerations on both sides of Atlantic.[23]

22 *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0882*
23 *https://ec.europa.eu/social/main.jsp?catId=1202*

2.3.5 Accessibility Due to Physical/Cognitive Differences and Bridging the Digital Divide

The Spatial Computing and XR industries are building products, platforms, and experiences without addressing unconscious biases, excluding particular populations that may not fall in their spectrum of product users. These products' makers can start to change this problematic perception and mindset by developing and testing such products inclusive for all. Considering people with different backgrounds, status (socioeconomic), gender, race, physical builds, and any emerging "difference", this is possible today. With the right mindset, companies find that their products have a far greater reach that is not limited to a small section of society.

With an aging society, statistics[24] say that by 2050 there will be 115 million people with dementia worldwide. That's why it is crucial that people with mild and moderate levels of dementia stay as active as possible and participate in society for as long as possible. However, at the moment, even people with only a mild cognitive decline may find standard applications impossible to use.[25]

These evolving immersive technologies are able to further cultivate experiences to suit individual needs and enhance our ability to explore and connect in new meaningful ways. To better assess, communicate, manage and prevent risks associated with privacy on accessibility needs, the architects of this ecosystem need to understand these differences and continue to push building the infrastructure of the future of computing further and with responsibility. A good starting point is by understanding World Wide Web Consortium (W3C) Cognitive Accessibility User Research that outlines how different people with cognitive disabilities may have problems in the following areas:

- **Memory:** Including Working Memory, Short-Term Memory, Long-Term Memory, Visual Memory, Visuospatial Memory, Auditory Memory (memory for sound patterns and others).
- **Executive Functions:** Including Emotional Control and Self-Monitoring; Planning/Organization and Execution; and Judgment.
- **Reasoning:** Including Fluid Reasoning (logical reasoning), Mathematical Intelligence, Seriation, Crystallized Intelligence, and Abstraction.
- **Attention:** Including Selective Attention and Sustained Attention.
- **Language:** Including Speech Perception, Auditory Discrimination, Naming Skills, and Morphosyntax.
- **Understanding Figurative Language:** Including similes, personification, oxymorons, idioms, and puns.
- **Literacy:** Depends upon functions including Speech Perception, Visual Perception, Phoneme Processing, and Cross-Modal Association (association of sign and concept).
- **Other Perception:** Including Motor Perception, Psychomotor Perception.
- **Knowledge:** Including Cultural Knowledge, Jargon (subject matter); Web Jargon and Technology; Metaphors and Idioms; Symbols Knowledge (such as icons); and Mathematical Knowledge.
- **Behavioral:** Including Understanding Social Cues.[26]

24 *https://www.alz.co.uk/research/statistics*
25 *https://www.w3.org/TR/coga-user-research/*
26 *https://www.w3.org/TR/coga-user-research/*

2.3.6 The Cyber XR Coalition and W3C Accessibility Recommendations

When communicating privacy-related information, some of the critical accessibility aspects outlined in the Cyber XR Coalition's Top 10 accessibility recommendation and initially prepared by W3C can also be applied while communicating privacy-related information:

- **Text Alternatives**
  "Provide text alternatives for any non-text content so that it can be changed into other forms people need, such as large print, braille, speech, symbols or simpler language."
  XR technologies can display and render both 3D and 2D objects in space. These objects all need to have the capacity for text alternatives to be assigned to them for people who cannot see or have difficulty seeing the screen. The challenge lies in the scenario where the context sometimes may be lost in translation, leaving the privacy intent outside of the communicated guidelines or policies.
- **Enough Time**
  "Provide users enough time to read and use the content."
  XR technologies frequently require physical interactions to occur at timed intervals that require fine motor skills. Alternate modes of interactions or other considerations should be present to allow people more time to perform interactions. While making the privacy communication accessible, a lack of time-specific considerations could result in a lack of comprehension and uninformed decision making.
- **Input Modalities**
  "Make it easier for users to operate functionality through various inputs, including keyboard."
  XR extends users' physical input and output beyond any previous medium; its constant evolution toward increased fidelity of input and output in XR may amplify differences among users. Multiple input modalities are instrumental in assisting an individual to make selections for privacy decisions so that it is not restricted to only text form.
- **Readable in Local Languages**
  "Provide readable and understandable text and content."
  XR technologies should ensure that they support multiple languages and users. When relying on synthesized voices to pronounce textual information, words must be pronounced correctly to provide accurate privacy information and context.
- **Compatible**
  "Maximize compatibility with current and future user agents, including assistive technologies."
  XR platforms will continue to add support for assistive technologies as they expand and become available to a wider group of people. The support for user preferences for things like large text, high contrast themes, magnification, and screen reading can significantly increase user's awareness and understanding of the privacy-related information and even aid in informed decision-making.

The list of such recommendations, laws, and guidelines in the uncharted territories of Spatial Computing and XR will continue to evolve. However, as we commence the privacy effort in 2020, The XRSI Privacy Framework takes the existing considerations into account to help create accessible privacy controls and promote safety and trust.

3.0 The Privacy and Compliance Legal Frameworks

The XRSI Privacy Framework takes into account regulatory compliance and policy concerns to provide recommendations for compliance strategies related to the use of Spatial Computing and XR technologies. One of the primary goals of this framework is to get ahead of any privacy and safety risks related to the use of XR technologies. The approach taken to create this baseline framework is to investigate current regulations, such as GDPR, CCPA, FERPA/COPPA, and others as they relate to personal and sensitive XR data. The first step is to consider how these existing requirements apply to Spatial Computing and XR ecosystems. Immersive technologies such as Spatial Computing and XR allow individuals to experience alternate forms of realities with highly engaging and realistic content through expressive avatars. Yet, the degree to which the legal protections and rights afforded to individuals attach to their avatars is not a topic that has been rigorously explored by XR platform makers or in policy-making efforts, whether by individual education institutions or by lawmakers at any level of government. While some of the questions remain open, the XRSI Privacy Framework provides the industry with a minimum set of voluntary controls to help achieve a reasonable level of privacy and safety for Spatial Computing and XR stakeholders.

