PRIVACY in the era of Constant Reality Capture: Informed Consent in Extended Reality (XR)

Joshua Tooker

MBA/MSI in Human-Computer Interaction

April 2021

I present this Master's Thesis with gratitude
to my advisor Dr. Florian Schaub and committee member Dr. Steve Oney

Many thanks to my *very* patient and supportive wife, Courtney
and to my parents 'Up North'

Abstract

Extended Reality (XR) is expected to grow at a rapid pace over the next decade. Currently, especially in the United States, digital privacy protections do not provide adequate levels of privacy and safety protection from being violated as an individual or group. This thesis presents findings from 29 interviews with Expert and practitioners to understand how the XR industry begin to move forward given that binary options of consent will not suffice in XR, and we cannot wait to try to fix our mistakes as we have done in the online world with social media disinformation. This thesis first analyzed the XR Safety Initiative's Privacy and Safety Framework (XRSI), which served as the foundation for creating the questions for Expert and practitioner interviews. The priority of that analysis was to identify elements of the XRSI that had opportunities to provide deeper guidance on the existing XR privacy recommendations from the online world. It became clear that there were gaps around the Inform section (1.5) and specifically around consent (1.5.2), choice (1.5.3), and control (1.5.4), which allowed for the formulation and prioritization interview questions for participants (XRSI, 2020). The research found that privacy experts believe that the fear of negative financial implications, resulting from unknown business outcomes of privacy policies that provide adaptable levels of consent, increases users' risk is the biggest hurdle to overcome. XRSI can, and should, help address this issue by increasing its support for its stakeholders. Importantly, 64% of respondents stated that there should be an opportunity to opt-in or opt-out of parts of an experience. Moreover, of those interviewed, 14% of all respondents that did not initially name opt-in/out as their first choice choose this option as their second-most vital way to grant consent.

Table of Contents

Ch. 1: Motivation

The explosion of the internet has led to an exponential increase in the information of the world, which does not seem to be slowing down (Pariser, 2011). Today, private sector organizations virtually dictate consumer privacy protections and, generally, prioritize profit over consumer safety (Thurman and Kane, 2010). With data collection serving as a foundation for internet-based business models, a consistent practice in the development and deployment of privacy policies has relied on limited choice of whether to use a digital or online service and agree to the terms set by the organization or one can choose not to participate in essentially a binary scenario, forcing one to agree to a one-sided privacy agreement to use a digital product/service or not, puts people at increased risk to their personal safety (Acquisti, 2009). Consumers can often only adhere to whatever privacy policy provided by the digital platform or not use the product/service, which ensures profit-making scenarios play out as a result of the complete control an organization has over an individual's behavioral data (Thurman and Kane, 2010; Obar and Oeldorf-Hirsch, 2018).

Over the last twenty-five years, the digital advertising business model has built its foundation around the consumption and application of consumers' behavioral and preference data for financial gain; and it is unlikely to be changed without significant regulation (Beshears, 2008). Unfortunately, the legislating bodies in the United States, one of the main countries in focus for this research, have proven to be inept and unwilling to understand the needs of their constituents as it relates to privacy regulation, so it seems unlikely that these web-based business models will be forced to become less reliant on advertising revenue to provide fair privacy practices for consumers (Feigin, 2004). For example, when companies like Facebook and Twitter, which are referred to as the digital town square, are woven into and often drive public discourse, citizens who choose not to participate are being censored in their ability to contribute to these conversations (Roux, 2020). On an interpersonal level, when one decides not to use Facebook, Twitter, TikTok, individuals are also not provided with equitable access to knowledge sharing. In conceding that individuals can actively choose not to use a product or service without legislation to protect consumers truly, it is only a matter of time before one-dimensional privacy procedures cause more profound safety risk and potentially societal inequity (e.g., company compensating citizens for the consumption of personal data) (O'Brolcháin et al., 2016; Acquisti et al., 2014).

That leaves emerging technologies as a pathway where society can apply learnings from the web to create a digital ecosystem that protects consumers' privacy rights while also establishing revenue and cost structures that can achieve profitability and act as an alternative to the online advertising business model. After reviewing existing research related to Extended Reality (XR, henceforth) and the role of consent in establishing practices, it appears that XR is new enough to where both organizational and social norms are related to privacy have not been fully established. The development of XR hardware and software and an expected exponential growth rate for consumer adoption demonstrates the business, policy, and social need to identify sufficient XR privacy policies as soon as possible.

With limited guidance on digital privacy protections at the federal level for consumers, especially as it relates to consent, this research aims to help consumers, policymakers, academics, and industry

leaders by highlighting what meaningful consent may look like for those developing XR technology and those creating XR content but also where common ground between privacy advocates and private sector XR organizations is more likely to be found.

At the center of the implied tension above are privacy policies because of the way in which consent is gained and the comprehensive governance over a user's online activity. Privacy policies are often unrealistically complex and potentially jargon-filled, creating situations where users often may not be aware of the implications or scope upon collection of some data types, which has been true throughout the internet age but is increasingly troublesome in the age of XR (Litman, 209). Highlighting the importance of understanding how one's data is used and the importance of freely giving consent, Stanford University, Miller and Herrera, found that a VR system identifies 95% of users correctly when trained on less than 5 min of tracking biometric data, like head movement, per person (Miller and Herrera et al., 2020). Data collected in this way can be used to track patterns, which can identify sensitive medical data (e.g., eye tracking) for individuals that could be used to discriminate during job interviews, access financial information, or other activities that currently use biometric data for identity authentication when this data is stored and sold to third parties. While this may be a helpful feature for some, the implications on user privacy, and ultimately safety, should be communicated clearly. Users should still be able to use a service but opt-out of this type of data collection. It should be the technology provider's responsibility to ensure baseline and shared knowledge of the risks associated with a product or service's use. Nevertheless, current practice of limited choice and control over one's data in the online world is carrying over into XR and, increasingly, could lead to physical harm for individual consumers and those around them as a result of the data collected, stored, and processed by XR organizations should these data fall into the hands of predators.

To address some of these issues, the XR Safety Initiative (XRSI) was created with a vision to help build safe immersive technological environments and its mission is to inspire and support the safe use of extended reality (XR) technologies. XRSI's core functions include: 1) Collaborating with university-based researchers; 2) Partner with industry stakeholders to build safety standards that promote trust; 3) Encourage critical thinking across XR stakeholders with media and awareness campaigns; and finally, 4) Serve as a first-line of advisory and oversight (XRSI, 2020). In Fall 2020 the XRSI published their first-ever privacy and safety framework to serve as guidance across the XR industry.

This thesis investigates the XR Safety Initiative's Privacy and Safety Framework 1.0 and its relative feasibility to have its primary recommendations implemented by Extended Reality (XR) hardware and software creators (XRSI, 2020).

Using feedback from industry experts the second phase of this research sought to understand not only the elements where academics, privacy experts, and XR industry professionals find agreement in XR privacy practices but, possibly, more importantly, highlight areas in need of compromise to accelerate the development and adoption of XR-privacy-related public policy that is framed with consumer consent as a key pillar.

While initial guidance has been provided by the XR Safety Initiative (XRSI) in the form of the XR Privacy and Safety framework, the probability of implementing the framework's recommendations is not specific without business incentives or federal regulation (XRSI, 2020). Moreover, in the XRSI Privacy and Safety framework, the little information discussing choice and consent is likely insufficient to address the changing needs of users in XR (XRSI, 2020). The current version of the XRSI Privacy and Safety Framework combines elements of existing privacy policies like the GDPR and NIST frameworks and singular references that serve to provide cursory-level context for the recommendation. For example, in the consent section 1.5.2, XRSI briefly raises the point that consent in XR might be different from today's expectations in the online world and then follows it with a singular example of the collection of biometric data and a bullet point from the GDPR that acknowledges how the processing of data should that is not necessary for performance should not be included. In short, these sections are incomplete and do not do much more than recycle existing elements of privacy and safety in today's online world. It would be in the best interest of the XRSI team to take proactive measures to figure out a way to accommodate today's XR industry stakeholders to specifically identify new and/or unique considerations for privacy and safety in XR.

The main research questions that this research hopes to gain insight into are based on the XRSI Privacy Framework 1.0:

- How do experts understand/view XRSI's (more information below) proposed minimum, desired, and ideal privacy requirements?
- How easy/difficult is it for companies to implement the proposed measures?
    - What hurdles and/or incentives do organizations need to address to establish more comprehensive privacy design/policies that can be successfully implemented?

Therefore, this thesis investigates, through a framework analysis and interviews with 29 Experts and practitioners, the proposed XRSI Privacy Framework and its relative feasibility to have its primary recommendations implemented by the Extended Reality (XR) technology and content creators.

This thesis first analyzed the XR Safety Initiative's Privacy and Safety Framework, which served as the foundation for creating the questions for Expert and practitioner interviews. The priority of that analysis was to identify elements of the XRSI that had opportunities to provide deeper guidance on the existing XR privacy recommendations from the online world. It became clear that there were gaps around the Inform section (1.5) and specifically around consent (1.5.2), choice (1.5.3), and control (1.5.4), which allowed me to formulate and prioritize interview questions for participants (XRSI, 2020).

Interviewees stated that privacy in XR should be determined by a multi-stakeholder group and noted, definitively, the importance that sole responsibility for definition not be granted to the private sector. A majority of interviewees stated that existing laws and regulations are insufficient for adequate protection in XR because of the lack of clarity in these laws and added experiential and technical complexity that is currently defined by law. There is broad consensus that augmented reality technology presents an unprecedented risk, if unchecked, to humans. To address this adequately, a collaborative effort is required to:

1. Educate consumers;
2. Collaborative effort to establish social norms;
3. Apply technological solutions such that bystanders are protected from constant capture by default.

To accomplish this, technological applications like jammers or blurred vision that protects bystanders without requiring any action on their behalf were suggested by many interviewees as a potential solution. Privacy experts believe that the fear of negative financial implications, resulting from unknown business outcomes of privacy policies that provide adaptable levels of consent, increases users' risk is the biggest hurdle to overcome. Currently, to provide valid permission in XR, most of the experts shared the opinion that users must be aware of:

- Which data is being collected and/or sent (and to whom);
- How the users' data will be used;
- Will the users' data be sold to a third party;
- How long any collected data will be stored;

Importantly, once that information has been understood, 64% of respondents stated that there should be an opportunity to opt-in or opt-out of parts of an experience. Moreover, of those interviewed, 14% of all respondents that did not initially name opt-in/out as their first choice choose this option as their second-most vital way to grant consent.

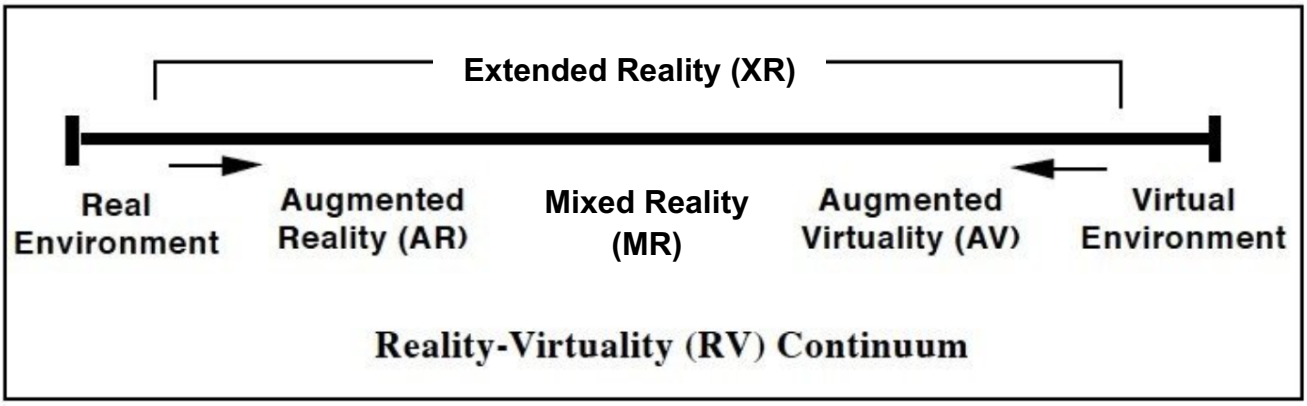
Going forward, this thesis will share related work while providing a high-level overview of the history of XR and its growth potential in chapter 2. Both are vital to understanding the underlying urgency in addressing the lacking choice and consent in XR. Following this related work, in chapter 3, an overview of the research methods and study protocols served as the foundation for the 29 user interviews completed at the end of March and early April 2021. Results of the XRSI analysis are presented in chapter 4 and followed by a discussion and analysis of the interview findings in chapter 5. Lastly, the conclusion in chapter 6 will provide preliminary recommendations and highlight some future work that could be completed to build on the findings resulting from this thesis.

Ch. 2: Related Work

This chapter provides a foundation for understanding what XR is and the origins of the technology. After setting the baseline for what XR is and its history, it is important to contextualize why studying this topic is essential. To do that, one must first understand the general demand and market impact of the emerging technology. This is accomplished by presenting market forecasts from industry publications that share the recent history and expected trajectory of impact XR would have on society in the coming years, understanding the technology and its capabilities, along with the scale at which it will be introduced to society. It is with a global scale and a growth rate that outpaces much of what is seen in the marketplace, requiring an understanding and assessment of the potential externalities that the introduction of XR presents. Because of the combination of granularity and scale of data collection for individuals' personal information, it is important to understand this technology's privacy and safety implications. This understanding of the technology, why it is important, and how its growth will affect an individual is why it is important to understand the role that consent plays in these technologies.

WHAT IS XR?

Extended Reality (XR) is an umbrella term for many common digital interfaces that have exponentially increased in popularity over the last decade. However, what is Extended Reality? Is it augmented reality? Is it mixed reality? Is it virtual reality? The convoluted yet straightforward answer is that it is all of these: augmented reality, mixed reality, and virtual reality. But how can this be? Well, one of the more helpful ways it has been explained is by Paul Milgram and Fumio Kishino back in 1994, where they explained that Extended Reality (XR) is more of a continuum, as shown in Figure 1 below (Milgram & Kishino, 1994).



Milgram and Kishino's Mixed Reality on the Reality-Virtuality Continuum .[Milgram and Kishino 1994]

Figure 1: Milgram and Kishino's Continuum

Ultimately XR, which is commonly referred to solely as Mixed Reality, takes the 'real' world that humans interact with today and blends it with the technological, digital world (Nebeling et al., 2019).

On one side of this spectrum is augmented reality where one sees a digital overlay, think: using an Ikea or Wayfair app to drop a digital furniture overlay into a room in a house, or the now-defunct Google

glasses, in their ‘real world. It takes a digital object and puts it in the ‘physical’ world to project the digital object into the digital camera’s viewable space (Tsukayama, 2014). A common definition for Augmented Reality (AR) was established nearly three decades ago by researchers like Ronald Azuma and his research team at Hugh Laboratories (Azuma, 1993, Azuma and Bishop, 1994). According to their definition, AR technology has three essential requirements: 1) It combines real and virtual content 2) It is interactive in real-time 3) It is registered in 3D space. Early efforts to develop this technology were costly, limiting research in the early years of Augmented Reality. Some of the significant breakthroughs came from Jun Rekimoto and Katashi Nagao in Sony’s Computer Entertainment Lab in Japan, where sufficient capital could be allocated to develop computer vision technology to replicate the ways humans visualize objects in the physical world. To do this, AR technologies have to scan outward landscapes and can turn nearly everything we observe in the physical world into a digital data point (Neumann and Cho, 1970). Augmented Reality also collects data from how we interact with our broader environment; one can think of these data as our behavioral data within a digital experience.

Moving to the other end of the spectrum, Virtual Reality (VR) is a fully immersive experience that, at this time, requires a head-mounted display (HMD) or sensors that create a room called a “VR Cave” that closes one-off from the outside world (Brown et al., 2017). In 2021, major hardware developers for Virtual Reality displays include Facebook’s Oculus with the Quest 2, and the more expensive options like HTC’s Vive. In its simplest form, Virtual Reality has been defined, for nearly three decades, as an immersive way for “humans to visualize, manipulate and interact with computers and extremely complex data" (Isdale, 1993). These data can come in many forms, and the type of data that is collected differs based on the technology’s hardware and/or software developers’ product design and business model. Virtual reality data collection does not require scanning and data collection of the outward landscape. However, it still may collect some of these data; VR mainly collects usage data for both the hardware and software. For VR, one must sense head orientation and head movement to adjust the viewport to what the user is looking for. It is that head movement that serves as an individual data point. Many of the best early uses for Virtual Reality have been developed for use at theme parks, and its introduction to consumers has most often come in the form of a video game (Levine, 2018; Chuah, 2018). The gaming element, which already suspends reality and puts control of a world into the user’s hands, has accelerated because of the added benefit of moving beyond traditional handheld controls (Kholer 2016). Moreover, the visual technology is enhanced by additional technologies to immerse a user and enhance other sensory mechanisms, such as physical touch or audio, by blocking out contradictory senses (Brooks, 1999).

In the middle of the Milgram and Kishino continuum is Mixed Reality, which is also known as Augmented Virtuality, which blends augmented and virtual reality. There are four different ways to define MR, which have become apparent in early research: 1) Mixed Reality according to Milgram et al.’s continuum; 2) Mixed Reality as a “stronger” version of AR due to the complete immersion in the digital world; 3) Mixed Reality as a combination of AR and VR (potentially bound to specific hardware or devices), and 4) Mixed Reality as a synonym for AR (Nebeling et al., 2019). What is agreed upon, even in 2021, is that certain technologies are required for XR to reach its maturity, both in terms of human reach and usefulness.

HOW DID IT START

The idea of extended reality in the United States dates back nearly 100 years to Pygmalion's Spectacles, a science fiction story written by Stanley G. Weinbaum. This may be the foundation for our early understanding of how virtuality exists today, which is in the form of goggles accompanied by virtual sense-making - for example, sight, smell, touch, and taste (Weinbaum, 1935; Cater, 1994). While below, I will present a thorough, yet relatively concise, overview of the history of Extended Reality, there may be things that have been accidentally, and unintentionally, left out due to the incomplete record and recognition of human accomplishments, especially those made outside of the Euro-centric Western world.

In the 1930s, at that time, the complete hardware from Pygmalion's Spectacles were not constructed. However, the individual technologies are traced back to as early as the 17th century where theatres and museums used large plates of glass to merge reflections of objects with the natural world (Brooker, 2007). Building on that capability, in 1838, Charles Wheatstone invented the Stereoscope, which allowed for separate images to be viewed by each eye, which created a three-dimensional (3D) effect for the viewer (Wade, 2002). Then, in 1891, Thomas Edison and William Dickenson's Kinetoscope sent film between lenses and used light to show through a peephole multiple images at 46 frames per second (FPS). In 1929, Edwin Link created a flight simulator that mimicked the movement of an airplane cockpit and the potential dangers a pilot may encounter during flight (Culpepper, 2006 & Jeon 2015). In 1939 at the New York World's Fair, combining elements of these technologies, William Gruber and Harold Gravese presented the "Viewmaster," a 3D imaging tool that was explained to be an update to the scenic postcard (World Fair, 1939). Thus, with the conceptualization of Weinbaum's goggles and centuries of technological advancements in image recreation, as well as sensory augmenting tools, the advent of Extended Reality was upon humanity. Less than three decades later, in 1963, Ivan Sutherland developed the Sketchpad, the world's first interactive graphics application at MIT (Sutherland, 1964).

Shortly after that, Sutherland moved to Harvard University, and in 1968, with Bob Sproull, he created the prototype AR system [Sutherland, 1968]. In 1977, DeFanti and Sandin at the University of Illinois created a wired glove that used electric signals and user control to computerize finger movement (DeFanti and Sandin, 1977). Quickly building on this development, in 1982, Thomas Zimmerman and Jaron Lanier built a hand gesture interface and data glove that laid the groundwork for the hand tracking devices we use today (Zimmerman, 1986). As the 1980s progressed, there was a series of immersive environments that used XR technologies, like NASA's Virtual Interface Environment Workstation (V.I.E.W.), the U.S. Air Force Super Cockpit program, VR group arcade games, and others before handheld devices were ushered in during the 1990s (Robotics Business Review, 2019). It was at this time, in the early 1990s, that research in the field began to accelerate. Some of the foundational institutional knowledge that is still referred to today began at the University of Washington, the University of North Carolina at Chapel Hill, Columbia University, and the University of Toronto, where some of the earliest researchers built out the infrastructure for the development of Extended Related (XR) technologies, specifically as they relate to head tracking, display, and interaction (Billinghurst et al., 2014). This research was not limited to North America. Researchers in Europe and Japan were also pioneering the hardware technology and the applications for commercial use. For example, in Japan,

Rekimoto and Schmalsteig investigated how Augmented Reality could be used for collaboration, a topic gaining increasing interest now in 2021 (Schmalstieg et al., 2002; Rekimoto, 1996).

Notably, during this time where researchers were thinking about expanding the use cases for XR technologies, there was also the rapid development of the actual hardware and software. AR hardware systems of the 1990's used large bulky materials, which was a sign of significant runway in front of the XR consumer products seen in 2021 and expected to arrive in the coming decade. However, GPS technology, tracking sensors, and computer vision software take hold (Rekimoto and Ayatsuka, 2000). By 2000, open-source software began gaining popularity, and ARToolKit, which still exists today in 2021, established itself as one of the fastest-growing tracking libraries (Kato and Billinghurst, 1999). This made it possible to store more data from situations like interacting with objects from the physical world and tracking a user's viewpoint. Rapidly, these capabilities were built on, and by 2003 wireless data transfer allowed for the processing of an AR overlay to remote devices. At first, these devices were traditional personal computers, and in that same year, AR applications were applied to handheld devices, which paved the way for the 2004 demonstration of the first mobile phone AR application. ARToolKit on mobile devices quickly followed, and now AR was introduced to the masses (Mohring et al., 2004; Henrysson and Ollila, 2004).

Like many innovative technologies, significant breakthroughs in the early 2000s came from joint venture activities between the public and private sectors throughout the world. One of the more consequential alliances was between Canon and the Japanese government, which lasted four years. This partnership focused on imaging systems, specifically 3-D (Ohshima et al., 1998). However, the high cost of content production and hardware limited most accessibility of these technologies to the entertainment industry (Billinghurst et al., 2014). In 2007, the Playstation 3's The Eye of Judgement was released, which allowed for direct, in-home use of XR technologies for consumers (Billinghurst et al., 2014). Other media companies got into the mix to provide consumers with a direct application of augmented reality in both N.F.L. games and during the 2008 Beijing Olympics swimming competition (Billinghurst et al., 2014). With the advent of smartphones gaining popularity in 2009, AR's commercialization provided access to billions of potential consumers. However, in 2013, as virtual reality applications in gaming became more prevalent due to the relatively lower cost of purchasing head-mounted display and flash-based development provided opportunities for web-based VR programs, which was much easier to code than traditional C/C# (Billinghurst et al., 2014).

Over the last several years, the pace of development and excitement around augmented reality and virtual reality has increased. Augmented reality is seemingly more accessible as Apple, and Android smartphones now have standard features that allow for augmented reality applications. While head-mounted AR is still going through trials on its pathway to mass commercialization, AR hardware and software made by Microsoft, such as the Hololens, is still out of reach for many consumers in early 2021, a price tag of more than $3,500 USD (Bohn, 2019). This has limited the integration of augmented reality into everyday life; however, very soon, more accessible headwear, increasingly being referred to as digital eyewear, is rumored to be created by companies such as Apple, which will exponentially increase the application and use of augmented reality in one's personal and professional life (Staff, 2021). For example, many of the most useful applications of AR going forward will be in education tools and workforce training since it will accelerate the ability to access information in a more 'natural' way.

Because AR blends the digital and physical world, as more devices are introduced into the market, there will likely be an exponential increase in uses and applications of the technology that will once again surpass virtual reality.

Simultaneously, the entertainment industry has carried forward and popularized virtual reality for millions of people. While diversity of virtual reality applications today are, arguably, more limited than AR, the hardware is much more affordable thanks to the Oculus Quest launch at a price point of around $300, which is less money than other new gaming consoles Sony PlayStation 5 and Microsoft's Xbox (Oculus Quest 2, 2021; BBC, 2020). As the application and use of virtual reality expand, the immersiveness will increasingly blend with our expectations of the physical world. Baseline VR will move beyond the visual and audio sensory experiences to include all senses like touch, smell, and potentially even taste (Ranasinghe and Do, 2016; Cater, 1994).

In order to understand the requirements to protect individual and group privacy, one must have an understanding of the technology. As the degree of integration of the following technologies differs across Milgram and Kishino's continuum, the following crucial technologies should be considered when assessing any XR technology (Brooks, 1999):

- Visual (and aural and haptic) Displays that immerse the user in the virtual world and that block out contradictory sensory impressions from the real world;
- Graphics rendering system that generates, at 20 to 30 frames per second (fps), the ever-changing images (today, the baseline has more than doubled to more than 60 fps) (Oculus-a, 2021);
- A tracking system that continually reports the position and orientation of the user's head and limbs;
- Database construction and maintenance system for building and maintaining detailed and realistic models of the virtual world.

In the twenty years since Brooks' research was published, there have been significant advancements in these required technologies; for example, the capability of graphics rendering has tripled from an expectation of 30 frames per second (fps) to 60-90 fps in current applications of XR (Brooks, 1999; Oculus-a, 2021). As the technologies' adoption accelerates in the coming years, what were once seen as complementary but not yet necessary technologies, will become fundamental requirements for XR experiences.

Four of these technologies that are seeing an accelerated adoption and integration with XR experiences are (Billinghurst, 1999):

- Synthesized sound, displayed to the ears, including directional sound and simulated sound fields;
- Display of synthesized forces and other haptic sensations to the kinesthetic senses;
- Devices, such as tracked gloves with pushbuttons, by which the user specifies interactions with virtual objects; and

- Interaction techniques that substitute for the fundamental interactions possible with the physical world.

Overall, while the technologies' capabilities are quite literally evolving each day, many initial researchers like Azuma, Brooks, Cho, Isdale, Kishino, Milgram, Nagao, Neumann, and Rekimoto envisioned, are just now seeing their way to the consumer market. These use-cases still serve as the foundation for XR experiences in 2021, but there have been significant changes in the capabilities and expectations from an experiential standpoint in XR. Following Moore's law, the advancements in processing power and decreasing costs for applying these technologies in consumer products like smartphones have served as an early tipping point for XR technologies.

WHAT IS THE GROWTH AND MARKET POTENTIAL

The growth and market potential highlights the need to be proactive in understanding how XR technologies will be applied and adopted in the coming years. According to multiple market research organizations, in 2019, the extended reality global market was just under $19 billion (Technavio, 2020; Mind Commerce, 2020). More importantly, these organizations also expect that number to balloon to nearly $200 billion by 2025, at a compound annual growth rate (CAGR) of more than 60%. While this type of growth is incredible, it may be just a conservative estimate as early numbers from 2020 show the XR industry to have grown from anywhere between $25-$45 billion (Mordor Intelligence, 2021). While there is some disagreement across organizations about the specific size of the market, due to how variables are included in the analysis, these organizations all agree that the growth will be explosive as society shifts to an interactive online environment (Mind Commerce, 20202; Technavio, 2020; Unity, 2020; XRA, 2020). Even more, XR will soon be approaching a viral-loop-like development due to increasing applications, resulting in more significant investments in these technologies.

In 2021, just under a half-decade since Niantic put the broadest introduction of augmented reality into the hands of consumers with Pokemon Go, there are still significant barriers limiting the potential for XR to reach scale across mass consumer markets. For virtual reality, consumer introduction has mostly taken place at theme parks or museum exhibits (Pausch, 1996). At the end of March in 2021, and as briefly mentioned above, most of the early uses of XR technologies could only be afforded by larger businesses and as a luxury item for some consumers (Sherr, 2019). For augmented reality, in addition to a consumer furniture application (as referenced above), the technology is currently being used for things like vehicle design and training procedures across industries (Aukstakalnis, 2016). There are neurology departments in the United States that use augmented reality to go beyond traditional 2-dimensional tools to prepare surgery and train medical students (EagleView Imaging, 2021). In VR, gaming and architectural design allow the individual to create and analyze new ways to envision spatial arrangement and constructing buildings, submarines, and deep-sea oil platforms (XRA, 2020). The use and application of XR technologies can ultimately digitally transform nearly every aspect of the natural world known to humans today.

To achieve this, the development of sensor technology has driven down the cost while increasing accessibility that pairs with existing advancements in camera technology that now allows for XR technologies to be more mobile (Patil and Kumar, 2020). Moreover, the XR industry has been forced to let both technological capability and market demand achieve greater alignment with each other, which

is evidenced by the development of more powerful computational processing, an application that can drive revenue in entertainment and workforce augmentation, as well as the advent of a more widely connected digital network unlocked by 5G technologies (Patil and Kumar, 2020). With the convergence of these complementary technology components, the XR market can begin to realize its growth potential.

MARKET SEGMENTATION OVERVIEW

Today's market, in early 2021, can often seem to be confusing to those less familiar with Extended Reality (XR). Even in business scenarios, there is a lack of clarity around the differences between Augmented and Virtual Reality use-cases. Technavio industry reports project Virtual Reality will encompass roughly 40% of the market, while Augmented Reality will result in ~35% while Mixed Reality grows to ~25% of the market by 2024 (Technavio, 2020).

To clarify this further, Mind Commerce segmented their 2020-27 market report, and it is helpful to think in terms of separate categories for now as the XR industry remains decentralized and fragmented. The >60% Compound Annual Growth Rate (CAGR) mentioned above is expected to reach just under 100 million units (Mind Commerce, 2020).

AUGMENTED REALITY

Enhancing the natural world with digital assets, when discussing Augmented Reality (AR), it is important to note that there are two types of Augmented Reality experiences, whose differentiation becomes increasingly more important as privacy and safety considerations are made. AR most often uses a smartphone/handheld device or head-mounted display (HUD), otherwise known as a device that sits on users' heads. The HUD may be the largest segment of growth in AR over the next seven years, with a Compound Annual Growth Rate (CAGR) of more than 90%. According to Mind Commerce, Marker-based AR, which uses a physical identifier to present a static 2D image that acts as a placeholder for the projected AR asset, currently presents the most value. Marker-less AR has the fastest individual growth rate from now until 2027, with a CAGR of 67% (Mind Commerce, 2020) . By 2024, that means results in ~$63 billion in incremental growth as annual recurring revenue is forecasted to exceed $70 billion. Marker-less AR uses depth sensors to detect the external environment GPS and high-powered computing speed to project digital AR assets, often against a clear lense of a HUD or through the high-resolution camera on a Smartphone (e.g., iPhone, Android). This means there are nearly two billion augmented reality devices in markets worldwide (Statista, 2018; Technavio, 2020).

VIRTUAL REALITY

In the same Technavio report referenced earlier, the firm estimates that by 2024, with a CAGR of ~60%, Virtual Reality will grow by nearly $70 billion to an estimated annual recurring revenue of greater than $75 billion (Technavio, 2020). The main benefit that Virtual Reality provides its users is a fully immersive experience that has provided enhanced education and entertainment value for consumers. VR devices have lowered the entry barriers for many XR users as smartphones are turned into screens and companies like Google have created low-cost headwear. Through individual entertainment activities like gaming and education, consumers are more frequently provided with VR experiences, even though most carry their handheld devices (i.e., smartphones) daily. HMDs allow the user to feel

completely immersed in another world, and where Augmented Reality enhances the natural world, VR relies on the experience a user has, not necessarily the functionality or utility. From early in its days in the late 1990s, 62% of users studied by Randy Paush's team at Carnegie Mellon and The Walt Disney Company felt they were in a dream when using early versions of VR(Pausch, 1996). To entirely suspend reality, Virtual Reality relies on its ability to provide three degrees of freedom (3DoF) tracking rotational movement, or six degrees of freedom (6DoF), which tracks translational movement in addition to rotational movement. As the range of motion capabilities continue to improve, it should be expected that the great functionality and expanded utility will also broaden the user base (Google, 2019).

MIXED REALITY

Mixed reality leverages the strengths of augmented and virtual reality to create a fully interactive experience. Growing the fastest over the next few years, according to the Technavio report, Mixed Reality has a CAGR of more than 65% and will top $50 billion by 2025 (Technavio, 2020). While it will remain the smallest market size in XR for now, it is mainly due to technological limitations with limited application development and accessibility for potential customers. In the coming years, MR will provide users the opportunity to blend the digital and physical worlds in real-time thoroughly. This could manifest in holograms that seemingly teleport individuals from one location to another (Looking Glass Factory, 2021). While technology has advanced to provide practical demonstrations and prototypes for what one can expect in Mixed Reality, to commercialize the more boundary-pushing MR experiences for mass consumption, the sensors and computational graphic rendering and processing power must be produced at a much higher level and less expensive price point (Patil and Kumar, 2020). In the meantime, Mixed Reality technologies can be achieved by blending Virtual Reality visual with Augmented Reality audio experiences (Nebeling, 2019).

MARKET SEGMENTATION BY COUNTRY

Throughout the world, more than 95% of XR technologies are currently being developed and deployed by North American, European, and Asia Pacific countries where network availability and speeds (i.e., 5G), disposable income, and manufacturing activities are taking place. However, Latin America is projected to have the highest CAGR of 75% between 2020-2027, with most of Brazil and Argentina's growth (Mind Commerce, 2020; Technavio, 2020).

According to multiple market reports published by Technavio, Mind Commerce, and Statista, China and the United States significantly outpace the rest of the world when it comes to worldwide spending (Statista, 2018; Technavio, 2020). As the world's two largest economies, it does not appear to change in the coming years as investments in technology-forward infrastructure plans are funded throughout both countries. These investments will expand the availability of 5G and Mobile Edge Computing technology and improve the capability of XR and the immersiveness and digital integration of the user experience, which will be imperative to achieve the growth targets (Patil and Kumar (2020).

INDUSTRY DRIVERS

According to an XR Association report, ninety-four percent of surveyed business leaders believe XR has practical applications for their industries: retail, job training, and public safety, but currently, only thirty-eight percent are deploying XR technologies (XRA, 2020). In an industry that is still being

defined, correctly identifying the market drivers is an essential task to ensure projections for the industry are met in the coming years. One can assume that consumer awareness and acceptance will be the most critical element to demand generation, but in order to achieve this, the technology needs to have compelling applications and services. Below are some key industry drivers that will help determine the degree of success that XR achieves in the coming decade:

- Sensor Technology: Improved user experience in XR is made possible, in part, by improved capabilities of the sensor. As demand and technological advancements of sensors (e.g., miniaturization) take hold, more efficient production should lower hardware makers' costs, which should be cost savings passed onto consumers. This is evident in the commercialization of Facebook's Oculus Quest 2, which now has a consumer price point of ~$300 (Oculus-a, 2021).
- Compelling Consumer Applications: In addition to consumer awareness and interest in purchasing XR hardware, there must be experiences in which it is worth spending time. As consumers become more familiar with some of the unique capabilities of XR, there will have to be a way to excite consumers and solve their real problems. From an entertainment perspective in VR, this has manifested in 360-degree videos and gaming applications (Billinghurst, 2014)
- Business-to-Business (B2B) & Military Apps and Services: While the consumer adoption curve continues to approach its tipping point, there must be uses and applications that deliver significant benefits for businesses. Whether it is workforce training, surgery prep at a hospital, or simulating military training, B2B applications will subsidize and justify the research and development needed to advance the XR's capability (XRA, 2020). For example, the United States Army has contracted Microsoft worth roughly $22 billion to develop augmented reality technologies (Matney, 2021).

Going forward, it's this rapid growth in the technological capabilities and ease-of-use that demonstrate we need to immediately address the privacy risks in the digital world as these immersive technologies present exponentially increasing challenges to a safe society in the coming years.

WHAT ARE THE RISKS & CHALLENGES

Given the (relatively) early stage of XR technology, several potential risks and challenges could limit the advancement and adoption of augmented, mixed, and virtual reality. Whether it is funding, technological capability, or user perception, there are a few ways that the above projections are not met. The risks and challenges that need to be overcome are, most importantly, those that will stifle innovation and increase user risk like increased cost of individuals' healthcare, personal safety from home invasion, continued acceleration of economic and social inequality.

- Venture Capital Investment & Expectations: Significant private funding for XR comes from venture capital (VC) investments. However, an issue that has arisen from VC's investment in XR is that it has timebound innovation that may not match the adoption and application curve in the general market. This is exemplified by VC's investment and subsequent unmet expectations of Magic Leap (Bloomberg, 2020). While there must be accountability in the expectations set for new technologies, it is important to not stifle innovation due to (relatively) arbitrary investment timelines that hinder the XR's progress, prioritizing a financial return ~7 years, rather than focusing the quality and capability of the innovation. After misjudging the initial timing for earlier

XR investments, recently, the investment community might be less committed to funding the innovation, which increases the importance of government funding to move XR technologies forward (Matney, 2021).

- Government Regulation: In addition to risks associated with funding, there are currently inconsistent and unclear laws and regulations that raise questions and uncertainty related to the governance of XR technologies. Given the blending of the digital and physical world, there must be added clarity around governance at the local and national levels to streamline innovation and ensure continuity throughout the XR ecosystem (Dick, 2021).

- Consistent, Reliable Internet Access (Hughes, 2021): As mentioned earlier and discussed in more detail below, accessibility to low-latency internet access that complements the computing and processing power of XR technologies will be vital to broadening the uses of XR technology, as well as the experience. In addition to internet speed, a key factor will be cloud and mobile edge computing, which offloads some of the data processing and storage requirements for the XR hardware in public spaces.

- Individual and Community Privacy and Safety (Hosfelt et al., 2020): Privacy and Safety will present ongoing challenges to the industry's development. Never fully addressed in the two-dimensional online world where phishing attacks have exposed users to financial and personal risk, in immersive technologies (i.e., XR), there will be increasing privacy and safety concerns that present challenges with implications, potentially, to one's physical safety. Two major drivers of this challenge Without changes to how privacy, specifically the process for obtaining digital consent, is managed, there will be outsized safety risks to users and their family and friends (Miller and Herrara, 2020).