3.1 General Data Protection Regulation (GDPR)

Spatial Computing and XR systems involve collecting and processing more—and more intimate—personal data than other "traditional" technologies. The XRSI Privacy Framework takes into consideration the EU General Data Protection Regulation (Regulation 2016/679/EU—"GDPR"[27]) and local data protection regulations. For any organization wanting to comply with GDPR, the following 12 steps are outlined and often presented as the starting point. The XRSI Privacy Framework is based on the following key considerations and helps immersive technology organizations demonstrate compliance while mitigating privacy and safety risks, as a baseline measure.

- STEP 1: **Awareness**
- STEP 2: **Information you hold**
- STEP 3: **Communicating privacy information**
- STEP 4: **Individuals' rights**
- STEP 5: **Subject access requests**
- STEP 6: **Lawful basis for processing personal data**
- STEP 7: **Consent**
- STEP 8: **Children**
- STEP 9: **Data breaches**
- STEP 10: **Data protection by design and Data protection impact assessments**
- STEP 11: **Data protection officers**
- STEP 12: **International**

27 *https://eur-lex.europa.eu/eli/reg/2016/679/oj*

3.2 California Consumer Privacy Act (CCPA)

Before 2018, only three states had biometric privacy laws: Illinois, Texas, and Washington. By 2020, that number had nearly tripled. According to an internal survey conducted by the University of Michigan, approximately 20 states either have active privacy laws that affect biometric data collection and use protections or have recently introduced legislation in this area. While these laws were generally developed with concerns over the collection of data from health and fitness trackers, wearable devices, and facial recognition technologies, the statutory definitions for biometric data contained in these laws would almost certainly encompass data commonly collected through XR technologies, such as retina and iris patterns, facial features, and "other biological characteristics."

Among those three states, only the Illinois' Biometric and Information Privacy Act (BIPA, 740 ILCS 14/[28]) provided for a private right of action, giving individuals impacted by violators an opportunity to sue for damages, which has made it very attractive to the plaintiffs' bar. A few state laws also establish minimum security and disposal standards for data handling and establish certain consumer privacy rights, such as access to the biometric data collected and the ability to opt out of data sharing practices without facing discrimination. Some states have introduced legislation that grant individuals the right to request their biometric data be deleted, with limitations (e.g., Hawaii and Minnesota). While these states often draw distinctions between for-profit and nonprofit entities that impact the applicability of specific requirements and penalties, even for nonprofit institutions, some of these same responsibilities and penalties have the potential to pass through to the nonprofit (depending in large part on contractual terms) from a for-profit partner.

California's CCPA is perhaps the best known of the recent state privacy laws that applies to CA residents and provides GDPR-like individual rights as well as the steep penalties under the law that await violators. As is the case with many other state privacy laws, the CCPA does not always directly apply to nonprofit entities, including nonprofit colleges and universities. However, most nonprofit entities are likely to engage with for-profit (and CCPA-covered) service providers to process consumer information. Although recent CCPA guidance indicates that "a 'service provider' under the CCPA (as opposed to a 'business') does not need to comply with most of the CCPA's provisions regarding notices to consumers or compliance with consumers' requests".

3.3 The Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act (COPPA[29]) applies to "operators" of online services directed to children under 13 or have actual knowledge that they collect, use, or disclose personal information from children under 13. Most of the leading HMD providers and XR platforms often straddle that boundary but enforce no specific age restriction. Still, there is a warning that the "product was not designed to be used by children" and that if "older" children are permitted to use the product, an adult should monitor them. While many XR companies have mature COPPA-compliance efforts, XR devices' data collection potential should not be discounted. The U.S. government's Federal Trade Commission (FTC) is currently considering whether biometric data or other information should be included in COPPA's definition of personal information. Looking forward, the merging of XR headsets with brain-computer interfaces (BCIs) like electroencephalogram (EEG) sensors could permit app developers and game designers to make "personalized games" that respond differently based on whether a user is excited, happy, sad, or bored.

28 *https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57*
29 *https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children's-privacy*

3.3.1 The XR Safety Initiative (XRSI)'s Child Safety Risks and Recommendations

So far, there has been very little regulatory discussion around children's privacy in Spatial Computing and XR. The XR Safety Initiative (XRSI)'s Child Safety Working Group has outlined risks that arise from kids' data processing and their exposure to online content and interactions. The XRSI Privacy Framework incorporates most of these privacy and safety measures and techniques:

- **Verifiable parental consent**
  Deploy techniques that go beyond email confirmation (a method known as "email plus").
- **Age Assurance methods**
  Organizations should use methods of age assurance: artificial intelligence, third-party age verification services, account holder confirmation, technical measures, or hard identifiers.
- **Improved user matching**
  User interaction is one of the most severe risks to child audiences. Improving matching algorithms is a practical approach to minimize risks. By strengthening user profiles with relevant data (such as age range, gender, and user preferences), matching algorithms can be improved to consider critical variables and prevent potentially inappropriate user matching.
- **Moderation**
  There are many moderation layers that can be combined to cover content and discourage any kind of abuse. Organizations should deploy one or more moderation tools according to the context of an experience (immersive, augmented, competitive, social/casual) and the age range involved. Personal moderation, community moderation, and platform moderation are good examples.
- **Child exploitation detection too**
  Involves technologies that can identify, remove, and report child sexual abuse material (CSAM).
- **Parental control settings/Family safety settings**
  Develop accessible, easy-to-use, and practical technologies that support parents and caregivers to make better decisions regarding their children's digital experiences. When developing these tools, companies should consider that not all parents have digital literacy.
- **Reduced risks and Explicitly designated environments**
  Preventing and reducing multiple risks inside social virtual reality may also include placing child users in environments that are only populated by verified users (reduced risk environment) or in environments explicitly designed for them. These environments would be labeled as "family-friendly," which disallows swearing, rude gestures, "mature" content, etc.
- **Reports and protocols**
  Organizations need to create specific internal protocols to manage risk and or incidents within their services. Any collaborator handling those issues should be adequately trained and have the right tools to intervene. Time to respond should be calibrated based on risk severity. All reports and incidents should be properly registered and reports with pre-defined key performance indicators should be broadly distributed with specific action/improvement requirements to each supporting team (top management, product teams, marketing teams, user support, engineering, etc.).
- **Community rules and guidelines**
  Community rules and guidelines must be aligned to the risks identified (see section 3.1), enforced, and addressed with transparency.
- **Digital citizenship programs**
  Promoting safe and responsible use of digital tools among families and their children is as essential as developing technologies to prevent and mitigate risks. They should be empowered to understand and manage risks so that they can stay safe online. We encourage organizations to partner with and collaborate in digital citizenship programs for different development stages, contributing to the long-term goal of making digital worlds safer for this audience.

These measures must be aligned with data privacy and other applicable regulations such as COPPA and in accordance with the service provided, geography, the legal requirements of a given jurisdiction, and other factors.

3.4 Education-specific Data Regulations

3.4.1 Overview on the Family Educational Rights and Privacy Act (FERPA)

FERPA is a federal law that protects personally identifiable information in students' education records from unauthorized disclosure. It affords parents the right to access their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student ("eligible student"). The FERPA statute is found at 20 U.S.C. § 1232g and the FERPA regulations are located at 34 CFR Part 99. The law applies to all schools that receive funds under the U.S. Department of Education's applicable program.

3.4.1.1 FERPA: Protection of Education Record Considerations

Education records:

a. The term means those records that are:
    1. Directly related to a student; and
    2. Maintained by an educational agency or institution or by a party acting on behalf of the agency or institution.
b. The term does not include:
    1. Records that are kept in the sole possession of the maker are used only as a personal memory aid and are not accessible or revealed to any other person except a temporary substitute for the maker of the record.
    2. Records of the law enforcement unit of an educational agency or institution, subject to the provisions of §99.8.

These records include, but are not limited to, transcripts, class lists, student course schedules, health records, student financial information, and student disciplinary records.

The use of any Spatial Computing and XR platforms should follow the same access control principles applicable to the use of "2D type" instructional technologies (such as Learning Management System [LMS], discussion, or information-sharing platforms). For example:

- Only students from a given course/section should be able to access the set of digital instructional environments attached to that same course/section.
- Students should not be able to access the full class roster.
- The protection of education records extends to video class recording. Indeed, under FERPA, a video or photo of one or more students can be protected as an education record.[30]

30 *https://studentprivacy.ed.gov/faq/faqs-photos-and-videos-under-ferpa*

Therefore, the recording of in-person, remote, or hybrid teaching or instructional activities must be treated as an education record protected by FERPA when students "are participating verbally or visually, providing commentary, using a chat feature, or making a presentation."
Several universities have developed local FAQs on this topic:

- University of Michigan[31]
- Rice University[32]
- University of Maryland[33]
- Georgia Tech[34]

The controlled dissemination of video recording is a relatively simple and easily managed problem with video-conferencing platforms commonly used in higher education. Currently, a faculty member/instructor initiates the recording and decides how the recording will be shared. Instructional video recordings tend to be distributed through LMS platforms, particularly when an LMS to video conference integration exists. However, despite controls and policies in place, an attendee can try to record using ad hoc means (e.g., a cell phone). Some universities address this scenario by asserting copyrights through policies and student codes of conduct.

In contrast, leading emerging Spatial Computing and XR platforms may not have the same level of recording control-based mechanisms yet. Besides, these emerging platforms will likely provide new recording capabilities that do not presently exist in traditional 2D video conferencing platforms. An example might be the possibility for an attendee to record from their avatar's point of view. A student being able to record or have access to recordings from multiple points of view is valuable from a learning perspective. Therefore, simply disabling this option will significantly diminish the pedagogical value of Spatial Computing and XR in an instructional context.

The use of named avatars introduces new challenges that are not necessarily well understood. Video conferencing platforms display lists of attendees (partial class roster) and let students control their own cameras. In contrast, Spatial Computing and XR platforms rely on avatars with the participant name displayed on top.

The problem of Spatial Computing and XR-based recording becomes potentially even more complicated when considering scenarios that extend beyond a full virtual classroom/meeting space within XR.

3.4.1.2 FERPA: Protection of PII Considerations

Personally Identifiable Information (PII)
FERPA defines the term "personally identifiable information" (PII) to include direct identifiers (such as a student's or other family member's name) and indirect identifiers (such as a student's date of birth, place of birth, or mother's maiden name). Indirect identifiers, metadata about students' interaction with an app or service, and even aggregate information can be considered PII under FERPA if a reasonable person in the school community could identify individual students based on these indirect identifiers and other reasonably available information, including additional public info.