While there are many significant risks and challenges to consider, there are indications that the current and budding industry trends will address many of the current roadblocks to achieving the potential discussed at the beginning of this section.

BUSINESS AND SOCIAL TRENDS

The following trends provide insight into how, as the second or third wave of XR arrives, one understands previous levels of excitement around XR; the following trends are creating the momentum to meet the industry drivers:

- Adoption of 5G and Cloud technology (Pham et al., 2020): Over the next year or two, 5G will be deployed worldwide. This will allow for less latency and the speed required as well as added comfort for the user. As the industry ushers new technological features, such as high bandwidth and low latency, this technology can accelerate the adoption of extended reality products and ensure higher flexibility in various extended reality applications.

- Increasing Demand from Cost-savings for Gaming, Government, Healthcare, and Retail (XRA, 2020): Whether it is helping retailers turn your home into a digital showroom to help you buy

furniture, VR assists entertainment companies with more immersive gaming environments that allow you to suspend your reality, or use by the military to more effectively train soldiers at lower cost employees deploy XR technologies to address constituent issues in real-time has been increasing excitement and demand more generally.

- Rapid developments in sensor technology: As stated above, driving down the cost of sensors is imperative to lowering the acquisition cost for XR. Additionally, by shrinking the size of these sensors, it will become easier and more accessible for mass production.

With this level of growth, likely more than 60% over the next five to six years, and the existing issues related to consent, it is imperative that action be taken to pre-emptively understand the implications to privacy (and increases user safety) of XR Technologies. The importance of doing so before the technology reaches ubiquity results from lessons learned over the last decade about the impact that social media has had on disinformation and the blending of the digital and physical worlds foundational to the activities in immersive environments. What could be considered as only a privacy issue for the online world (it is not, which will be explained more later in the thesis) becomes both a privacy and safety issue that must be addressed in XR. To understand how to adapt consent and choice in these environments, I worked to understand how organizations across the XR industry can work together to develop technologies and policy that meets the dynamic and changing needs of those in XR.

PRIVACY IN XR

At the center of this urgency is that XR technologies are quickly developing, and in parallel, translating into real value for both consumers and business organizations (Yaoyuneyong et al., 2016). It should follow that as XR technologies create more value, there will begin an exponential increase in the production and use of these XR technologies and much greater levels of privacy issues. This is made evident in Kent Bye's XR Ethics manifesto, where he shows how with each application of XR technology that gets shared with a third party, the existing legal frameworks that protect ones' private information, like the Third Party Doctrine in the United States, which states that if your data is shared with a third party then your expectation of privacy is revoked, and this erodes the ability to protect the collective whole (Bye, 2019).

In understanding that each degree of movement made possible by the 3DOF or 6DOF headsets, for example, turns into a data point that could be shared with third parties and allow for inferences to be made about every single movement and individual makes and it introduces the risk that in XR the subconscious can be quantified (de Guzman, 2019). Moreover, as the external environmental data is captured, there is more significant uncertainty about how individuals can control their right to privacy (de Guzman, 2019). Unfortunately, it is not just the data capture and prospect of a permanent digital footprint that may be at stake. However, there is also potential that, in an extreme example for effect, a person could lose their individual liberties as they become more dependent on the assistive nature XR technologies can create and cannot control the use of their data over time (Werro, 2020).

While there is not currently a federal law, similar to Europe's GDPR that will be discussed in more detail in the Results, Discussion & Analysis chapter, there have been more prominent warnings that the U.S. should not adopt a watered-down version of the GDPR given the gaps it already presents in today's

digital environment (Hartzog and Richards, 2020). Currently, there are few privacy policies in XR that deviate from the exceedingly long terms and conditions and binary method of clicking a box to consent [de Guzman et al., 2019). That said, organizations like the XR Safety Initiative have published frameworks with recommendations for XR that serve as a foundation for this discussion (XRSI, 2020).

Companies are currently using legal ambiguity to their advantage by writing vague privacy policies that could be argued are incomplete documents as seen later in the Unity Technologies privacy policy. Most privacy policies are presented as a terms and condition pop-up in the user's XR experience. When it comes to privacy in XR, AccessNow has published one of the more comprehensive overviews of not only the industry but specifically privacy (Oribhabor et al. 2021). But again, while there is a mention of the importance that consent plays in the space. Improving the way in which consent is given i cannot be ignored in digital privacy and especially in XR. It is already proven by Hillman that users do not take the same level of care in agreeing to a legal requirement in online privacy agreements (Hillman, 2005). Furthermore, Luger highlights the need to take a broader understanding of societal context when defining consent in Extended Reality (Luger, 2012).

Even more pressing is the fact that these discussions have not been had in a sufficient manner. In a review of the best practices of privacy policies in XR, there is significant amount of guidance on the ethics and moral code, but very limited research related specifically to consent (Brey, 1999; Adams et al.,2018; Wassom, 2014; Madary and Metzinger, 2016). Underscoring this point, Mozilla, published their ethical considerations for XR (Mozilla 2021).

1. Educate and assist lawmakers
2. Establish a regulatory authority for flexible and responsive oversight
3. Engage engineers and designers to incorporate privacy by design
4. Empower users to understand the risks and benefits of immersive technology
5. Incorporate experts from other fields who have addressed similar problems

Unfortunately, the efforts made by Mozilla are one of the best representations of what companies have done to promote privacy and safety in XR. Even more concerning is the fact this sole group that working on defining what could be considered as an ethical standard for immersive technologies was disbanded in late 2020. The substantial majority of work that has been done to focus on consumers in XR has been from the product lens like we've seen with Snapchat's AR filters, which amount to little more than immersive advertising (Talbot, 2019).

Ch. 3: Methods

The main research methods used in this study consisted of content analysis and expert and practitioner interviews. The novel XRSI Privacy and Safety Framework served as the starting point of this research as I completed a detailed analysis, which was followed by expert interviews to understand the recommendations introduced by XRSI.

This content assessment of the XRSI Privacy and Safety Framework showed a lack of content and context surrounding consent and choice in extended reality, so through a survey, I worked to understand the minimum, desired, and ideal ways developers and organizations can gain consent while optimizing awareness and understanding, and choice for consumers. Choosing to focus on consent was an important decision because it has been manipulated to strip consumers of their rights while businesses drive revenue off of personal information (Acquisti, 2014).

The insights from individual interviews with industry professionals should help academics, industry, and policymakers inform operationalization and refinement of the XRSI Privacy and Safety Framework by understanding the limitations and constraints when developing and commercializing extended reality applications. Beginning to bridge the gap between privacy advocates that will promote a greater degree of privacy-protecting behavior on behalf of consumers and industry organizations that often prioritize revenue growth over consumer needs. The outcome provides more precise guidance on integrating the XRSI framework with the industry leaders' realistic limitations and constraints when developing extended reality applications.

METHODS OVERVIEW

Through this research, by working with diverse group stakeholders, I sought to identify compromises that can serve as a foundation as extended reality applications achieve ubiquity. The outcomes from this research provide a better understanding of whether protecting consumer privacy can be prioritized with or without legislation and are there ways to improve the development and utility of the XRSI framework that will placate both parties until we learn more about the adoption of extended reality for both consumers and businesses, and the consumption of data by first and third parties across industry players.

Specifically, this research process consisted of two phases:

Phase 1 - Content Analysis: For the content analysis, a thorough review and completing a critical analysis of the XRSI Privacy and Safety framework to inform specific research questions that would ultimately serve as the foundation for my interviews. The analysis included a read-through of the XRSI framework to identify opportunities for additional research. Following the collection of notes, the critical areas for review (Consent & Choice) were identified in a systematic and detailed point-by-point breakdown of the information from each section of the framework necessary for understanding the hurdles and incentives to improving consent and choice in XR. The missing information presented gaps that ultimately prompted the questions that served as the foundation for the individual interviews later in the research process.

Phase 2 - Individual Expert Interviews: The interviews were informed by an XRSI Privacy and Safety framework analysis after identifying areas where detail was not provided about specific guidance for privacy management. For example, in the Inform section (1.5.2), when focusing on consent, the section had tiered and specific recommendations for minimum, desired, and ideal expectations in XR that allowed one to understand the potential application XR fully (XRSI, 2020). However, there was not much more than a definition provided in the sections discussing consent and choice. To address this, after gaining approval from the IRB, I focused on asking and answering the questions that help understand the varying levels (i.e., minimum, desired, ideal) of privacy and safety, consent, and choice for stakeholders across the XR Ecosystem. Ultimately, this and future research aim to provide answers and recommendations into the rationale for a collaborative approach to privacy design throughout the XR industry that will improve consent and choice in the digital age.

By combining these two research methods, the research sought to understand the benefits and risks for consumers, policymakers, academics, and industry leaders that will create the environment for which we use extended reality hardware and content applications.

STUDY PROCESS & OVERVIEW

The interview method was a semi-structured interview that were conducted via Zoom default video with an audio-only option to interview. The interview script was designed with specificity in mind to get a better understanding of the interviewee's connection to the XR industry and answer the following general questions:

- About the interviewee's role in XR and their proximity to privacy-related issues, which was not only crucial in understanding their general interest in consent and choice in XR but also to better frame the specific questions throughout the interview and compare the type of impact the interviewee believes they may contribute to the development of consent and choice in XR.
- Discuss and get feedback on participants' understanding of specific parts of the existing XRSI Privacy Framework, like their perspective on whose responsibility it is to define and design privacy policies in XR. This is important because it identifies where the industry perceives the ultimate authority to be held by.
- Identify participants' specific interests, constraints, and future related to privacy in XR within the context of their particular professional group (e.g., industry private sector professionals, non-profit privacy advocates). These interests and constraints help inform the incentives and hurdles currently in place within the XR ecosystem. Moreover, to make progress toward enhanced methods of gaining consent, it is essential to understand more about the history of the levers that have resulted in the current state of consent and choice. Finally, by understanding the future interest of the interviewee, more general assumptions could be made about their interest in promoting enhanced consent and choice in their given professional capacity.

The median time for the interviews lasted 45 minutes in the semi-structured format. The longest interview lasted 65 minutes and the shortest interview was 29 minutes. Because this study collects information about individuals, the primary risk was a loss of confidentiality. To mitigate data loss and ensure confidentiality, individual interview record(s) were codified to anonymity. To earn IRB approval and protect interview, a separate file creating a key with the code(s) used to anonymize the data, and

any individually identifiable information will be stored in a different location. There were two additional locations where data was stored, and the data storage was designed so that it would be necessary to have access to three separate files, in three separate file locations, to identify a single interviewee. The anonymized data was held on a local storage drive. Moreover, the data key has been stored in a separate University of Michigan Google Drive account. Access to the files was only provided to the primary researcher.

The process for anonymizing the data was threefold. First, I assigned individual code names (e.g., xr1) to participants. Before the interview, selected participants had a unique interview script generated to their anonymous participant code. Finally, I separated any identifiable contact or demographic data into a separate Google spreadsheet.

HOW WERE PARTICIPANTS RECRUITED?

The research goals were accomplished by speaking with 29 Experts and practitioners from across the XR industry to understand what might be possible as it relates to the future of privacy in XR and provided practical guidance for both industry organizations and government to deploy sufficient privacy protections for consumers and companies that adopt and continue to use XR in the coming years.

To do so, I compiled a list of potential interviewees by seeking out experts at XR organizations and reached out to via social media (e.g., Linkedin, Twitter) and directly emailed to schedule time for an interview. I relied on my primary and secondary professional networks to help drive participation. To help with participant recruitment, I asked people such as my thesis advisor, Florian Schaub, and the XRSI CEO Kavya Pearlman to share a standardized participation request sent via email and posted on Twitter. Of the 29 interviewees that I spoke with, 22 came as a referral from the XRSI, which could be seen as a limitation in my research. However, nearly all of these participants were not involved in the XRSI Privacy and Safety Framework development; they're more-so just part of the XRSI mailing list.

To optimize efficiency during the recruitment efforts, prospective participants solicited from social media were directed to participate in an ingestion survey via the University of Michigan Qualtrics platform. This survey provided the confidentiality and consent agreement for taking part in the online Qualtrics survey and the following interview(s) as a part of this ingestion survey. The ingestion survey was requested information about the professional and personal interest in XR, professional role and collected limited demographic information (e.g., gender, geography). Participants solicited directly via email were provided with the opportunity to consent at the beginning of the interview verbally. There were two instances where interviewees asked not to be recorded, so only written notes were taken.

STRUCTURE FOR DATA ANALYSIS

Information from each question was first added to a single summary page in the locally-stored excel file. Then, each question was organized into its tab, so each participant's coded answer to that specific question is available. The next step was to identify similarities and differences across participants' answers. After similarities and differences were identified, the themes that emerged were named and categorized for an aggregated data analysis that provided themes for each question and a corresponding set of responses. The next step was to see how the generalized answers for individual questions relate to each other to identify any insights derived from the interviews. Ultimately the goal is

to provide a perspective on the relationship for the organized themes on the application and/or use across stakeholders seeking to understand existing and potentially establish new expectations and norms for privacy and consent in XR. This established an adoption criteria and ranking integral to the recommended next steps for applying this data by private industry, non-profits, and the public sector rooted in the feasibility across the XR privacy landscape.

Ch. 4: XRSI Privacy and Safety Framework Analysis

The XR Safety Initiative (XRSI) has published its XRSI Privacy and Safety framework in late 2020 to serve as “a baseline approach to research, guidance, design, development, and thought leadership for privacy” in Extended Reality (XR). Its primary 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” (XRSI, 2020)

The XRSI Privacy 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. Its goal is to provide initial guidance to members of the XR community for how to incorporate privacy considerations into the development and deployment of their work in the XR space. The XRSI 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 (XRSI, 2020):

- Leave no one behind
- Be accessible: Everyone must be able to participate in the digital society
- 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
- Keep everyone safe and secure: Shape rules and practices to enable a secure and resilient immersive environment

Build new rules to promote trust: Develop new, flexible, participatory governance mechanisms to complement traditional policy and regulation in a constantly evolving domain

The document provides a flexible framework with *only* recommendations hoping that organizations actively develop guidance and policies for privacy and safety in XR. Currently, information is limited, and/or regulatory procedures in place state confidently that harm to humanity is protected when using XR technology, which creates challenges addressing "the most significant challenge lies in addressing how that data is collected, processed, stored, and destroyed safely and ethically" (XRSI, 2020).

The XRSI Privacy Framework has four main foundational components that I have summarized below:

1. Assess - Data sets are complicated. Organizations should assess which data are required for a specific activity and further define which data are essential to operate the XR technology

2. Inform - Privacy needs should stem from legally defined privacy rights, which should be communicated to understand individuals’ expectations.

   Note: it is in the Inform section that contains Consent and Choice

3. Manage - Organizations should have controls allowing them to take action to protect data

4. Prevent - Security and policies maintained to prevent harm

Additionally, across many stages of the framework, there are three levels of privacy outcomes, each with a progressively more stringent recommendation. Below, the three levels are outlined, and because these levels are applied throughout the XRSI framework, they are included below in Figure 2**.**

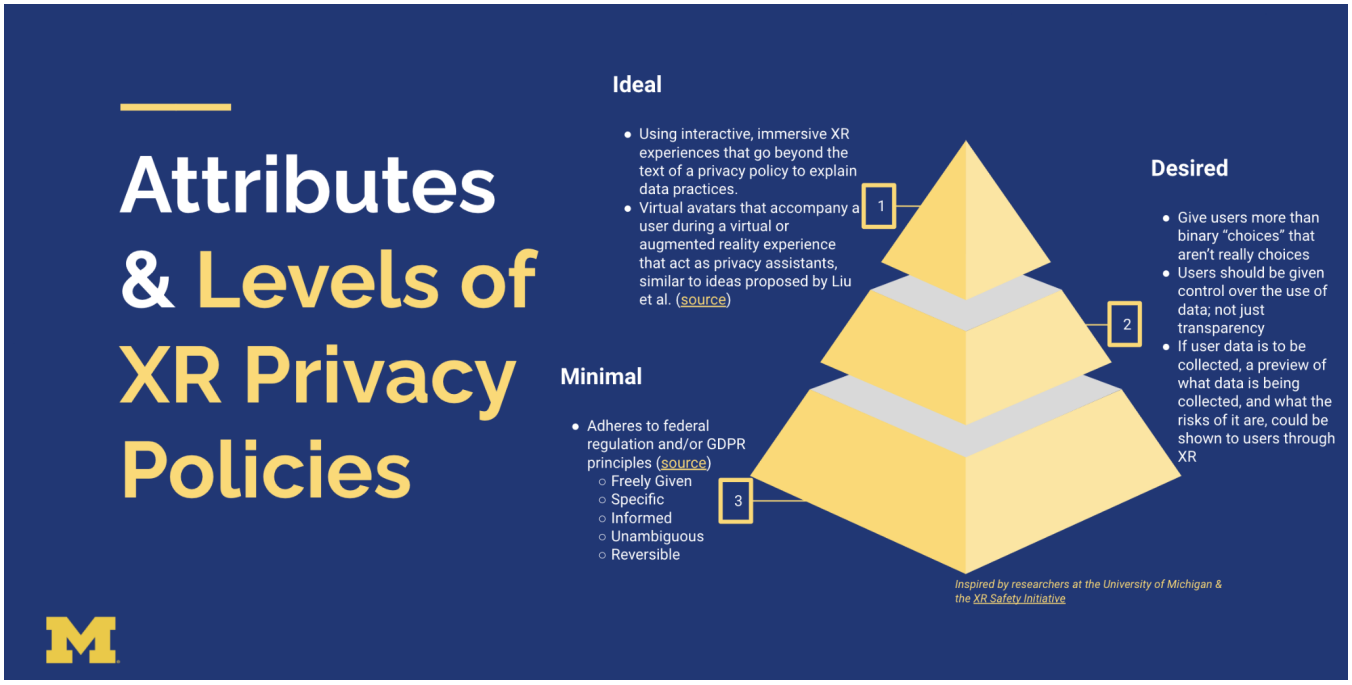


Figure 2: XRSI Proposed Privacy Levels

These tiers do not exist for the Inform (1.5) section's consent and choice, which is why this research decided to prioritize the Inform section. Moreover, after analyzing both the point-by-point recommendations in the XRSI's core foundation document, the following questions stood out as areas that could be addressed by speaking with stakeholders throughout the XR ecosystem during the interview portion of the research.

- Minimum
    - *Question: Given that very little is defined by federal law in the United States, how can one be assured that the organization properly fulfills its obligation?*
    - *Question: What does the minimum level of protection provide?*
- Desired
    - *Question: What must be valid for organizations to move privacy practices from minimum into desired requirements*
- Ideal
    - *Question: Does the ideal state go far enough, or too far, in protecting users (across the four components of the XRSI framework)?*

The framework's baseline is "privacy by design" and "privacy by default" baked in, driven by trust, transparency, accountability, and human-centric design" (XRSI, 2020). However, one of the biggest

questions that this research will begin to help answer is: to what degree organizations can deploy a focus on privacy that will result in deeper consumer trust without compromising their existing business model; especially as this trust and transparency might result in more significant value creation for the XR organization.

Organizations can improve trust by proactively moving beyond the status quo of complex and convoluted privacy policies. In Article 4, the GDPR defines consent as an "indication of the data subject's wishes by which [they], by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." According to the GDPR, this consent must meet five metrics: it must be (1) freely given, (2) specific, (3) informed, (4) unambiguous, and (5) reversible (GDPR, 2016).

The XRSI Privacy Framework v1.0, section 1.5.1 (Privacy Policies) calls for legally compliant privacy policies. However, privacy policies have often been written within a legal context and/or use jargon terms that few people can read and/or understand (Navaro, 2019). This is a problematic process for obtaining consent because organizations rely too heavily on presenting notices and an over-abundance of relevant and potentially irrelevant information but often do not provide alternative terms or appropriate context for which an individual can make an informed decision. For example, even before the popularization of mobile apps, IoT, and XR, if someone wanted to understand their privacy rights, researchers estimate that it would take ~220 hours for someone to read the privacy policies word-for-word every time they visit a new site or use a new digital product in a given year (McDonald and Cranor, 2008). Moreover, consent in the physical world is not always granted in this way, so it is unreasonable, especially in XR, that the existing method for obtaining consent in the digital world IS jargon-heavy and obscure terminology when trying to use a digital product.

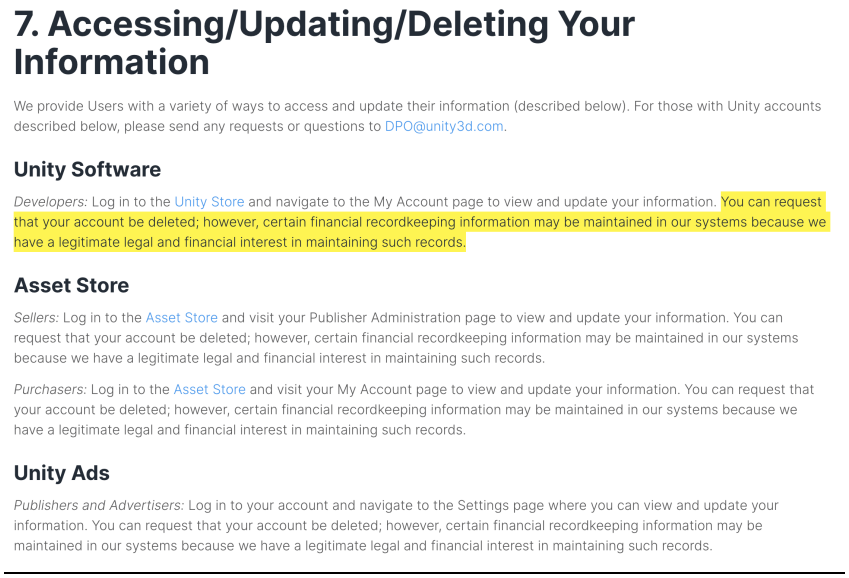
Instead, alongside privacy policies, there should be human-readable resources that explain the same information in the privacy policy but accessible to a broader audience. The GDPR provides a template for a privacy notice, but even this can be long and add unnecessary complexity for users (GDPR, 2016).

Below, I will outline an example of where there are issues in applying privacy policies in XR. I have chosen Unity as an example, not because they are the worst offender, but rather because of their ubiquity across the XR industry. They are by no means the only organization that continues to practice in a way that limits their privacy and safety efforts to the GDPR, but the following examples should provide sufficient context to understand the rest of this thesis.

> **Unity Example:** *Efforts to gain consent still lack transparency and are not sufficient efforts to protect users*
>
> The XRSI Privacy Framework section 1.5.2 discusses models of consent today that rely on the assumption every person using a digital product (e.g., iPhone, Oculus Quest) has an equal ability to access and understand the range of a digital product's capabilities. This is a problem in the context of a legally binding agreement and evidenced throughout Unity's privacy policy through its avid commitment to redirecting users looking to limit their consent or redirect users in

a confusing effort to collect and use an individual's information (Unity, 2020). In XR, these policies can be disconnected between the hardware and/or software experience. This is problematic because people are even less likely to seek out the privacy policy if they have to locate it outside their use context (Schaub et al., 2015).

As shown below in Figure 3, starting in Section 7 of Unity's privacy policy: Accessing/Updating/Deleting Your Information, at best, the organization goes out of its way to limit the way data is shared by a user. It is important to note that the only sub-sections relate to advertising and commerce-related activities, yet Section 7 is the only dedicated area that focuses on the action users can take to directly understand how to access, update, or delete information. From the onset, it guides users to email what appears to be a standard inbox and does not provide any assurance or guidance for how to resolve issues. Specifically, the policy directs individual users (i.e., Purchasers) to go to their provider to request some data get deleted. Still, Unity immediately follows that stating their 'legitimate legal and financial interests' might prohibit your ability to delete data, which violates a fundamental element of proper consent: the ability to use a product or service but not agree to its terms. Thus, the only unstated way to maintain control over a user's data is to completely opt-out of the service.



7. Accessing/Updating/Deleting Your Information

We provide Users with a variety of ways to access and update their information (described below). For those with Unity accounts described below, please send any requests or questions to DPO@unity3d.com.

Unity Software

Developers: Log in to the Unity Store and navigate to the My Account page to view and update your information. You can request that your account be deleted; however, certain financial recordkeeping information may be maintained in our systems because we have a legitimate legal and financial interest in maintaining such records.

Asset Store

Sellers: Log in to the Asset Store and visit your Publisher Administration page to view and update your information. You can request that your account be deleted; however, certain financial recordkeeping information may be maintained in our systems because we have a legitimate legal and financial interest in maintaining such records.

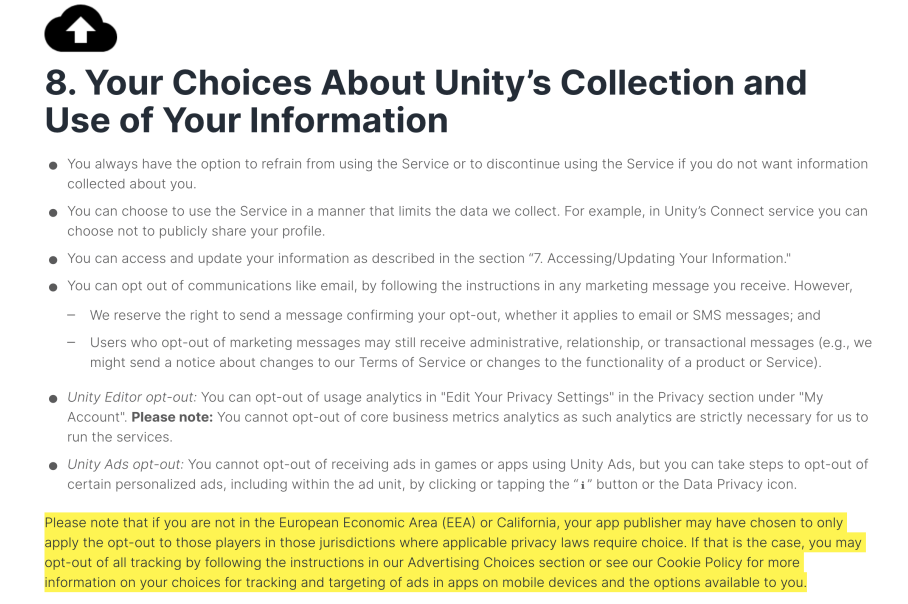
Purchasers: Log in to the Asset Store and visit your My Account page to view and update your information. You can request that your account be deleted; however, certain financial recordkeeping information may be maintained in our systems because we have a legitimate legal and financial interest in maintaining such records.

Unity Ads

Publishers and Advertisers: Log in to your account and navigate to the Settings page where you can view and update your information. You can request that your account be deleted; however, certain financial recordkeeping information may be maintained in our systems because we have a legitimate legal and financial interest in maintaining such records.

Figure 3: *Screenshot from Section 7 of Unity's Privacy Policy*

To make matters worse, in Section 8 of Unity's Privacy Policy: Your Choices About Unity's Collection and Use of Your Information, the number one option provided to a user is not actionable guidance on Choice. Instead, this section begins by telling the user that if they do not want information collected about them [the user], they can refrain from using the Service. That type of ultimatum can and probably should read as a threat stated more simply: If you do not like what we are doing, there is nothing you can do about it. Continuing in this section, the opportunity for Unity is to not only provide a privacy policy that states what you can do, but sufficient transparency should provide pathways to act. Instead, this section continues embedding the procedures to protect one's privacy exposure in confusing paths and misdirection across the platform. Even more, each action contains a significant number of qualifications or limitations to the degree to which one can genuinely opt-out. Unity's ultimate abdication stems from its deflection to the legal jurisdictions and third-party operators and publishers for which the platform relies upon, essentially punting responsibility to other entities.



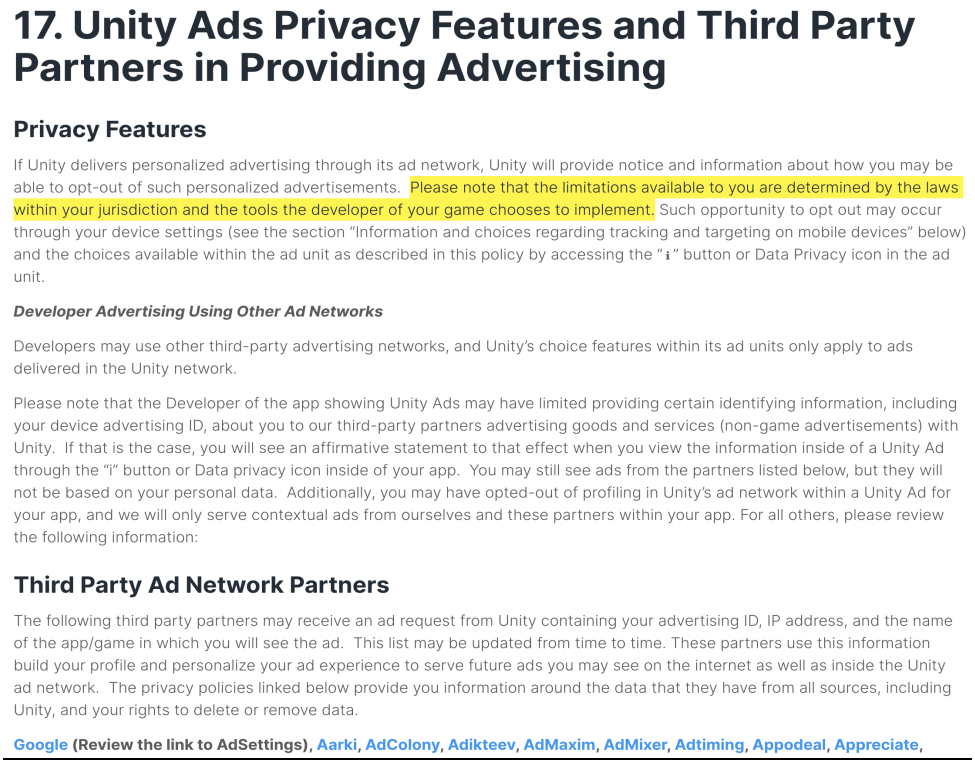
8. Your Choices About Unity's Collection and Use of Your Information

- You always have the option to refrain from using the Service or to discontinue using the Service if you do not want information collected about you.
- You can choose to use the Service in a manner that limits the data we collect. For example, in Unity's Connect service you can choose not to publicly share your profile.
- You can access and update your information as described in the section "7. Accessing/Updating Your Information."
- You can opt out of communications like email, by following the instructions in any marketing message you receive. However,
  - We reserve the right to send a message confirming your opt-out, whether it applies to email or SMS messages; and
  - Users who opt-out of marketing messages may still receive administrative, relationship, or transactional messages (e.g., we might send a notice about changes to our Terms of Service or changes to the functionality of a product or Service).
- *Unity Editor opt-out:* You can opt-out of usage analytics in "Edit Your Privacy Settings" in the Privacy section under "My Account". **Please note:** You cannot opt-out of core business metrics analytics as such analytics are strictly necessary for us to run the services.
- *Unity Ads opt-out:* You cannot opt-out of receiving ads in games or apps using Unity Ads, but you can take steps to opt-out of certain personalized ads, including within the ad unit, by clicking or tapping the "i" button or the Data Privacy icon.

Please note that if you are not in the European Economic Area (EEA) or California, your app publisher may have chosen to only apply the opt-out to those players in those jurisdictions where applicable privacy laws require choice. If that is the case, you may opt-out of all tracking by following the instructions in our Advertising Choices section or see our Cookie Policy for more information on your choices for tracking and targeting of ads in apps on mobile devices and the options available to you.

Figure 4: Screenshot from Section 8 of Unity's Privacy Policy

This lack of real accountability and responsibility for adequately allowing genuine consent on the Unity platform is emphasized in Section 17: Unity Ads Privacy Features and Third Party Partners in Providing Advertising (see: Figure 5). Unity defers to individual jurisdictions in this section rather than taking a centralized, unified stance at deploying a privacy policy. This sends a dangerous message to developers and other partners that Unity will only limit your infringement on human rights as the local jurisdiction mandates. This abdication of standardizing user rights to grant and revoke consent to privacy policies becomes even more dangerous when collecting biometric data.



17. Unity Ads Privacy Features and Third Party Partners in Providing Advertising

Privacy Features

If Unity delivers personalized advertising through its ad network, Unity will provide notice and information about how you may be able to opt-out of such personalized advertisements. Please note that the limitations available to you are determined by the laws within your jurisdiction and the tools the developer of your game chooses to implement. Such opportunity to opt out may occur through your device settings (see the section "Information and choices regarding tracking and targeting on mobile devices" below) and the choices available within the ad unit as described in this policy by accessing the "ℹ" button or Data Privacy icon in the ad unit.

Developer Advertising Using Other Ad Networks

Developers may use other third-party advertising networks, and Unity's choice features within its ad units only apply to ads delivered in the Unity network.

Please note that the Developer of the app showing Unity Ads may have limited providing certain identifying information, including your device advertising ID, about you to our third-party partners advertising goods and services (non-game advertisements) with Unity. If that is the case, you will see an affirmative statement to that effect when you view the information inside of a Unity Ad through the "i" button or Data privacy icon inside of your app. You may still see ads from the partners listed below, but they will not be based on your personal data. Additionally, you may have opted-out of profiling in Unity's ad network within a Unity Ad for your app, and we will only serve contextual ads from ourselves and these partners within your app. For all others, please review the following information:

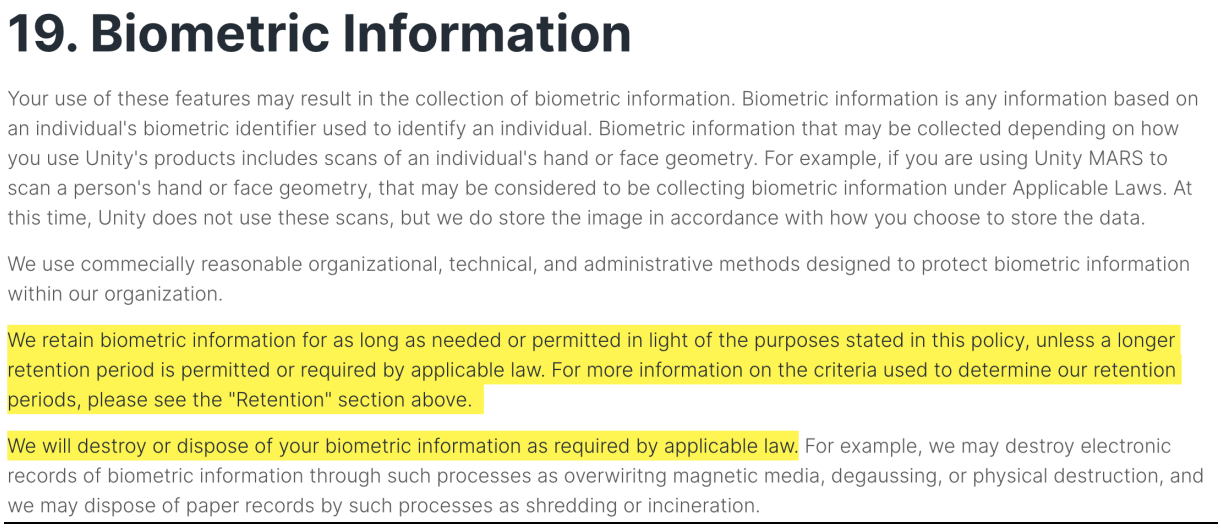
Third Party Ad Network Partners

The following third party partners may receive an ad request from Unity containing your advertising ID, IP address, and the name of the app/game in which you will see the ad. This list may be updated from time to time. These partners use this information build your profile and personalize your ad experience to serve future ads you may see on the internet as well as inside the Unity ad network. The privacy policies linked below provide you information around the data that they have from all sources, including Unity, and your rights to delete or remove data.

Google (Review the link to AdSettings), Aarki, AdColony, Adikteev, AdMaxim, AdMixer, Adtiming, Appodeal, Appreciate,

Figure 5: Screenshot from Section 17 of Unity's Privacy Policy

Buried in Unity Privacy Policy, Section 19: Biometric Information (see Figure 6), is an opaque and confusing explanation that implies no more than the biometric data will be stored and retained for as long as 'needed or permitted.' This is exceptionally alarming because, in this section, Unity does not even bother to commit to not using these data in perpetuity or specify the limitations that a user can understand. Problematic for its inconsistency and incomplete information, even more so, given the developing use of technologies like eye-tracking, the little explanation misses an opportunity to properly inform users for how they might use this technology and why it is vital collect. This is just another example of where Unity's Privacy Policy is unclear and one-directional in its effort to gain users' consent, one that should alarm anyone hoping that technology companies have begun to prioritize a consensual relationship with their users.



19. Biometric Information

Your use of these features may result in the collection of biometric information. Biometric information is any information based on an individual's biometric identifier used to identify an individual. Biometric information that may be collected depending on how you use Unity's products includes scans of an individual's hand or face geometry. For example, if you are using Unity MARS to scan a person's hand or face geometry, that may be considered to be collecting biometric information under Applicable Laws. At this time, Unity does not use these scans, but we do store the image in accordance with how you choose to store the data.

We use commecially reasonable organizational, technical, and administrative methods designed to protect biometric information within our organization.

We retain biometric information for as long as needed or permitted in light of the purposes stated in this policy, unless a longer retention period is permitted or required by applicable law. For more information on the criteria used to determine our retention periods, please see the "Retention" section above.

We will destroy or dispose of your biometric information as required by applicable law. For example, we may destroy electronic records of biometric information through such processes as overwiritng magnetic media, degaussing, or physical destruction, and we may dispose of paper records by such processes as shredding or incineration.

Figure 6: Screenshot from Section 19 of Unity's Privacy Policy

> Presenting a binary choice, one where a user either agrees to the terms set by an organization's legal team or not using the product/service imposes consent to a broad range of circumstances before understanding or experiencing the various ways one will use the digital product. Even more, developers are carrying binary measures to gain consent in the XR experience, which continues to ignore the unhealthy power dynamics and misses an opportunity to use enhanced consent models to engage the user.