A biometric record, as used in the definition of personally identifiable information, is one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequences; facial features; and handwriting.
International students have the same rights as domestic students under FERPA.

31 *https://safecomputing.umich.edu/be-aware/privacy/privacy-u-m/videoconferencing/recording-privacy-concerns*
32 *https://registrar.rice.edu/facstaff/ferpa_FAQs*
33 *https://umd.service-now.com/itsupport/?id=kb_article_view&sysparm_article=KB0015451&sys_kb_id=30d66c3f1b7fc850ef518738cd4bcbe3*
34 *https://provost.gatech.edu/academic-restart-frequently-asked-questions#recordings*

Current XR devices (such as AR or VR headsets) can capture a different type of biometric data. Some examples include:

- Iris-based recognition for authentication and authorization purposes;
- Eye-tracking movement;
- Head, hand tracking, and full body tracking;
- Voice recognition.

Current "2D" large-scale online courses have provided researchers with access to large data sets in the form of students' clickstreams and events. These data sets are then analyzed using machine learning for various objectives such as developing adaptive learning systems, understanding learners' behavioral patterns, and improving the instructional design of the courses. At the time of writing, and to the best extent of our knowledge, there is no set of instructional apps or platforms that systematically leverage these types of metadata. However, in our opinion, it is only a matter of time. Even if there is no present way to systematically analyze this enhanced learner metadata, instructional providers will likely collect them for future processing. Given the richness and potential of these data, collection, and medium to the long-term collection should be expected. After all, let's consider that online proctoring services such as Honorlock retain the following for 12 months after the event:

- A webcam video recording that includes desktop activity and audio recording.
- Exam and web pages visited by a student during an examination.[35]

3.4.2 Overview of Student Anti-discrimination Regulatory Framework[36]

The U.S. Congress has passed several civil rights statutes that impact institutions of higher education that receive federal funding, including Title VI of the Civil Rights Act of 1964 (prohibiting discrimination based on race, color, or national origin), Title IX of the Education Amendments of 1972 (prohibiting discrimination based on sex), and Section 504 of the Rehabilitation Act of 1973 (prohibiting discrimination based on disability, and the Americans with Disabilities Act of 1990 (which expands upon the protections of Section 504 and broadens the reach of its protections to include state-funded institutions through Title II and private entities through Title III).

3.4.2.1 TITLE VI of the Civil Rights Act

Title VI states that no person in the United States "shall, on the ground of race, color, or national origin, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving Federal financial assistance." The U.S. Department of Education's (ED) Office of Civil Rights (OCR) enforces Title VI concerning "education programs and activities" receiving funding through ED, with implementing regulations found at 34 CFR 100.

Much of OCR's Title VI investigations and guidance involving higher education institutions are focused on the discrimination by the institution's employees against students or discrimination through its admissions practices. Nevertheless, the responsibility of the institution to address instances of peer-to-peer harassment grounded in race, color, or national origin should not be overlooked. Specifically, institutions may be liable if considered "responsible for a racially hostile environment, i.e., harassing conduct (e.g., physical, verbal, graphic, or written) that is sufficiently severe, pervasive or persistent to interfere with or limit the ability of an individual to participate in or benefit from the services, activities or privileges provided by a recipient."[37] In addition to creating or encouraging such a hostile environment, liability may

35 *https://honorlock.com/studentprivacy/*

36 *Additional anti-discrimination regulations apply to institutions of higher education through Title VII of the Civil Rights Act, which focuses on employment discrimination and is enforced by the Equal Employment Opportunity Commission. Research into the potential for workplace discrimination covered under Title VII in the XR context is beyond the scope of this document, which focuses on student protections, but would likely uncover many of the same interpretation challenges due to the overlapping standards among these civil rights laws.*

37 *OCR, Title VI Investigative Guide, 1994, https://www2.ed.gov/about/offices/list/ocr/docs/race394.html*

also attach if severe, persistent, or pervasive harassment is tolerated, including if the institution fails to correct a hostile environment of which it has notice.

Educational programs and activities delivered through XR introduce new and unique patterns for Title VI's application. Namely, the degree to which faculty- or student-controlled avatars can harass or experience harassment under Title VI remains a novel issue that could benefit from additional rulemaking, OCR guidance, or institutional policymaking.

3.4.2.2 TITLE IX of the Higher Education Amendments Act

Title IX is a federal law that bans discrimination based on sex, protecting students at schools that receive federal funds. The court's interpretation of the law extends the discrimination ban beyond gender and includes sexual harassment and discrimination for failing to conform to gender stereotypes. By statute, no person in the United States shall, based on sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any education program or activity receiving Federal financial assistance (20 U.S. Code § 1681).

In federal rulemaking updates that took effect in 2020, the U.S. Department of Education formally adopted what is known as the "Davis standard" into its Title IX rules—i.e., institutions will now only be held liable for student-to-student sexual harassment if they acted deliberately indifferent to harassment for which they had actual knowledge and only if the harassment is so severe, pervasive, *and* objectively offensive that it can be said to deprive the victims of access to the educational opportunities or benefits provided by the school.[38] This new standard differs from previous guidance issued by the Department of Education, which most recently applied a farther-reaching "severe *or* pervasive" test, matching Title VI standards, when determining a school's liability. Additionally, the new Title IX rules have established geographic limitations for liability, holding institutions responsible only for conduct on campus or in locations under the institution's ownership or control.

While these new rules are currently subject to numerous legal challenges, including these very changes, the penalties for Title IX violations remain. These include reputational harm, federal compliance reviews with a potential loss of federal funding, and the costs associated with private, individual lawsuits.