Using this example from Unity's privacy policy as a foundation that compliments my analysis of the XRSI framework, part two of this research sought to answer questions of industry experts to understand if perspectives of these experts match the reality of what is seen in the market (i.e., Unity example). The interviews, as mentioned above, will mainly concern themselves with the second component of the XRSI Privacy and Safety framework, Inform, which is further broken out by consent, context, choice, and control. Throughout these interviews, all four of these topics were discussed; however, there is the most glaring discrepancy between industry actions and expert perspectives related to consent and choice, which has resulted in my focus on these areas.

Ch. 5: Interview Results, Analysis and Discussion

A note on the following chapter: the interview results, analysis, and discussion will be in individual sections that are bucketed by interview question. This is due to the fact that the analysis and discussion of these interview questions warrants an independent review and segmenting the chapter by interview question will help structure the analysis and discussion. The overall themes and takeaways will then be discussed in the Conclusion (these questions due to the numerous questions and points of reference

Participant Overview

Moving onto the interviews, the research was conducted over three weeks in the Spring of 2021. The scope of the research included 29 individuals from across the world. Four continents were covered; participants from North America and Europe were the most frequent interviewees. Nearly 83% of the participants were from the United States, as depicted in Figure 7 below.

Geography	**COUNT**
USA	20
UK	3
Canada	2
Australia	2
Germany	1
Colombia	1
Grand Total	**29**

Figure 7: Current country

There was nearly an equal distribution of self-identifying men (n = 16) and women (n = 13). This is not representative of gender distribution throughout the industry but provides a sample size that is more in line with the general population. However, three quarters of the interview candidates represented were white, which is a shortcoming in this research.

Gender	**COUNT**
Male	16
Female	13
Grand Total	**29**

Figure 8: Gender

Race/Ethnicity	**COUNT**
white	21
Black, Indigenous, Person of Color	8
Grand Total	**29**

Figure 9: Race or Ethnicity

The interview participants spanned nine different professional functions throughout the XR ecosystem, as shown in Figure 10 below. The participants range from Academics and Activists to Industry professionals from both Big Tech and Independent (Indie) Developers. While most participants were from the private sector, the diversity of roles and functions stretches throughout the XR ecosystem. The participants also ranged in seniority from undergraduate students working part-time in XR to Senior Executives with multiple decades of experience. This range ensures that perspectives from nearly each part of the XR ecosystem were considered.

Role	**COUNT**
Independent Developer	7
Industry	6
Designer	5
Academic	4
Think Tank	3
Student	1
Legal	1
Journalist	1
Activist	1
Grand Total	**29**

Figure 10: Professional Role in XR Ecosystem

Coding Process

Many questions were asked to participants throughout the interview process; however, a few were asked to no less than 20 participants, and those questions have been prioritized in the below analysis. As stated in the 'Methods' chapter, a systematic process was followed for each question asked to interview participants. It followed 1) Isolating the question; 2) Summarizing each interviewee's answer; 3) Identifying themes amongst the answers and generalizing those answers into a handful of categories.

<u>QUESTION 1:</u> Whose responsibility is it to define privacy requirements in XR, and how should privacy protection be provided?

"I think it really, really comes down to everybody. I think it needs to be a conversation between the academics that are researching it, the government that sets fundamental laws, the industry companies that are creating these simulations, how the technology works, and how you can put those standards into place. And obviously, the users that are using the technology." Xr15

Takeaway: Interviewees stated that privacy in XR should be determined by a Multi-stakeholder group and noted, definitively, the importance that sole responsibility for definition is not granted to the private sector.

<u>Results</u>
After coding the answers in the three-stage process outlined above, the following answer categories were identified:

- Independent Standards Body
- Industry (Private Sector)
- Legal/Regulatory Body
- Multiple Stakeholder Group – Government, Industry, NGO, Consumer Advocates
- Third-Party (i.e., None of the above)

Recurring points of agreement or disagreement: Nearly two-thirds of respondents, 15 people, thought that a Multiple Stakeholder Group should be determining what privacy is required and how it is provided. In more than 90% of responses, there is an acknowledgment that either Industry or Legal/Regulatory Bodies have a responsibility to define XR privacy policies. Additionally, implied in the answers, 30% of interviewees thought that Industry should NOT be included in this process and the responsibility should fall to regulators or other independent bodies. Only two respondents believe that it should be the sole responsibility of the Industry to define these privacy policies.

Responsible Functional Group for XR Privacy Design	Total Respondents
Independent Standards Body	1
Industry	2
Legal/Regulatory	4
Multiple Stakeholders - Gov, Industry, Consumers	15
Third Party	2
Grand Total	24

Figure 11: Responsible Functional Group for XR Privacy Design

Discussion & Analysis

The most important finding for this question is the affirmation that across the XR ecosystem, there is a precise alignment that Industry should not be defining what privacy requirements are in XR. This is important because the functional diversity and distribution across interviewees, which transcends, on an individual basis, the argument that these findings could be disregarded as a subjective assessment based on one's own personal and professional priorities. Moreover, throughout the interviews, some of the more compelling methods for designing privacy in XR highlighted the importance of approaching privacy design from a cross-sectoral perspective. The agreement lies in the importance that contributions are not made in isolation or even within a specific sector (i.e., public, private, non-profit).

This clear alignment, shedding light on where the conversation can begin across stakeholder groups to find the compromise, clearly shows that Industry should not be excluded in the process of XR privacy design. The importance of including a collaborative, multi-stakeholder approach to privacy design will ultimately rely on the accountability related to the enforcement of the defined XR privacy policies. By collaborating on the initial design, there should be a greater level of transparency and communication across these functional groups. It was noted by several interviewees, across answers to multiple questions, that Industry has an essential role to play in communicating the technology requirements to not only ensure XR experiences can work as expected but also not stifle innovation in the underlying capabilities of Extended Reality (XR).

An acknowledgment of this research must be made, given that interviewees were addressed professionally and not directly as a consumer. As one interviewee stated, "I think there should be a collaborative approach in that, and that you need to understand users' concerns, like, what are privacy concerns of the users, and then you need to establish some baselines, and these need to be enforced." There may be significantly divergent opinions amongst consumers due to many factors; one may be a lack of holistic understanding of the privacy and safety implications in XR, so more work should be done to understand the perspective of consumers before the development of a multi-stakeholder body to define, design, and enforce privacy in XR.

The important distinction made by proponents of a multi-stakeholder approach to privacy design lies within the role that enforcement of privacy policies plays in defining what privacy in XR should look like. While key performance indicators for establishing measurements for governance can, and should, be jointly created across stakeholder groups, proponents for the multi-stakeholder approach are clear that governance (i.e., accountability and enforcement) should be managed by at least a third party (Jerome, 2021). More than half of all respondents, in an unprompted manner, further called out that enforcement will not be wholly enforced should it be left to the discretion of Industry players due in large part to the business model incentives of larger technology companies and the nebulous and complexity in navigating and adhering to requirements for Independent [Indie] Developers. There was pessimism on the probability for successful accountability, though, which can be summarized by interviewee xr24, "ideally, a company that is, like, you know, like Facebook, for example, or Oculus would integrate this [Multi-stakeholder recommendations] in their platforms." Therefore, this sort of feedback underscores the importance of legislating bodies' efforts and the sense of urgency they should place on these challenges.

Regardless, in the meantime, privacy advocates, academics and think tanks, and legal professionals should seek continued collaboration with Industry through a group like the XR Safety Initiative to co-create the privacy and safety requirements for Extended Reality.

One representative from Industry noted that the responsibility should be on the “the gatekeepers are the platforms.” While the prospect of Industry defining the rules for itself may be a point of contention for activists and privacy advocates, xr3’s proposal goes on to explain its relevance by sharing an example that “if you have Android or iOS, it is Apple or Google, who takes the first step to ensure that all these apps, third-party apps are not abusing the system it is possible to restrict to what is coming in from the platform that they are controlling.” This is an important point because these large technology companies control the experiences on their device that the XR industry may see initial cooperation around privacy. A further promising acknowledgment then followed from xr3 as they highlighted that “a better auditing system” could then be deployed to hold organizations accountable.

<u>QUESTION 2:</u> Is legal enforcement of the California Consumer Privacy Act /General Data Protection Regulation sufficient as a minimum expectation in XR?

"A lot of these laws do not cover a lot of the data that's collected in XR, especially biometric data, and especially the United States where we do not have a unified definition of what biometric information is. So that makes it super complicated for anyone developing XR to be compliant." xr8

Takeaway: A majority of interviewees stated that existing laws and regulations are insufficient for adequate protection in XR because of the lack of clarity in these laws and added experiential and technical complexity that is currently defined by law.

<u>Results</u>

Nearly two-thirds of interviewees believe that the existing California Consumer Privacy Act (CCPA)/ General Data Protection Regulation (GDPR) requirements are not sufficient as a minimum requirement to protect user privacy and safety in XR. While just over one-third of respondents stated that these laws were sufficient for XR users, in all but one of those responses, there was an immediate, unprompted, qualification that the creation of XR content must follow the law, and since these are the laws, they are sufficient. Inferring in this qualification, one could justify having also marked this response as a 'no,' that the existing legal requirements are not sufficient to protect privacy and safety in Extended Reality.

Are existing legal requirements for digital privacy and safety sufficient?	Total Respondents
No	14
Yes	9
Grand Total	23

Figure 12: Sufficiency of legal requirements to protect privacy & safety in XR

<u>Discussion & Analysis</u>

One of the most frequent explanations called out by interviewees for why these laws and regulations are insufficient is due to the additional complexity of choice and consent in XR. However, due to the blended and inherent nature of the digital and physical world, even the same individual data used in XR can have drastically different implications due to the scale and scope of data collection required for activities in XR. These technologies may introduce questions as to what we can define as a "natural person" because, as one interviewee put it, the current laws present "an awful compromise. You are combining pieces of data, which represents our soul" (Lenggenhager et al., 2004).

Additionally, this potential is important because of the possible negative implications for a natural person should a person's avatar, digital representation of oneself, be violated in a way that is deemed illegal in the natural/physical world (Bye, 2019). Throughout my interviews, this was a common concern voiced by multiple interviewees based on their first-hand experiences in social VR. In addition to the

negative psychological impact for the individual, the added confusion and a potential lack of trust surrounding the safety of XR could hinder the adoption and acceptance of XR technologies (Bozorgzadeh, 2019). Moreover, these issues and the corresponding experiences in a way that directly and indirectly stifles innovation and investment for XR tools. Much of what the GDPR protects is defined as personal data, which means any information relating to an identified or identifiable natural person ('data subject'). One example of added complexity arises in the requirement that a user must be 'alive,' which is complicated by the potential use of digital autonomous agents that could falsely represent and also act in a legal capacity as it takes the place of a natural person's identity while in an XR experience.

Using biometric data in the United States as an example, there is no federal-level guidance for how biometric data should be collected and stored, so individual states have created their laws (Kracht et al., 2018). This has created a set of decentralized, fragmented definitions for what biometric data can and should be (Dick, 2021). Multiple interviewees highlighted this as a significant concern because "looking at what qualifies as personally identifiable information and that [the biometric data collected] is the minimum amount of information it takes for somebody to recognize [the identity of another person]." While interviewees acknowledged that they do not want to stifle innovation, an important consideration when discussing biometric data in the context of XR because of the current technological requirements, these same interviewees continued to stress that more needs to be done to define how the biometric data will be collected, stored, and used by XR organizations.

Many of the interviewees that stated the CCPA and GDPR do not go far enough did acknowledge that XR's added complexity, trying to address user consent and choice in XR, can quickly invert to a point where these laws and regulations become too restrictive. One of the major differences between good choice and consent in the online world results from the mandatory processing of biometric data for the XR functionality. When raising this issue, however, it did not change their original answer. Instead, it just introduced new ways of thinking about data storage. The added data collection should just lead to deeper questioning and more diverse solutions for data storage. For example, interview participants advocated for more of the required biometric data to be stored locally on the XR device, such as a VR headset or AR glasses.

This sort of consideration for data storage, while necessary in VR, should be considered an even more pressing matter as AR technologies expand and begin to introduce non-users (i.e., bystanders) into the considerations.

<u>QUESTION 3:</u> Do the visual or audio indicators of when data is being collected and recorded go far enough to protect bystanders

Takeaway: There is broad consensus that augmented reality technology presents an unprecedented risk, if unchecked, to humans. To address this adequately, a collaborative effort to

4. ***Educate consumers;***
5. ***Collaborative effort to establish social norms;***
6. ***Apply technological solutions such that bystanders are protected from constant capture by default.***

To accomplish this, technological applications like jammers or blurred vision that protects bystanders without requiring any action on their behalf were suggested by many interviewees as a potential solution.

<u>Results</u>

Many of the challenges related to consent and choice will be consistent for an individual user across augmented and virtual reality. However, given that augmented reality overlays digital XR technology over the physical world, it is important to recognize that there are externalities in the environment, like people walking down the street that may be involved in capturing an environment. This forces a new assessment of what consent and choice look like in a way that has not been considered in online privacy laws and regulations to date. It is likely the severity of the implications on these externalities, which resulted in more than 80% of respondents stating that novel and somewhat undefined proposals to properly inform and provide notice to third parties that coexist in an environment enabling XR technologies (see figure 13 below).

Do visual and audio indicators on Augmented Reality hardware go far enough to protect bystanders (i.e., 3rd parties)	Total Respondents
No	18
Yes	3
Grand Total	21

Figure 13: Sufficiency of Visual Indicators on AR Hardware to protect bystanders

<u>Discussion & Analysis</u>

In a relatively untested and unproven environment, one of constant capture in the age of augmented reality, interviewees acknowledged that the most common issue is the fact that there is so much unknown about not only the technology but also the potential human physical and sociological implications as there could be adverse effects that the broader society has only begun to understand. Whether it is uncertainty surrounding the data that's currently being collected, processed, and stored; or the fact that the age of AR and VR brings surveillance society full circle, educating both the users of AR

technology, as well as the third parties or bystanders of the effects will be imperative to set a course that allows humanity to coexist successfully with immersive technologies like XR (Yadin, 2017). Therefore, not surprisingly, a lack of education on AR's implications was the most frequently provided response (eight instances across interviews) for why interviewees stated that the proposal of visual and audio indicators did not go far enough in protecting bystanders.

Another common theme across interviewees opinion on this topic, as well across the other questions, was the limited accessibility a visual or audio indicator provides given the fact that it relies on two senses (sight and hearing) to provide notice, and there is a segment of the population that may be blind and not see the red light or deaf and not hear an audio indicator. Therefore, introducing accessibility issues as a complexity to the broad adoption and use of AR only strengthens the other sentiment shared by interviewees that the current lacking understanding of the implications of AR demands more action be taken to protect non-consenting bystanders.

Additionally, with this new age of constant capture and the unprecedented situation that this presents to society, the second-most frequently provided answer to whether or not audio and visual indicators go far enough to protect bystanders in the age of constant capture was an acknowledgment that once society is has a better grasp and understanding of AR's implications, the adoption of these technologies requires the reassessment and redefinition of social norms. To build trust, there must be agreed-upon principles that govern the application and use of AR. The definition of these new social norms will be complex as social contracts may differ across geographies and populations.

This part of the interviews brought up one of the more globally-known examples of a past failed attempt to introduce XR to the broader society. In more than six interviews, just over a quarter of all interviewees mentioned how 'Glassholes,' people who used Google's AR glasses in the past and were presumed to be recording bystanders, had highlighted the importance of social acceptance of third parties. As xr5 stated, "*'Glassholes'* were a thing for a reason, social norms matter." However, social norms are not immutable. Many XR companies have learned from the mistakes made by Google, and in that same response, xr5 highlighted that "it is worth acknowledging that companies, and huge technology companies, [since then] worked very hard to shift social norms." This is why it is important to get a range of perspectives to define privacy and safety requirements in XR.

As pointed out in answer to Question 1 above, it will take a collaborative, multi-stakeholder approach to define these social norms and acknowledge the existing cultural and sociological nuances that currently exist. Even more, there are technological considerations, such as cloud computing and data collection, that further complicate how social norms have been established previously (Chuah, 2018; de Guzman et al., 2019). For example, while there is precedent for this standard, through the use of video cameras, for example, because of the recording's data collection and processing for commercial use, it is insufficient to use older technology, like the video camcorder, as an analogy for setting social norms in the age of XR. More likely is an example similar to what xr14 proposes, highlighting, "Google street view is capturing people that haven't given consent, things like people's not car number plates and things like that" so "in terms of blurring out so you can detect in the image data that there are other people blur out their faces, pixelate their faces."

Thus, if society must rethink its understanding and definition of human rights in the age of constant capture and XR technologies, there must be technological solutions provided to accommodate for this. During the expert interviews, a follow-up question was asked about how bystanders might be granted greater control over their privacy and safety, precisely to control the loss of an ability to provide valid consent and maintain choice. Mentioned multiple times was jamming technology that would essentially send a signal from the bystander back to the AR user to block the digital capture of the bystander. Additionally, and more frequently mentioned, is using similar technology to that of Google Maps in the AR hardware, which would blur the faces of bystanders, automatically protecting, at least, the visible features of a natural person. While there are many technological hurdles in applying these, one of which is the existing processing power of AR hardware, the private sector should provide these capabilities as a possible solution to adequately protect bystanders.

<u>QUESTION 4:</u> What are the hurdles that organizations encounter in their effort create more comprehensive privacy design/policies? What are some incentives that can be leveraged?

"The only time that I really see organizations willing to make change, like true change, and do a really good job at policy is either when their reputation is challenged, right, or when their bottom line is challenged" – xr18

Takeaway: Privacy experts believe that the fear of negative financial implications resulting from unknown business outcomes of privacy policies that provide adaptable levels of consent increases users' risk is the biggest hurdle to overcome.

<u>Results</u>

Half of all respondents believed that the biggest hurdle preventing the development of privacy and safety measures in XR was the unknown risk to business models (see figure: 14a). As noted throughout these results, Interviewees saw lacking regulation and/or agreed upon social norms as the second-most tricky hurdle. Two individual responses that tie to these overall most frequently stated results: A new funding model for early-stage XR companies and the potential for outsized legal ramifications for small organizations will be discussed in more detail during the analysis.

What are the hurdles and/or risks to enhanced privacy and safety in XR?	Total Respondents
Unknown risk to business model	9
No Regulation or Social Norms	3
Technological challenge: sometimes it actually requires large architectural changes.	2
Creative/innovation may be killed	1
Require a new funding model for early-stage companies (away from VC)	1
Legal ramifications from too many regulations for small companies could put them out of business	1
Not knowing something needs to be done	1
Grand Total	**18**

Figure 14a: What are the hurdles and/or risks to enhanced privacy and safety in XR?

It followed that interviewees believed the most critical incentive was rooted in the economics of the business model (see figure: 14b). While the method to achieve that incentive differed widely across nearly every interviewee, there were five instances where interviewees specifically called out the idea of trust playing an integral role in more robust economic results. The other responses support previous questions, highlighting the importance of improved regulation or the existing technological challenges or complexity it adds to the development process.

What are the incentives/potential benefits to enhanced privacy and safety in XR?	Total Respondents
Social Trust	5
Pressure from regulators and an accountability protocol similar to healthcare, education, advertising that de-risks organization	4
Consortium of compromise and shared standards (more rigorous checklists to streamline development)	3
Fear of consequence where industry leaders could drive top-down protocol	2
Bottom line indicator create environment where risk of not addressing privacy poses more significant financial risk	1
Common language/norms that help certify/streamline creation	1
Sell a service or solution not; independent taudit	1
Grand Total	**17**

Figure 14b: What are the incentives/benefits to enhanced privacy and safety in XR?

Discussion & Analysis

The challenge for organizations to adopt privacy policies that allow for more flexible models of consent is rooted primarily in the uncertainty, virtually untested, reconsidering the business model that the online world has relied on for the last two decades (Acquisti, 2016). This data collection is possible because of the binary nature of online privacy policies: one either agrees to the product/service provider's conditions or cannot use the product/service. Even as consumers have become more aware of how their data is being collected and used by organizations across sectors, as mentioned above, little has been done to address the power imbalance at the center of the conditions at the center of these online privacy policies, but with the transition to immersive XR experiences that blend the digital and natural world how consent is granted must be reconsidered.

To do this properly, it is essential to understand the digital landscape and data collection practices. However, arguably the most important consideration must be made to understand the business models' hurdles and incentives to adapt existing practices that have proven to be incredibly lucrative (Acquisti, 2016). Speaking with stakeholders from across the XR, and more broadly digital, this research sought to inquire what type of incentives might need to be made to overcome the hurdles in place to establish more equitable methods of consent for consumers.

Throughout twenty-nine interviews with the XR stakeholders from throughout the world and across many domains, the most frequently provided answer to which hurdles are the most difficult to overcome in the pathway to enhanced consent, the 'unknown risk to the business model' was most frequently referenced. Unfortunately, this response is essentially a fear of the unknown or minimal risk tolerance, perpetuating the status quo of binary methods to gain consent. There are two potential explanations for why this risk has not been overcome.

The first was highlighted by multiple interviews throughout the conversation: The role that (venture capital) investment plays in determining an organization's priorities and attempting to commercialize a product before it is truly ready for the marketplace. The second, which is more commonly understood:

Why risk something one does not have to (i.e., switch up a very profitable business model) without any sort of pressure?

XR23 noted that “you have got all this VC money coming in being sold this idea that magically is going to change the world, and this device is going to do all this stuff. And then when you put [the headset] on, and it doesn’t work. You know, the whole thing collapses.” This is true and referenced during the related work section by Magic Leap’s inability to fulfill its promises made while soliciting early-stage investment. This has led to what two interviewees believe to be a nearly five-year setback for the industry, through stifled innovation, because of how wary investors are to allocate capital to an industry with such a significant amount of technological uncertainty. This is a different explanation for the broader issue that is commonly understood (and documented above): economic incentives drive decision-making for these firms, not their users’ privacy and safety. These examples of lacking investment in new, early-stage companies also provide a rationale, beyond limited regulation, for why organizations do not test different business models related to privacy. It is more difficult for new companies to grow with lacking investment, and without new growth, we see a more significant impact of the already crowded and consolidated technology industry. In what is purported to be a market-driven economy, these largest organizations do not face sufficient competition at scale to incentivize non-monetary business model innovation that could ultimately provide sufficient privacy and safety for users. Inherently underscore the need for regulators to play a significant role in protecting individuals’ privacy and safety in XR. Ultimately, multiple interviewees shared an opinion similar to xr7, that “incentive wise, you would hope that these companies just want to do good in the world and protect their consumers.”

Informing the second-most identified example of a hurdle that provides insight into why both emerging and established organizations have not adequately addressed issues with consent and choice in the digital age: The legal and regulatory guidance is not in place to provide clear direction. These responses are supported by previous research that highlights the “protection of personal privacy is rapidly emerging as one of the most significant public policy issues” (Acquisti et al., 2016). Unfortunately, the reason this can be listed as a hurdle is crystalized through the responses, and supported by documented experience, provided by interviewees, as two individuals stated that government leaders do not understand the technology, and therefore the underlying issues, to sufficiently regulate the industry (Kang et al., 2018). As mentioned in an earlier analysis in this thesis, this lack of regulation is primarily due to a lack of knowledge amongst legislating bodies, mentioning “the biggest hurdle is not knowing that something needs to be done about it.”

Going forward, there must be an emphasis, instead of regulation at the federal level, that mandates and enforces comprehensive XR privacy policies, creative ways to overcome the challenges to existing business models, and technological capabilities to provide adequate privacy and safety for users in XR. A good place to start with finding new ways to incent organizations to adopt expanded policies around consent and choice might be through creative thinking as described by xr29, “I think that there could be models in the natural world, we can call the natural world as compared to the, you know, the internet worked digital environment. Meaning, you know, hospitals, institution, schools, museums, shopping malls, these are all different kinds of spaces with different protocols, different expectations among the people who are there.” Research completed by Professor Alessandro Acquisti in “The Economics of Privacy” reaffirms the feedback from these interviews that highlights the importance of how the use of individual data has high individual costs, but also that there is precedent in other industry, such as healthcare, for government regulation of an individuals’ data costs (i.e., those that make it a profitable endeavor for companies) (Acquisti, 2016).

The interviewees’ interesting comment throughout interviews was that privacy is not a one-size-fits-all approach, which is sentiment validated by Dr. Acquisti’s research underscores the importance of finding creative solutions to protect users XR. Numerous interviewees shared this belief, and some examples of what that might look like will be discussed in the conclusion.

<u>QUESTIONS 5 & 6:</u> How do we ensure that user choice is incorporated in XR activities and experiences? What, in your opinion, ensures "valid permission" (i.e., consent) is granted in the context of XR?

Takeaway: Currently, to provide valid permission in XR, most of the experts shared the opinion that users mechanism for awareness:

- ***Which data is being collected and/or sent (and to whom);***
- ***How the users' data will be used;***
- ***Will the users' data be sold to a third party;***
- ***How long any collected data will be stored;***

Importantly, once that information has been understood, 64% of respondents stated that there should be an opportunity to opt-in or opt-out of parts of an experience. Moreover, of those interviewed, 14% of all respondents that did not initially name opt-in/out as their first choice choose this option as their second-most vital way to grant consent.

<u>Results</u>

A significant majority believe that consent should not be a binary transaction in XR as it is in nearly all of today's online experiences. The fact is that an overwhelming majority highlight that more needs to be done to achieve consent underscores research that is already supported by informed notice and choice are insufficient (Cranor and Schaub, 2020). Often, this was explained simply as providing notice to users and then allowing them to choose the level of experience they desire, acknowledging that all capabilities of the experience or tool may not be accessed if some of the privacy and safety preferences supersede the requirements for the technology to operate.

What, in your opinion, ensures "valid permission" is granted in the context of XR?	Total Respondents
As experience requires, opt in/out as you want	14
Notice is a minimum	3
Grand Total	17

Figure 15: What, in your opinion, ensures "valid permission" is granted in the context of XR?

<u>Discussion & Analysis</u>

While the GDPR can be a baseline for privacy and safety in XR, as discussed above, it should not be the minimum requirement. As highlighted in the previous section, biometric data is of particular concern to interviewees regarding their perspectives on notice and consent. Additionally, just as with smartphones, interviewees, explained by interviewee xr8, also are looking for "a wide range of options to opt-in or out," relative to "their comfort levels when it comes to privacy. Some people might be okay with sharing their location, some people might be in physical danger if they do, as highlighted earlier, and so making sure that the applications and the devices have those options for users to decide for

themselves is going to be the most important thing to do." The challenging part for interviewees across the spectrum was that as society evolves and adopts more XR technologies, the contexts for what is relevant and not relevant might also change. , the bottom line is that consent needs to evolve beyond its binary choice today for reasons that go far beyond one of today's main uses: advertising. With XR, these individual data points combined to tell the story of who a person is can present real danger when combined with other emerging technologies such as facial recognition.

While indeed some information new types of information need to be captured to run these XR experiences, the industry must heed sentiment heard throughout interviews, which is summarized well by xr5, "notice and choice frameworks are not ideal ways to protect privacy. However, we do not know what stuff is doing if you're using boilerplate privacy policies. And, you know, part of this is because Facebook and Oculus privacy policies are impenetrable to normal people." Therefore, just as in the natural world, there are deeper complexities and safety issues associated with immersive experiences and environments that require new thinking toward the definition of consent and how it is obtained. However, little has been done to address the issue (de Guzman et al., 2019). That said, there are many examples throughout the interviews of what might be done to improve the privacy and safety in XR and the process for gaining consent. This is currently evident in the field where publishers like Tobii, discussed below, have been reasonable faith efforts to improve notice, yet, the binary choice remains oft-used by leading XR companies like Unity, which was discussed above.

The existing consent process relies on a one-sided agreement between the digital and human (Cate, 2006). These online agreements are often given without another option than to agree to the binary terms presented, which fundamentally is not analogous to consent (Cate 2010). The same is true in the development of XR applications, where binary terms (i.e., consent or quit) deployed as a default practice for presenting and obtaining consent (Cate 2010).

The example in Figure 16 below, Tobii's VR framework for transparency, brings the binary choice for consent into an XR experience by presenting a "Yes, and Accept" or "No, and Quit" option for agreeing to the terms of an XR experience's privacy policy (Tobii, 2020). While their Data Transparency policy is a significant step further than Unity, discussed above, it is inadequate in addressing the minimum needs in XR to provide protections for user biometric data as well as the data of completely unrelated bystanders, both of which are now issues for the digital and physical world. Simply: we live in a complex world, and that complexity is increasingly relevant in our digital lives where binary options are insufficient. Most importantly, providing more transparency while asking for consent does not compromise a developer's ability to receive valuable, we have data from its participants. If presented with transparent and complete information, individuals will respond reasonably. They will likely make privacy decisions that protect their privacy and adequately support the objectives of the digital organization (Tsai, Egelman, Cranor, Acquisti; 2011).

Data Transparency

If you are developing an application that stores or transfers Tobii eye tracking data, Tobii requires that your application complies with the Eye Tracking Data Transparency Policy.

We have created an example scene with a few prefabs to help you follow this policy, which can be found in: **TobiiXR > Examples > DataTransparency_Example**.

Examples When Opening the App

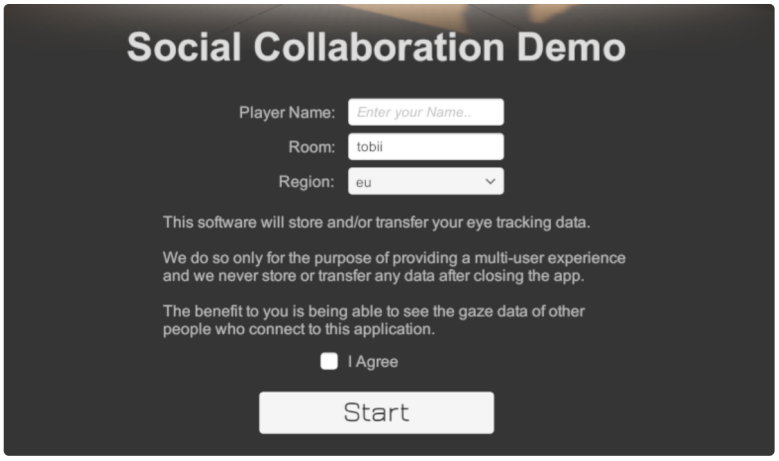
Applications that stores or transfers Tobii eye tracking data should implement active user acceptance: informing people what you are doing with their data and why.

Below are a two examples on how to achieve this:

A VR world-space user acceptance UI shown in a separate scene when starting a VR app. To prevent accidental selection, the Unity example requires the user to press and hold the trigger while looking at a button.

Figure 16:Tobii Transparency Policy

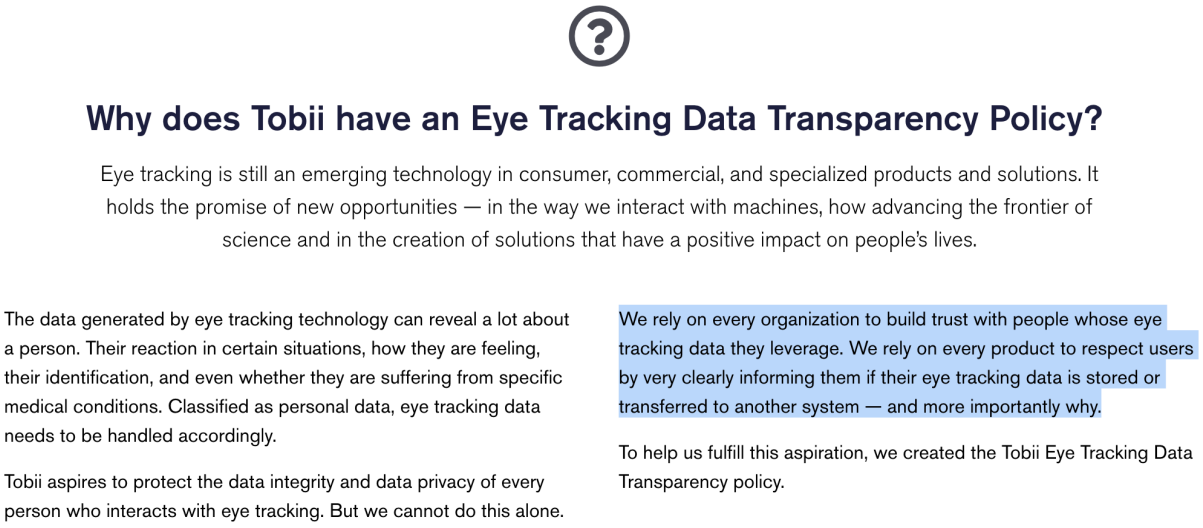
While Tobii's transparency notice provides more context, as shown in Figure 16 (above) and Figure 17 (below), we've already established that notice is not synonymous with consent. Moreover, the Tobii Transparency Policy provides a 'why' for their policies. Still, where newer technology (for consumers) is introduced (i.e., eye tracking), the transparency policy in Figure 17 stops short of providing proper context to understand what eye-tracking data is and how someone can access their information before agreeing to use the service.



A desktop user acceptance UI shown before putting on the VR headset.

Figure 17:Tobii Transparency Policy

Ultimately, Tobii takes measures beyond Unity to provide greater transparency to understanding one's right to privacy when using their software. However, its transparency policy does not amount to much more than delivering appeasing optics to demonstrate some awareness of the challenges related to privacy and consent users face in the age of XR. Tobii properly explains the necessity to have a transparency policy, but just like Unity, others' responsibility is to develop and deploy comprehensive methods to gain user consent.



Why does Tobii have an Eye Tracking Data Transparency Policy?

Eye tracking is still an emerging technology in consumer, commercial, and specialized products and solutions. It holds the promise of new opportunities — in the way we interact with machines, how advancing the frontier of science and in the creation of solutions that have a positive impact on people's lives.

The data generated by eye tracking technology can reveal a lot about a person. Their reaction in certain situations, how they are feeling, their identification, and even whether they are suffering from specific medical conditions. Classified as personal data, eye tracking data needs to be handled accordingly.

Tobii aspires to protect the data integrity and data privacy of every person who interacts with eye tracking. But we cannot do this alone.

We rely on every organization to build trust with people whose eye tracking data they leverage. We rely on every product to respect users by very clearly informing them if their eye tracking data is stored or transferred to another system — and more importantly why.

To help us fulfill this aspiration, we created the Tobii Eye Tracking Data Transparency policy.

Figure 18: Tobii Eye Tracking Policy

Without comprehensive privacy policies and procedures, the history of our digital lives and new research has already shown that users are forced to consent to existing policies that do not provide adequate safety. The implications of not understanding XR's privacy policies have already been proven, underscoring the need for comprehensive methods to gain user consent. Because of the complexity for which privacy policies are created. Current approaches only provide limited transparency and often result in transparency conflated with consent, worsening in an XR environment. Going forward, as xr28 stated, "everyone needs to be able to participate in society -- it is not a choice." For this reason, I hope that the Extended Reality ecosystem will take heed of this research to ensure that XR is created for all, and by doing so, will protect not only the privacy of users but also their safety in the natural and built world.

Ch. 6: Conclusion

PRELIMINARY FINDINGS

This research has highlighted some of the most pressing issues in technology related to the role that privacy plays in our digital lives. With the advent of Extended Reality (XR) technologies, there needs to be a concerted effort to address fragmented legal policy developed by a multi-stakeholder group of experts from across the industry, like many of the people interviewed for this research.

A group like the XRSI can facilitate such work and help educate the public on the benefits and risks of XR. However, regulators must put a policy into place that mandates a new definition for digital consent be outlined. One that will provide sufficient choice to users, such that they can participate in society and realize the benefits of these technologies. There needs to be a collective effort to redefine social norms such that a common understanding, a set of social norms, is established in a way that does not force oneself to take action without understanding: the data that is being collected about them, how that data will be used, and how long it will be stored.

Binary options of consent will not suffice in XR, and this is especially urgent for the issues related to bystanders as there is no middle-ground and new and creative solutions must be established in an XR environment. We cannot wait to try to fix our mistakes as we have done in the online world with social media disinformation. It is imperative to give users multiple options in an experience and will likely build trust that may make up for any perceived sacrifices the business has to make by limiting its data consumption.

STUDY LIMITATIONS

Throughout the study, I've highlighted a few areas that have limited my research and will require additional work as I move toward dissemination to the broader public. The first, is that I must expand the diversity interview pool. Both limited by the number of XRSI referrals (22/29 interviewees) and lacking racial and ethnic diversity will be essential to have a more complete set of findings.

RECOMMENDATIONS FOR XRSI

There are two main recommendations for the XR Safety Initiative to consider as it continues to develop its privacy and safety framework. The first is to assess and address the process and project management methods for creating this framework. The second, an expansion on current XRSI goals, is to provide more XR-relevant and specific content and/or guidance on consent, choice, and control in the Inform Section 1.5 as the 'heavy lifting'.

The first recommendation is to assess and update the process for collaborating with key stakeholders to create the XRSI Privacy and Safety Framework because the process should inform any recommendations to the XRSI Privacy and Safety Framework content. The XRSI goes to great lengths to include diverse voices in creating its framework to reach stakeholders across the XR ecosystem throughout the development and co-creation of the XRSI Privacy and Safety Framework. However, the actual number of individuals and diverse groups providing input throughout the development process is much less than those that initially engage or have loose ties to the group, which places limitations on the effort to implement some of these changes. For example, no one credited with contributing to the

XRSI Framework 1.0 currently works for Facebook, Sony, or HTC; and according to Statista, these companies accounted for nearly 80% of all VR device shipments in 2019. are two of the largest firms working on XR in the world that currently own. The main point is that because many of the most prominent creators and enablers of XR are not contributing to the creation of this framework, there may not be as much buy-in to its recommendations. So, how does that get remedied?