As has been the case for online and remote education, to the extent that an XR or Spatial Computing initiative would be considered an "education program or activity," Title IX rules and consequences would attach. To our knowledge, the degree to which sexual harassment against student avatars used in XR and Spatial Computing learning environments could be considered "severe" under Title IX remains untested in courts and has not been directly addressed through OCR guidance. When Title IX-responsible employees are made aware of harassment in an XR or Spatial Computing setting that is affiliated with the institution's education programs or activities, the legally and ethically responsible practice would be to treat the situation seriously, proceeding under the institution's Title IX policies as applicable to the behavior.

38 *Davis vs. Monroe, https://supreme.justia.com/cases/federal/us/526/629/*

3.4.2.3 Title VI and IX Considerations

The shift from a "2D" digital to a "3D" digital or hybrid digital-physical learning environment presents challenges that are not yet well understood from a Title VI and Title IX perspective. The following is a non-exhaustive list of actions and behaviors that might need consideration.

Concept of personal space: Could a student feel unsafe or harassed if their digital avatar gets suddenly surrounded by a group of students that would prevent their digital movements?

Sexual harassment: What non-verbal, avatar-based interaction could be defined as sexual harassment? Previous universities experimentation with environments such as Second Life highlighted similar problems such as "avatar rape."[39]

Presentation: What level of freedom will be provided to students to create and manage their digital avatars within a virtual classroom environment? Will students be expected to have an accurate digital twin of themselves? Or will students be provided with the freedom to have avatars close to who they feel they are (from a gender, sex, race, and ethnicity point of view)?

3.4.2.4 Sections 504 and 508 of the Rehabilitation Act and the Americans with Disabilities Act (ADA)

In an educational context, enforcement of Section 508 is most familiar concerning public websites and open content such as Massive Open Online Courses (MOOCs), with closed educational environments still permitted some flexibility as long as accommodations are provided to students upon request. With regard to Spatial Computing and XR, many WCAG and therefore Section 508 (with a requirement to follow WCAG 2.0 level AA at present) standards remain applicable where these requirements would otherwise attach. Designing XR hardware and content with accessibility in mind can help eliminate the need to retroactively create accommodations for students in need and expand the potential audience in more open settings, when providing accommodations may no longer be practical where Section 508 may directly apply.

39 *https://www.insidehighered.com/views/2010/02/25/avatar-rape*

4.0 Conclusion and Future Roadmap

Spatial Computing and XR can no longer be dismissed as passing trends. In the COVID era, we are witnessing remarkable technological advancements in these domains. We also see a surge of state biometric data bills and legislation, exposing XR organizations to global and state regulatory actions. While the actual requirements and impact of recent biometric privacy court cases remain unclear, the XR Safety Initiative and various interdisciplinary experts have taken the first step in creating a baseline foundation for privacy in the immersive domain. Until the voluntary framework is adopted into a regulation or law, organizations are expected to self-regulate and consider local and state laws to demonstrate compliance when dealing with individuals' privacy in Spatial Computing and XR. On the one hand, organizations may consider adopting the most demanding standard: the GDPR. On the other hand, organizations can regulate themselves using the XRSI Privacy Framework and seek ongoing guidance from the XR Safety Initiative's advisory team on various evolving topics within the framework. The Spatial Computing and XR industry are booming, with global organizations seeking to establish themselves as leaders. Achieving recognition as both a cutting edge and responsible innovator is a critical step in winning the trust of individuals, consumers, organizations, and institutions.

As the **XRSI Privacy Framework** continues to evolve, the following topics remain on the future roadmap:

- Geolocation and geo privacy;
- Standardized semiotic labels for XR;
- Adoption and enforcement of the framework;
- Data protection impact assessment for Spatial Computing and XR;
- Analysis of dark patterns and their impact on trust in Spatial Computing and XR;
- XR Data Classification Framework (continue XR-DCF effort XRSI started in 2019);
- Technical standards for informed consent (human readable labeling schema for adoption).

Taxonomy

Extended Reality (XR)

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 broad spectrum of hardware and software, including sensory interfaces, applications, and infrastructures. XR is also referred to as immersive video content, enhanced media experiences, as well as interactive and multi-dimensional human experiences.
Taken from the XRSI Taxonomy.

Spatial Computing

Spatial Computing is an umbrella term referring to the type of interaction we have with reality more than a specific technology. The definition puts function over form, as it relates to the use of the space around us as a medium to interact with technology. Spatial Computing defines a human-machine interaction in which the machine retains and manipulates referents to real objects and spaces. Spatial Computing differs from related fields such as 3D modeling and digital design as it requires the forms and spaces it deals with to pre-exist and have real-world valence. It is not enough that the screen is used to represent a virtual space—it must be meaningfully related to an actual physical place.
Taken from the CyberXR Standard Taxonomy.

Framework

A framework is a set of decisions, directives, codes of conduct, regulatory policies, guidelines, recommendations, procedures, and practice directives (whether or not having the force of law).
A privacy framework is needed for immersive technologies to mitigate privacy risks to individuals and organizations and promote trust within the Spatial Computing and XR ecosystems.

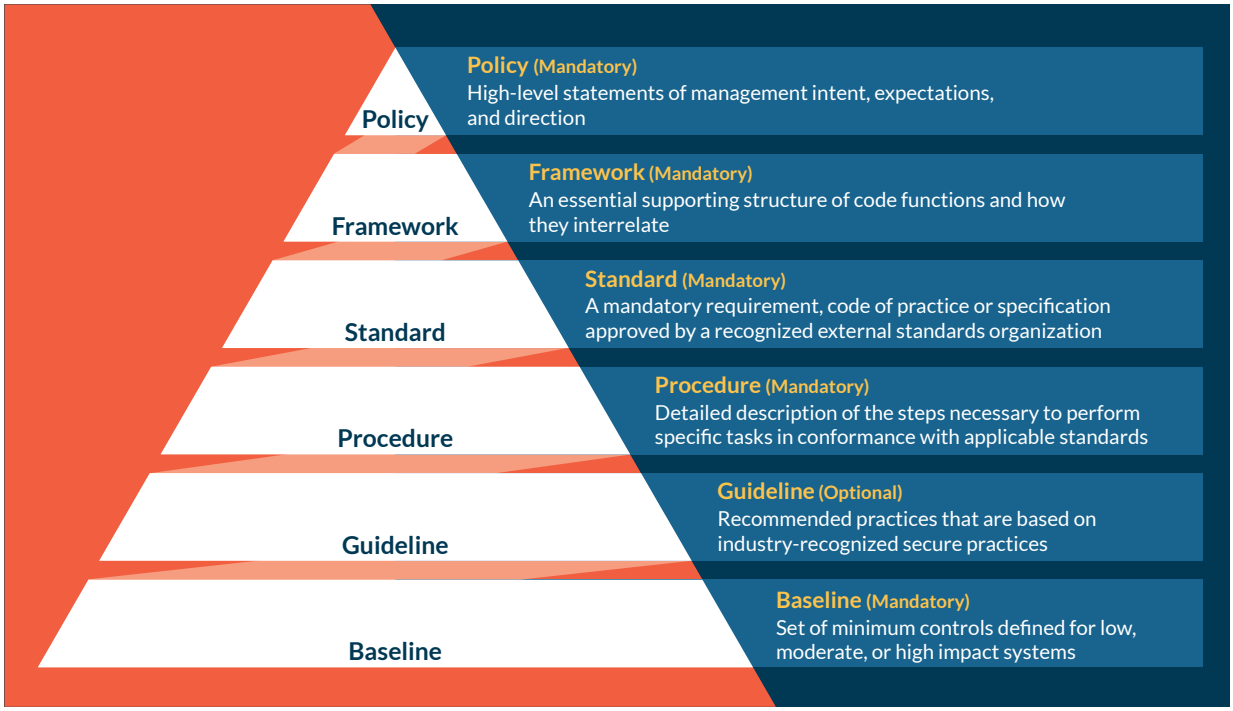

Figure 4: What is a framework

The XRSI Privacy Framework

The XRSI Privacy Framework is a free, globally accessible baseline rulebook curated by the XR Safety Initiative (XRSI) that has a layered structure, outlining the focus areas that act as a set of functions within a system and how they interrelate to achieve privacy; standardized subcategories; and the corresponding set of privacy controls for Spatial Computing and XR domain. The framework provides a baseline set of standards, guidelines, and best practices that are regulation-agnostic. It includes privacy requirements drawn from the EU's General Data Protection Regulations(GDPR), the U.S. government's National Institute of Standards and Technology (NIST) guidance, the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Rule (COPPA), and a few other evolving laws, but is designed to adapt and include new requirements as new regulations come into effect. The framework is not a law or standard; it is a free tool that is continuously evolving.

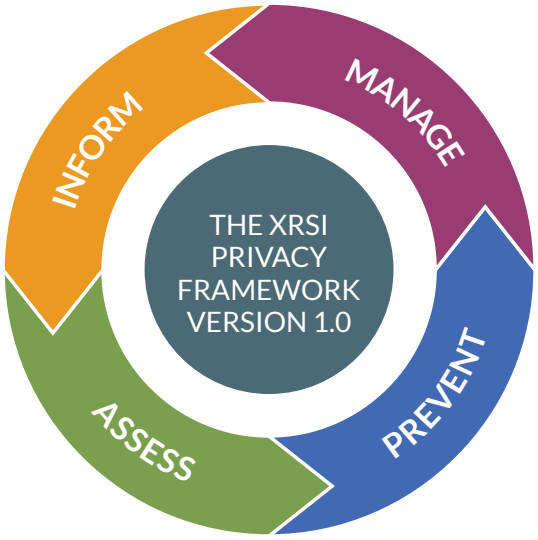

Figure 5: Overview of the XRSI privacy Framework

ASSESS	INFORM	MANAGE	PREVENT
Assessment and Mapping	Context	Awareness and Training	Data Protection
	Choice	Monitoring and Review	Identity and Access Control
Risk Assessment	Control	Data Processing	Data Security
	Child Safety	Special Data Type Considerations	Harm Prevention

Figure 6: Areas of Work and Subcategories in the XRSI privacy Framework

5G

What is 5G? The term "5G" refers to the 5th generation mobile network and a new global wireless standard, designed to virtually connect every machine, object, and device together, including potentially humans via a brain computing interface (BCI).

As the latest in wireless technology, 5G delivers higher peak data speeds, ultra-low latency, more reliability, massive network capacity, increased availability, and potentially a more consistent user experience to more users.

6G

The term "6G" refers to the sixth-generation wireless network and is the successor to 5G cellular technology. With 6G, networks will use higher frequencies than 5G networks and provide substantially higher capacity and much lower latency. Both humans and machines will be the primary users of 6G and 6G will be characterized by the provision of advanced services such as truly immersive extended reality (XR), high-fidelity mobile holograms, and digital replica.

Edge Computing

The word "edge" here means literal geographic distribution. Edge computing is a distributed computing framework that brings enterprise applications closer to data sources such as the Internet of Things (IoT) devices or local edge servers. This proximity to data at its source leads to faster insights, improved response times, and better bandwidth availability.