My suggestion stems from observations while conducting my research with the XRSI; one concern is the degree of additional daily work required by the XRSI team and its creation of a working schedule. Moreover, numerous interviewees stated they had hoped to work more on the next version of the framework but could not be due to their schedule. While one of the strengths of XRSI is its global network, however, it is precisely this global nature that proves to be a challenge as one develops the XRSI framework since this work requires time for active engagement and discussion across these groups in different time zones. This complexity, which is a significant issue of its own, is exacerbated by XRSI leadership's limited coordination and scheduling of the working meetings where key contributors may not have the availability to conduct this work. For example, while presumably well-intentioned as XRSI leadership began working on updates to the XRSI Privacy and Safety Framework 1.1, only one meeting day and time was communicated for the United States, and the same was true for European collaborators. Lacking what can appear to be a collaborative effort to include key stakeholders, specifically those from the largest players in the XR industry, and coincidently those with the lesser incentives to participate in rule creation that might limit their businesses' profitability, could lead to a deprioritization of the work outside their daily responsibilities, and ultimately a loss of interest in contributing to the XRSI Privacy and Safety Framework. Therefore, in lieu of federal regulation specific to XR, optimizing the recruitment and scheduling efforts may result in higher stakeholder engagement and more relevant and specific content in the XRSI Privacy and Safety Framework.

With 100 participants in its kickoff call for the XRSI Privacy and Safety Framework's version 1.1 update, with representatives across some of the leading XR hardware and software companies, it is clear that there is interest from key stakeholders in contributing to this effort. Importantly, for XRSI, there is an incentive in these stakeholders' participation from XR content creation and device companies. These are the individuals who know both the business needs and technological requirements. Understanding their requirements should then directly enable more relevant additions to the framework, which is important because the current version of the XRSI Privacy and Safety Framework could be considered a relatively generic and overly simplistic identification and explanation of privacy and safety goals for XR. These immersive technologies are currently without expectations and social norms. Nevertheless, these technologies also blend the digital and physical world in an unprecedented way, so content and technological experts are essential to identifying what is truly needed to provide adequate privacy and safety in the age of XR.

This leads to my second recommendation: XRSI should provide more specific definitions and/or guidance on the areas of confusion throughout the industry as identified through previous work completed by legal and policy experts like Joe Jerome and Elysse Dick (Dick, 2021; Jerome, 2021).

As a result of lacking participation from some key industry stakeholders, parts of the existing framework, for example, the Inform (1.5) section of the XRSI Privacy and Safety Framework, which

contains guidance on consent (1.5.2), context (1.5.3), choice (1.5.4), control (1.5.5) are incomplete and currently limited in the guidance they provide to the XRSI's key stakeholder audience. The current version of the XRSI Privacy and Safety Framework combines elements of existing privacy policies like the GDPR and NIST frameworks and singular references that serve to provide cursory-level context for the recommendation. For example, in the consent section 1.5.2, XRSI briefly raises the point that consent in XR might be different from today's expectations in the online world and then follows it with a singular example of the collection of biometric data and a bullet point from the GDPR that acknowledges how the processing of data should that is not necessary for performance should not be included. In short, these sections are incomplete and do not do much more than recycle existing elements of privacy and safety in today's online world. It would be in the best interest of the XRSI team to take proactive measures to figure out a way to accommodate today's XR industry stakeholders to specifically identify new and/or unique considerations for privacy and safety in XR.

Based on this research, believe that improving how we attempt to include people and maybe frame how we are soliciting participation could enhance some of the content and make it more relevant. Moreover, the legacy research from the digital to the online world currently published does not answer these questions sufficiently. Continuing with the example of consent in XR, one example from my research findings relates to a bystanders' (i.e., third party) consent. This is often an issue in augmented reality due to the current technological requirements because of what is now commoditized: marker-less AR technology that scans the entire external (I.e., outward-facing) environment (i.e., the physical world). While my research provides direction that the existing understanding and protection of bystanders is incomplete, and other researchers have highlighted this important fact, there is an opportunity for the XRSI to help clarify and define how bystanders either provide their consent in a physical world using AR technology or collaborate across stakeholder groups to co-create technological solutions to protect bystanders adequately. To provide a specific example that might get the conversation started, throughout my interviews, multiple participants suggested that we create technology to blur individuals' faces out automatically, in a similar way to how Google addresses this issue in the Google Maps product. Without a comprehensive, unifying, federal law, implementing these technological solutions are dependent on if XR organizations choose to deploy them, so the collaboration across stakeholders that XRSI can facilitate is so important. In place of a technological solution, it will be important that the XRSI seek compromise and creativity in establishing continuity across XR organizations as they seek to set social norms for its users. Providing consistency in the norms and expectations for all participants in this process may accelerate adopting these technologies due to increased comfort levels that consensus in setting social norms might provide (Tene and Polonetsky, 2013). Suppose that proves to be accurate, given the benefit and lessened risk to an XR organization's business model. In that case, XRSI is, again, in an ideal position to facilitate these discussions across private, public, and non-profit sector stakeholders.

RECOMMENDATIONS FOR INDUSTRY & POLICY MAKERS

First, Industry must move beyond traditional Notice and Choice to make sure that people understand what they're agreeing to. Immersive technologies present an excellent opportunity to understand better what knowledge is required to know what one agrees. One of the things is trying to understand and look at ways to use tiered, not necessarily notifications, but exposure to different risks as they come up. People can choose whether to enter an XR experience or participate in an activity based on multiple

levels of which information is collected, stored, and used by the XR experience developer and/or organization. There might be an explanation in the VR game's existing introductory tutorial: if the application collects biometric data (e.g., playing tennis where arm movement tracking data is required for the game's physics to work), which already exist when onboarding the XR user. So, by adding an explanation that states something like: "Hey, we are collecting XYZ data (e.g., arm movement data) while you are swinging your arm and we are going to do ABC (e.g., collect it only to ensure the game will work properly and store it for 24 hours without sharing it with a third party), could be a way to introduce some of the broader risk or rationale for the XR organization's activities while pre-emptively clarifying potential points of concern that a user might in that particular moment. Furthermore, based on previous research conducted with colleagues at the University of Michigan, this practice should also be applied as data collection and storage change. The user advances in the XR experience or requirements for data collection, storage, and use might change.
Based on my research interviews across many industries and disciplines, I think that this would not only be feasible but also lead to higher engagement and understanding for the broader public as we become more immersed in the digital economy. While I cannot speak to it with certainty now, as the basis for this proposal is rooted in anecdotal feedback during my interviews, it could be an exciting area for future work: to understand what psychology looks like within the immersive technology of how users truly understand what they agree with.

Second, make sure to emphasize safety and go beyond expectations for digital privacy as immersive technology experiences blend of the digital and physical world. One of the more impactful learnings for me throughout this research was recognizing the various safety concerns or other privacy risks beyond an individual's digital privacy. As my interviews progressed, the narrative around these conversations clarified that the data collection, storage, and use (e.g., selling to third parties) is not only a privacy risk, but also arguably, more often a broader safety problem in the natural and physical world. Acknowledging the existing privacy issues (e.g., lacking choice) from this perspective, the issue of data collection, storage, and use of immersive technologies becomes more problematic as our society integrates technology like XR over the next 10 to 15 years. As VR headset costs decrease and people begin wearing augmented reality contacts, it may follow that more traction on incentivizing technology organizations to adapt privacy to the issues of digital privacy by framing these issues within the context of one's own and familial safety. Emphasizing safety may be more relatable and rightful priority of ensuring public safety and security in the natural world or the physical world may be a compelling way to incentivize industry stakeholders to adopt more protective privacy and safety policies. Moreover, by advocating for user safety, a requirement that can be seen as less of a business model driver than digital privacy and consent, could allow organizations to properly complete some initial consequence planning and get ahead of costly issues for an organization in coming years (e.g., Facebook and Twitter's role in disinformation). Ultimately, framing privacy protection from the perspective of public safety, and not necessarily the lens of individuals' privacy, it may be a pathway to bring broader diversity of industry stakeholders to the discussion table. Collecting my eye tracking performance and the general assumptions made about an individual from these data might get more traction from industry leaders if communicated as a safety issue because it bridges the digital and physical world. This presents a second area that should be studied more going forward.

References

- 1939, https://1939nyworldsfair.com/worlds_fair/viewmaster/reel_89-2.htm. Accessed 26 Mar 2021.
- Alessandro Acquisti and Ralph Gross. Predicting Social Security numbers from public data. Proceedings of the National Academy of Sciences of the United States of America, 106(27):10975—-10980, 2009. doi:10.1073/pnas.0904891106.
- A. Acquisti, R. Gross, and F. Stutzman. 2011. Privacy in the age of augmented reality. Proc. National Academy of Sciences.
- Alessandro Acquisti, Curtis Taylor, & Liad Wagman. (2016). The Economics of Privacy. Journal of economic literature, 54(2), 442–492. Feature, Nashville: American Economic Association.
- Alessandro Acquisti, Veronica Marotta, and Vibhanshu Abhishek. Online tracking and publishers' revenues: An empirical analysis. Working Paper2, 2019. URL: https://weis2019.econinfosec. org/wp-content/uploads/sites/6/2019/05/WEIS{_}2019{_}paper{_}38.pdf.
- Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musabay, Kadeem Pitkin, and Elissa M Red miles. Ethics Emerging: The Story of Privacy and Security Perceptions in Virtual Reality. In USENIX Symposium on Usable Privacy and Security (SOUPS) 2018, 2018. doi:10.13016/M2B853K5P
- Aukstakalnis, Steve. (2016). Practical Augmented Reality: A Guide to the Technologies, Applications, and Human Factors for AR and VR. Usability. Addison-Wesley Professional.
- Jeremy Bailenson. Protecting Nonverbal Data Tracked in Virtual Reality, 2018. doi:10.1001/jamapediatrics.2018.1909.
- Beshears, John, Choi, James J, Laibson, David, & Madrian, Brigitte C. (2008). How are preferences revealed? Journal of public economics, Journal of Public Economics, 92(8),
- Mark Billinghurst, Adrian Clark, and Gun Lee. A survey of augmented reality, 2014. doi:10.1561/1100000049.
- "Bloomberg - Are You A Robot?". Bloomberg.Com, 2020, https://www.bloomberg.com/news/features/2020-09-23/why-magic-leap-failed-ar-hype-exceeded-product-s-capabilities.
- Bohn, Dieter. "Microsoft'S Hololens 2: A $3,500 Mixed Reality Headset For The Factory, Not The Living Room". The Verge, 2019, https://www.theverge.com/2019/2/24/18235460/microsoft-hololens-2-price-specs-mixed-reality-ar-vr-business-work-features-mwc-2019.
- Bozorgzadeh, Amir. "Avatars Will Be Our Guides In Immersive AR Worlds — And Brands Need To Be Ready."What is Venturebeat, 2019, https://venturebeat.com/2019/04/04/avatars-will-be-our-guides-in-immersive-ar-worlds-and-brands-need-to-be-ready/.
- Jeremy Brooker THE POLYTECHNIC GHOST, 2007. Early Popular Visual Culture, 5:2, 189-206, DOI: 10.1080/17460650701433517
- Frederick P. Brooks. What's honest about virtual reality? IEEE Computer Graphics and Applications, 1999. doi:10.1109/38.799723.
- Johnathan Brown, Elisa White, and Akshya Boopalan. Chapter 12 - Looking for the Ultimate Display: A Brief History of Virtual Reality. In Jayne Gackenbach and Johnathan Bown, editors,

Boundaries of Self and Reality Online, pages 239–259. Academic Press, San Diego, 2017. URL: http://www.sciencedirect.com/science/article/pii/B9780128041574000128, doi: 10.1016/B978-0-12-804157-4.00012-8.

- Philip Brey. The ethics of representation and action in virtual reality. Ethics and Information Technology, 1999. doi:10.1023/A:1010069907461.
- Bye, Kent. "XR Ethics Manifesto". Youtube.Com, 2019, https://www.youtube.com/watch?v=CXgY3YXxqJ8.
- Cate, Fred H., The Failure of Fair Information Practice Principles (2006). Consumer Protection in the Age of the Information Economy, 2006, Available at SSRN: https://ssrn.com/abstract=1156972
- Cate, Fred H., "The Limits of Notice and Choice," in IEEE Security & Privacy, vol. 8, no. 2, pp. 59-62, March-April 2010, doi: 10.1109/MSP.2010.84.
- J. P. Cater, "Smell/taste: odors in reality," *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, San Antonio, TX, USA, 1994, pp. 1781 vol.2-, doi: 10.1109/ICSMC.1994.400108.
- Chuah, Stephanie Hui-Wen, Why and Who Will Adopt Extended Reality Technology? Literature Review, Synthesis, and Future Research Agenda (December 13, 2018). Available at: http://dx.doi.org/10.2139/ssrn.3300469
- DeFanti, T., Sandin, D. J., Sayre Glove Final Project Report, US NEA R60-34-163 Final Project Report, November 10th, 1977.
- DellaVigna, Stefano. 2009. "Psychology and Economics: Evidence from the Field." Journal of Economic Literature, 47 (2): 315-72.
- Dick, Elysse. 2021. “Balancing User Privacy and Innovation in Augmented and Virtual Reality.” https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality
- Ehrsson HH, Spence C, Passingham RE. That's my hand! Activity in premotor cortex reflects feeling of ownership of a limb. Science. 2004 Aug 6;305(5685):875-7. doi: 10.1126/science.1097011. Epub 2004 Jul 1. PMID: 15232072
- "Extended Reality (XR) Market - Growth, Trends, COVID-19 Impact, And Forecasts (2021 - 2026)". Mordorintelligence.Com, https://www.mordorintelligence.com/industry-reports/extended-reality-xr-market.
- GDPR. "General Data Protection Regulation (GDPR) – Official Legal Text". General Data Protection Regulation (GDPR), 2016, https://gdpr-info.eu/.
- Feigin, E. (2004). Architecture of Consent: Internet Protocols and Their Legal Implications. Stanford Law Review, 56(4), 901-941. Retrieved February 2, 2021, from http://www.jstor.org/stable/40040166
- Jaybie de Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. A First Look into Privacy Leakage in 3D Mixed Reality Data, pages 149–169. 2019. doi:10.1007/978-3-030-29959-0_8.
- Henrysson, Anders & Ollila, Mark & Billinghurst, Mark. (2005). Mobile phone-based AR scene assembly. 154. 95-102. 10.1145/1149488.1149504.
- Hillman, R. A. On-line Consumer Standard-Form Contracting Practices: A Survey and Discussion of Legal Implications, Cornell Law Faculty Publications, Paper 29 (2005) http://scholarship.law.cornell.edu/lsrp_papers/29

- Hosfelt, Diane. Making Ethical Decisions for the Immersive Web. 2019.
- Hosfelt, Diane, Outlaw, Jessica, Snow, Tyesha, & Carbonneau, Sara. (2020). Look Before You Leap: Trusted User Interfaces for the Immersive Web.
- Hughes, Neil. "Why Businesses Are Preparing For An Extended Reality (XR) | Cybernews". Cybernews, 2021, https://cybernews.com/editorial/why-businesses-are-preparing-for-an-extended-reality-xr/.
- "Infographic: The History And Future Of Augmented & Virtual Reality". Robotics Business Review, 2019, https://www.roboticsbusinessreview.com/news/infographic-the-history-and-future-of-augmented-virtual-reality/.
- Jerry Isdale. What Is Virtual Reality?, 1993. URL: http://www.columbia.edu/~rk35/vr/vr.html.
- Jeon, Chihyung. "The Virtual Flier: The Link Trainer, Flight Simulation, And Pilot Identity". Technology And Culture, vol 56, no. 1, 2015, pp. 28-53. Project Muse, doi:10.1353/tech.2015.0017.
- Joe Jerome - Establishing privacy controls for virtual reality and immersive technology
- Kang, C., Kaplan, T. and Fandos, N., 2018. *Knowledge Gap Hinders Ability of Congress to Regulate Silicon Valley (Published 2018)*. [online] Nytimes.com. Available at: <https://www.nytimes.com/2018/04/12/business/congress-facebook-regulation.html> [Accessed 8 April 2020].
- Kato, Hirokazu & Billinghurst, Mark. (1999). Marker tracking and HMD calibration for a video-based augmented reality conferencing system. The 2nd International Workshop on Augmented Reality (IWAR 99). 85-94. 10.1109/IWAR.1999.803809.
- Kholer, Chris. "Review: Oculus Touch Controllers Put VR Within Arm's Reach". Wired, 2016, https://www.wired.com/2016/12/review-oculus-touch/.
- Kohane, Isaac S. 2015. “Ten Things We Have to Do to Achieve Precision Medicine.” Science 349 (6243): 37–38.
- Kracht, T., Mueller, M., Sterns, D. and Sotto, L., 2018. Biometric Information Protection: The Stage is Set for Expansion of Claims. [online] The Practical Guidance Journal. Available at: <https://www.lexisnexis.com/lexis-practical-guidance/the-journal/b/pa/posts/biometric-information-protection-the-stage-is-set-for-expansion-of-claims>.
- Lavoie, R., Main, K., King, C. et al. Virtual experience, real consequences: the potential negative emotional consequences of virtual reality gameplay. Virtual Reality 25, 69–81 (2021). https://doi.org/10.1007/s10055-020-00440-y
- Levine, Arthur. Usatoday.Com, 2018, https://www.usatoday.com/story/travel/experience/america/theme-parks/2018/06/20/virtual-reality-vr-tech-theme-park-rides-attractions/714563002/.
- Lenggenhager B, Tadi T, Metzinger T, Blanke O. Video ergo sum: manipulating bodily self-consciousness. Science. 2007 Aug 24;317(5841):1096-9. doi: 10.1126/science.1143439. PMID: 17717189.
- Litman-Navarro, Kevin. "Opinion | We Read 150 Privacy Policies. They Were An Incomprehensible Disaster.". Nytimes.Com, 2019, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.
- "Looking Glass Factory · The World's Leading Holographic Display". Looking Glass Factory · The World's Leading Holographic Display, 2021, https://lookingglassfactory.com/.