Internet of Things (IoT)

The Internet of Things (IoT) is a system that aims to connect people to people (P2P), people to machine (P2M), and machine to machine (M2M) through an interconnected, heterogeneous platform for devices and systems. The IoT has allowed devices, people, and technologies to interact with each other and process millions of terabytes of data for everyday commercial, industrial, technical, and personal usage.

Brain-computer interface (BCI)

Sometimes called neural-control interface (NCI), mind-machine interface (MMI), direct neural interface (DNI), or brain-machine interface (BMI), a brain-computer interface is a direct communication pathway between an enhanced or wired brain and an external device. A BCI allows for bidirectional information flow. BCIs are often in service of researching, mapping, assisting, augmenting, or repairing human cognitive or sensory-motor functions. The term BCI is often used to refer to an emerging technology domain where brain activity is used directly without any motor involvement to activate a computer or other external devices. The brain signals are usually measured using electroencephalography (EEG) and processed by neural interfaces.

Artificial intelligence (AI)

Artificial intelligence is the study/domain of problem-solving, pattern recognition, and rationality within machines.

Biometric data

Biometric data, as defined in Article 4(14) of General Data Protection Regulation (GDPR):
"'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data."

Examples of physical or physiological biometric identification techniques:

- Facial recognition;
- Dactyloscopic data (fingerprint verification;)
- Iris scanning;
- Retinal analysis;
- Voice recognition; and
- Ear shape recognition.

Examples of behavioral biometric identification techniques:

- Keystroke analysis;
- Handwritten signature analysis;
- Gait analysis; and
- Gaze analysis (eye-tracking).

Biometrically-Inferred Data (BID)

Biometrically-inferred data is a collection of datasets resulting from information inferred from behavioral, physical, and psychological biometric identification techniques, and other nonverbal communication methods. Prime examples of biometric identification techniques that potentially contribute to BID are:

- Facial recognition;
- Dactyloscopic data (fingerprint verification;)
- Iris scanning;
- Retinal analysis;
- Voice recognition; and
- Ear shape recognition.
- Keystroke analysis;
- Handwritten signature analysis;
- Gait analysis; and
- Gaze analysis (eye-tracking).

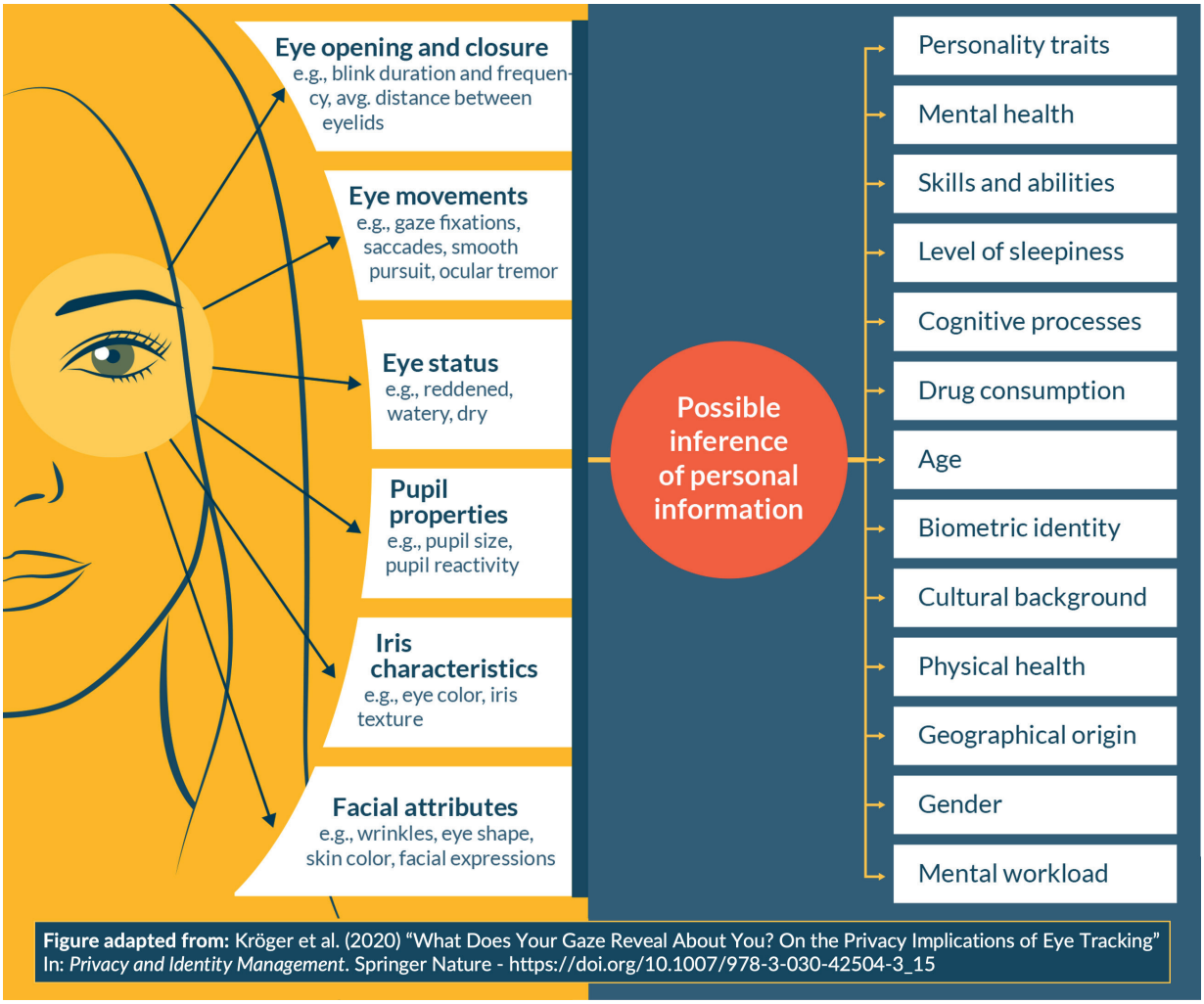

Figure 7: Biometrically Inferred Data commonly captured by eye trackers and sensors

Privacy Compliance

Privacy Compliance is a company's accordance with established personal information protection guidelines, specifications, or legislation.

GDPR

The General Data Protection Regulation (GDPR)[40] is a comprehensive privacy law that has become a model for privacy and data governance legislation worldwide. Though enacted by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation came into effect on May 25, 2018. The EU governments and regulatory authorities will levy harsh fines against those who violate the GDPR's privacy and security standards, with penalties reaching tens of millions of euros.

COPPA

The Children's Online Privacy and Protection Act[41], more commonly known as COPPA, is a law dealing with how websites, apps, and other online operators collect data and personal information from kids under 13. Among its several requirements, COPPA states that tech companies making apps, websites, and online tools for kids under 13 must:

- provide notice and get parental consent before collecting information from kids;
- have a "clear and comprehensive" privacy policy;
- keep the information they collect from kids confidential and secure.

CCPA

The California Consumer Privacy Act (CCPA)[42] is a state-wide data privacy law that gives California residents more control over the personal information that businesses collect about them. This landmark law secures new privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information;
- The right to not be discriminated against exercising their CCPA rights.

Businesses, including data brokers, are required to give consumers specific notices explaining their privacy practices.
The CCPA is the first law of its kind in the United States and went into effect on January 1, 2020.

FERPA

The Family Educational Rights and Privacy Act (FERPA)[43] is a Federal law that protects the privacy of student education records. The rule applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights concerning their children's education records. These rights transfer to the student when they reach the age of 18 or attend a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

40 *https://gdpr.eu/*
41 *https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule*
42 *https://oag.ca.gov/privacy/ccpa*
43 *https://www2.ed.gov/policy/gen/guid/fpco/ferpa/students.html*

NIST Privacy Framework

The National Institute of Standards and Technology's (NIST) *Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*[44] is a voluntary tool intended to help organizations identify and manage privacy risk so that they can build innovative products and services while protecting individuals' privacy. The XRSI Privacy Framework was inspired by the approach taken by the NIST privacy framework and strategically designed to be compatible with existing domestic and international legal and regulatory regimes and usable by any type of organization to enable widespread adoption.

Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is a process to help organizations identify and minimize the data protection risks of a project.
GDPR mandates DPIAs for "a type of processing, in particular using new technologies and taking into account the nature, scope, context, and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, before the processing, assess the impact of the envisaged processing operations on the protection of personal data."

Geolocation

The geolocation defines a high-level interface to location information associated only with the device hosting the implementation, such as latitude and longitude. It allows the user to provide their location to applications if they so desire. For privacy reasons, oftentimes, the user is asked for permission to report location information.

Geospatial Data

Data about objects, events, or phenomena that have a location on the Earth's surface or any other planet in the galaxy (including the space stations). The location may be static in the short-term (e.g., the site of a road, an earthquake event, children living in poverty), or dynamic (e.g., a moving vehicle or pedestrian, the spread of an infectious disease). Geospatial data combines location information (usually coordinates on the earth), attribute data (the characteristics of the object, event, or phenomena concerned), and often uses temporal information (the time or life span at which the location and attributes exist).

Data Breach

A data breach is a security or privacy incident leading to the accidental destruction, loss, or alteration of information or the unauthorized disclosure or access to that information. Data breaches can hurt businesses and consumers in various ways. Breaches can be a costly expense for companies, requiring time and resources to identify and remedy, and can damage the lives and reputations of individuals whose data was breached.

Personal Data

Personal Data, as defined in Article 4 of General Data Protection Regulation (GDPR), means "any information relating to an identified or identifiable natural person ('data subject'); an 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." Under GDPR, pseudonymous data is also considered personal data.

44 *https://csrc.nist.gov/projects/risk-management/compliance*

Data Processing

Data processing is "the collection and manipulation of items of data to produce meaningful information."[45]. It includes converting raw data to machine-readable form; the flow of data through the CPU and memory to output devices; and formatting or transformation of output. Any use of computers to perform defined operations on data can be included under data processing. The data processing may consist of collecting, recording, organizing, structuring, storing, using, erasing, etc.

Opt-in versus Opt-out

Opting in means that a user will take an affirmative action to offer their consent, whereas opting out means a user will take action to withdraw their consent.

45 *French, Carl (1996). Data Processing and Information Technology (10th ed.). Thomson. p. 2. ISBN 1844801004*

XR Safety Initiative
www.xrsi.org

The **XRSI Privacy Framework** is meant to be used as a baseline ruleset to enahance privacy, create accountability, and build trust.

The four focus areas, 14 functions and ~125 controls serve as a guide to build Human-Centric privacy by design in the evolving domain of extended reality and spatial computing. This framework is an ongoing collective effort by XR Safety Initiative (XRSI). We continue to further develop and update the framework, in collaboration with the following organizations:

OPEN AR CLOUD
www.openarcloud.org

CENTER FOR ACADEMIC INNOVATION
UNIVERSITY OF MICHIGAN
ai.umich.edu

GEORGIA INSTITUTE OF TECHNOLOGY
www.gatech.edu