- E. Luger, T. Rodden, Terms of Agreement: Rethinking Consent for Pervasive Computing, Interacting with Computers, Volume 25, Issue 3, May 2013, Pages 229–241, https://doi-org/10.1093/iwc/iws017
- Ewa Luger, Stuart Moran, and Tom Rodden. 2013. Consent for all: revealing the hidden complexity of terms and conditions. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, 2687–2696. DOI:https://doi.org/10.1145/2470654.248137
- Matney, L. "Microsoft Gets Contract Worth Up To $22 Billion To Outfit US Army With 120,000 AR Headsets". Techcrunch.Com, 2021, https://techcrunch.com/2021/03/31/microsoft-wins-contract-worth-up-to-22-billion-to-outfit-u-s-army-with-120000-ar-headsets/.
- Paul Milgram and Fumio Kishino. Taxonomy of mixed reality visual displays. IEICE Transactions on Information and Systems, E77-D(12):1321–1329, 1994. URL: https://www.researchgate.net/publication/231514051{_}A{_}Taxonomy{_}of{_}Mixed{_}Reality{_}Visual{_}Displays.
- P J Metzger. Adding reality to the virtual. In Proceedings of IEEE Virtual Reality Annual International Symposium, pages 7–13, 1993. doi:10.1109/VRAIS.1993.380805.
- Miller, M.R., Herrera, F., Jun, H. et al. Personal identifiability of user tracking data during observation of 360-degree VR video. Sci Rep 10, 17404 (2020). https://doi.org/10.1038/s41598-020-74486-y
- Madary, Michael, and Metzinger, Thomas K. “Real Virtuality: A Code of Ethical Conduct. Recommendations for Good Scientific Practice and the Consumers of VR-Technology.” Frontiers in Robotics and AI, Frontiers Research Foundation, 2016, doi:10.3389/frobt.2016.00003.
- Mind Commerce. Augmented And Mixed Reality Market Outlook And Forecasts 2020 – 2027. Mind Commerce, 2020. Accessed 29 Apr 2021.
- Mohring, M. & Lessig, C. & Bimber, O.. (2004). Video see-through AR on consumer cell-phones. 252- 253. 10.1109/ISMAR.2004.63.
- Mozilla. (2021). Mozilla Manifesto. https://blog.mozvr.com/making-ethical-decisions/
- Lebeck, Kiron, Ruth, Kimberly, Kohno, Tadayoshi, & Roesner, Franziska. (2018). Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End Users. 2018 IEEE Symposium on Security and Privacy (SP) (pp. 392–408). orig-research, IEEE.
- Lenggenhager B, Tadi T, Metzinger T, Blanke O. Video ergo sum: manipulating bodily self-consciousness. Science. 2007 Aug 24;317(5841):1096-9. doi: 10.1126/science.1143439. PMID: 17717189.
- Neumann, Ulrich & Cho, Youngkwan. (1970). A Self-Tracking Augmented Reality System for Assembly-Guidance Applications.
- Nimesha Ranasinghe and Ellen Yi-Luen Do. 2016. Virtual Sweet: Simulating Sweet Sensation Using Thermal Stimulation on the Tip of the Tongue. In Proceedings of the 29th Annual Symposium on User Interface Software and Technology (UIST '16 Adjunct). Association for Computing Machinery, New York, NY, USA, 127–128. DOI:https://doi.org/10.1145/2984751.2985729
- Ohshima, T, et al. “AR/Sup 2/Hockey: A Case Study of Collaborative Augmented Reality.” Proceedings. IEEE 1998 Virtual Reality Annual International Symposium (Cat. No.98CB36180), IEEE, 1998, pp. 268–75, doi:10.1109/VRAIS.1998.658505.

- Jonathan A. Obar and Anne Oeldorf-Hirsch. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services, 2018. doi:10.1080/1369118X. 2018.1486870.
- ISEDUA ORIBHABOR, DANIEL LEUFER, GASPAR PISANU. 2020. https://www.accessnow.org/what-is-augmented-reality-risks/
- O'Brolcháin, Fiachra, Jacquemard, Tim, Jacquemard, Tim, Monaghan, David, Monaghan, David, O'Connor, Noel, et al. (2016). The Convergence of Virtual Reality and Social Networks: Threats to Privacy and Autonomy. Science and engineering ethics, 22(1), 1–29. Research Support, Non-U.S. Gov't, Dordrecht: Springer Netherlands.
- "Oculus Quest 2: Our Most Advanced New All-In-One VR Headset | Oculus". Oculus.Com, 2021, https://www.oculus.com/quest-2/.
- "Testing And Performance Analysis | Oculus Developers". Developer.Oculus.Com, 2021, https://developer.oculus.com/documentation/unity/unity-perf/.
- Playstation 5 Matches The Price Of The Xbox Series X". BBC News, 2021, https://www.bbc.com/news/technology-54178375.
- Pausch, Randy, et al. "Disney's Aladdin : First Steps toward Storytelling in Virtual Reality." Proceedings of the 23rd Annual Conference on Computer Graphics and Interactive Techniques, ACM, 1996, pp. 193–203, doi:10.1145/237170.237257.
- Pham, Quoc-Viet, et al. "A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art." IEEE Access, vol. 8, IEEE, 2020, pp. 116974–7017, doi:10.1109/ACCESS.2020.3001277.
- Eli Pariser. The Filter Bubble: What the Internet Is Hiding from You. Penguin press, New York, 2011. doi:10.4079/pp.v19i0.10431.
- Rekimoto, Jun & Nagao, Katashi. (1995). The World through the Computer: Computer Augmented Interaction with Real World Environments. UIST (User Interface Software and Technology): Proceedings of the ACM Symposium. 10.1145/215585.215639.
- Rekimoto, Jun. (1996). Transvision: A hand-held augmented reality system for collaborative design. Proceedings of Virtual Systems and Multi-Media (VSMM '96).
- Rekimoto, Jun & Ayatsuka, Yuji. (2000). CyberCode: Designing Augmented Reality Environments with Visual Tags. ACM Designing Augmented Reality Environments. 10.1145/354666.354667.
- Roux D.B., Parry D.A. (2020) The Town Square in Your Pocket: Exploring Four Metaphors of Social Media. In: Hattingh M., Matthee M., Smuts H., Pappas I., Dwivedi Y.K., Mäntymäki M. (eds) Responsible Design, Implementation and Use of Information and Communication Technology. I3E 2020. Lecture Notes in Computer Science, vol 12067. Springer, Cham. https://doi.org/10.1007/978-3-030-45002-1_16
- Seinfeld, Sofia & Arroyo Palacios, Jorge & Iruretagoyena, G. & Hortensius, R. & Zapata, Lenin & Borland, David & Gelder, B. & Slater, M. & Sanchez-Vives, Maria. (2018). Offenders become the victim in virtual reality: impact of changing perspective in domestic violence. Scientific Reports. 8. 10.1038/s41598-018-19987-7.
- Sherr, Ian. "Microsoft's Hololens 2 Isn't Meant For You, But It Could Change Your Tech In The Future". CNET, 2019, https://www.cnet.com/news/microsofts-hololens-2-isnt-meant-for-you-but-it-could-change-your-tech-in-the-future/.

- Sumit Patil and Rahul Kumar. Accelerating Extended Reality Vision With 5G Networks. 2019. doi:10.1109/iceca.2019.8821836.
- Maximilian Speicher, Brian D Hall, and Michael Nebeling. What is Mixed Reality? In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, CHI '19, pages 537:1—-537:15, New York, NY, USA, 2019. ACM. URL: http://doi.acm.org/10.1145/3290605.3300767, doi: 10.1145/3290605.3300767.
- William S Ryan, Jessica Cornick, Jim Blascovich, and Jeremy N Bailenson. Virtual Reality: Whence, How and What For, pages 15–46. Springer New York, New York, NY, 2019. URL: https://doi.org/ 10.1007/978-1-4939-9482-3{_}2, doi:10.1007/978-1-4939-9482-3_2
- Schmalstieg, Dieter & Fuhrmann, Anton & Hesina, Gerd & Szalavári, Zsolt & Encarnação, L. & Gervautz, Michael & Purgathofer, Werner. (2002). The Studierstube Augmented Reality Project. Presence. 11. 33-54.
- Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2015. A design space for effective privacy notices. In Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (SOUPS '15). USENIX Association, USA, 1–17.
- Schaub, F., & Cranor L. F. (2020). Usable and Useful Privacy Interfaces. In T. D. Breaux (Ed.), An Introduction to Privacy for Technology Professionals (pp. 176-229). IAPP.
- Sutherland, I. E. (1964). Sketchpad a Man-Machine Graphical Communication System. SIMULATION, 2(5), R-3-R-20. https://doi.org/10.1177/003754976400200514
- Statista (2018) 'Extended reality (XR)', available at: https://www.statista.com/statistics/539713/worldwide-virtual-and-augmented-realityhardware-shipments/ (accessed 16 September 2020).
- Staff. "Apple Glasses: VR And AR Are Coming". Macrumors, 2021, https://www.macrumors.com/roundup/apple-glasses/.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)
- Technavio. Global Extended Reality Market 2020-2024. Infiniti Research Limited, 2020. Accessed 12 Dec. 2020.
- "The XRSI Privacy Framework Version 1.0 | XRSI – XR Safety Initiative". XRSI – XR Safety Initiative, 2020, https://xrsi.org/publication/the-xrsi-privacy-framework. Accessed 14 Dec 2020.
- Thurman, Scott, and Yukari Iwatani Kane. "Your Apps Are Watching You". WSJ, 2010, https://www.wsj.com/articles/SB10001424052748704694004576020083703574602.
- Tene, Omer, and Jules Polonetsky. "A theory of creepy: technology, privacy and shifting social norms." Yale JL & Tech. 16 (2013): 59.
- Tobii Data Transparency. https://vr.tobii.com/sdk/develop/unity/unity-examples/data-transparency/
- Tsai, J. Y., S. Egelman, L. Cranor, and A. Acquisti (2011). The effect of online privacy information on purchasing behavior: An experimental study. Information Systems Research 22 (2), 254–268.

- Tsukayama, Hayley. Everything You Need To Know About Google Glass. 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/02/27/everything-you-need-to-know-about-google-glass/. Accessed 14 Apr 2021.
- Unity Privacy Policy. (2020, October 18). Privacy Policy. https://unity3d.com/legal/privacy-policy
- Unity. Top 2020 Trends: Enterprise AR & VR. Unity Technologies, 2020. Accessed 14 Jan 2021.
- Wassom, Brian. (2014). Augmented Reality Law, Privacy, and Ethics : Law, Society, and Emerging AR Technologies. Electronic books, Rockland, MA: Elsevier Science & Technology Books.
- Werro F. (2020) The Right to Be Forgotten: The General Report—Congress of the International Society of Comparative Law, Fukuoka, July 2018. In: Werro F. (eds) The Right To Be Forgotten. Ius Comparatum - Global Studies in Comparative Law, vol 40. Springer, Cham. https://doi.org/10.1007/978-3-030-33512-0_1
- Woodrow Hartzog, & Neil Richards. (2020). PRIVACY'S CONSTITUTIONAL MOMENT AND THE LIMITS OF DATA PROTECTION. Boston College law review, 61(5), 1687A – 1761. Newton Centre: Boston College School of Law.
- XRA. A New Reality in Immersive Technology: Insights and Industry Trends. Xra.Org, 2020. https://xra.org/wp-content/uploads/2020/09/XRA-Insights-and-Industry-Trends-Rev-31.pdf.
- XRCollaboration. https://xrcollaboration.com/guide/a-global-resource-guide-to-xr-collaboration/avatars/
- Yadin, Gilad. (2017). VIRTUAL REALITY SURVEILLANCE. Cardozo arts & entertainment law journal, 35(3), 707. Cardozo School of Law.
- Gallayanee Yaoyuneyong, Jamye Foster, Erik Johnson, and David Johnson. Augmented Reality Marketing: Consumer Preferences and Attitudes Toward Hypermedia Print Ads. Journal of Interactive Advertising, 2016. doi:10.1080/15252019.2015.1125316.
- Zimmerman, Thomas G, et al. "A Hand Gesture Interface Device." SIGCHI Bulletin, vol. 17, no. SI, 1986, pp. 189–92, doi:10.1145/30851.275628.
- "MIXED REALITY Security, Privacy, And Safety: Summit Report". ArSec.Cs.Washington.Edu, 2020, https://ar-sec.cs.washington.edu/files/MixedReality_SecurityPrivacySafety_Summit2019.pdf.

Appendix

WHAT IS BEING STUDIED? WHY?

This study is being conducted because there is a lack of federal regulations defining and providing human rights to digital privacy in the United States. More specifically, as it relates to emerging technologies, the advent of Extended Reality presents an unprecedented blending of the digital and physical world, which necessitates an immediate definition and prioritization amongst the protections provided across crucial players in today's private sector, public sector, and non-profit organizations.

While initial guidance has been provided by the XR Safety Initiative (XRSI) in the form of an XR Privacy Framework[1], this framework's details are not binding. They do little to address the lacking choice and consent that is currently standard across organizations' digital privacy 'agreements.'

Therefore, the main research questions that this research hopes to gain insight into through these interviews are based on the XRSI Privacy Framework 1.0:

- How do organizations understand/view XRSI's (more information below) proposed minimum, desired, and ideal privacy requirements (in place of federal law)?
    - What's most important?
- How easy/difficult is it for companies to implement even this minimal baseline?
    - What hurdles and/or incentives do organizations adopt more comprehensive privacy design/policies?

HOW ARE PARTICIPANTS RECRUITED?

The research goals will be accomplished by speaking with representatives from across the XR industry to understand what might be possible as it relates to the future of privacy in XR and will hopefully result in practical guidance for both organizations and government to deploy sufficient privacy protections for consumers and companies that adopt and continue to use XR in the coming years.

To do so, the researcher, and current UM dual-degree graduate student, Joshua Tooker, has compiled a list of potential interviewees that he will reach out to via social media (e.g., Linkedin, Twitter) and direct email to schedule time for a 30-45 minute interview. The researcher will rely on his primary and secondary professional networks to help drive participation. For example, between 2/28 and 3/6, with the help of his thesis advisor, Florian Schaub, and the XRSI CEO Kavya Pearlman, a standardized participation request will be sent via email, posted on Linkedin and Twitter.

To facilitate and optimize efficiency during the recruitment efforts, prospective participants will be directed to participate in an ingestion survey via the University of Michigan Qualtrics platform. This survey will provide the confidentiality and consent agreement for both taking part in the online Qualtrics survey, as well as the following interview(s) as a part of this ingestion survey.

STUDY PROTOCOL

As stated above, interview participants will be asked to complete a short survey and take part in a 30-45 minute interview. The interview style will be a semi-structured Zoom default video with an audio-only option to interview. The interviewee will determine whether to meet via video or audio-only. Note that only the Zoom audio will be recorded.

[1] https://xrsi.org/publication/the-xrsi-privacy-framework

The interview script has been designed with specificity in mind to get a better understanding of the interviewee's connection to the XR industry and answer the following general questions:

- About the interviewee's role in XR and their proximity to privacy-related issues
- Discuss and get feedback on participants understanding of specific parts of the existing XRSI Privacy Framework
- Identify participants' specific interests, constraints, and future related to privacy in XR within the context of their particular professional group (e.g., industry private sector professionals, non-profit privacy advocates)

For more information on the individual interview execution, an interview protocol has been attached to this application.

HOW WILL RESEARCHERS ENSURE CONFIDENTIALITY?

Because this study collects information about individuals, this research's primary risk is a loss of confidentiality. To mitigate data loss, individual interview record(s) will be codified to provide anonymity. Moreover, to then allow for proper analysis of the interview data, a separate file creating a key with the code(s) used to anonymize the data and any individually identifiable information will be stored in a different location. The anonymized data will be held on a University of Michigan Google Drive. In contrast, the data key will be stored in a separate University of Michigan Dropbox account. Access to both files will be granted only to necessary team members.

The process for anonymizing the data will be twofold. Upon completing the recruitment process, the primary researcher, Joshua Tooker, will download the data to his local machine. He will then separate any identifiable contact or demographic data into a separate excel spreadsheet. Next, he will assign individual code names (e.g., Participant 1) to both the spreadsheet generated from the survey results and the newly created participant key. As stated above, this separate key will then be stored in a different dropbox location. Moving forward to the second phase of data collection, the interviews, Joshua will identify participants for the interviews by analyzing their personal/professional interest and role in the XR industry. Before the interview, selected participants will have a unique interview script generated to their anonymous participant code.

ANALYZING THE DATA - identify themes/issues >> survey that takes themes/perspectives

The data will be analyzed after all interviews are completed. Information from each question will be organized, so each participant's answer to that specific question is available. The next step will be to identify similarities and differences between the solutions. After similarities and differences are identified, the themes that emerge will be named and categorized (for answers). I will then assess and provide a perspective on the relationship for the organized themes on the potential for adoption as an industry norm. This will establish the adoption criteria and ranking that will then be integral to the recommended next steps for applying this data by private industry, non-profits, and public sector is rooted in the feasibility across the XR privacy landscape.

Default Question Block

Study title: Understanding Extended Reality Across Sectors

Principal Investigator: Joshua Tooker, MBA/MSI Candidate, University of Michigan

Faculty Advisor: Dr. Florian Schaub, Asst. Professor, University of Michigan

You are invited to take part in a research study. This page contains information that will help you decide whether to join the study and answer this quick survey, with a potential follow-up interview if you decide to participate.

I am a current graduate student at the University of Michigan pursuing my MBA and Masters in Information with a focus on Human Computer Interaction in Extended Reality (XR). One of my program requirements is to complete a Masters Thesis for which I am focusing on understanding what consent looks like in XR. It's my goal to speak with business leaders, academics, privacy advocates, and policymakers to understand where there is the potential for collaboration and compromise in developing XR technologies, while giving users more agency in the providing consent without sacrificing the incentives that hardware and software developers have to develop these technologies.

1. Key Information
Things you should know: This research will help Joshua Tooker from the University of Michigan School of Information working on a Master's Thesis to understand: how business leaders, academics, privacy advocates, and policymakers understand where there is the potential for collaboration and compromise in developing XR technologies, while giving users more agency in the providing consent without sacrificing the incentives that hardware and software developers have to develop these technologies.

Taking part in this research study is voluntary. You do not have to participate and you can stop at any time, for any reason. Please take time to read this entire form and ask questions before deciding whether to take part in this research study.

2. What will happen to me in this study? You should expect a 30-45 minute conversation via a Zoom audio or video call, which will be determined by the participant. Upon completion of the interview, I will transcribe the notes from our conversation and store the anonymized responses in a secure location. For the interview transcript and report, a codename will be

used so your responses will be anonymous and secure. At that time, your participation will be considered complete.

3. What risks will I face by taking part in the study? What will the researchers do to protect me against these risks?

You do not have to answer any questions you do not want to answer.

Only your name and other information that can directly identify you will be stored securely and separately from the research information we collected from you.

Because this study collects information about you, the primary risk of this research is a loss of confidentiality. To mitigate a loss of data, your individual interview record(s) will be codified to provide anonymity. Moreover, to then allow for proper analysis of the interview data, a separate file creating a key with the code(s) used to anonymize the data and any individually identifiable information will be stored in a separate location. The anonymized data will be stored on a University of Michigan Google Drive, while the data key will be stored in a separate dropbox account owned by the primary researcher, Joshua Tooker. Access to both files will be granted only to necessary team members.

The process for anonymizing the data will be twofold. Upon completion of the recruitment process, the primary researcher, Joshua Tooker, will download the data to his local machine. He will then separate any identifiable contact or demographic data into a separate excel spreadsheet. Next, he will assign individual code names (e.g., Participant 1) to both the spreadsheet generated from the survey results and the newly created participant key. As stated above, this separate key will then be stored in a separate dropbox location. Moving forward to the second phase of data collection, the interviews, Joshua will identify participants for the interviews by analyzing their personal/professional interest and role in the XR industry. Before the interview, selected participants will have a unique interview script that will be generated to their anonymous participant code.

The results of this study could be published in an article or presentation, but would not include any information that would let others know who you are without your permission. The findings from both the survey and interview may be used as anonymous contributions to the Masters Thesis. In any use of publishing the data, the researchers will eliminate any potentially-identifiable details and/or information.

4. How could I benefit if I take part in this study? How could others benefit?
You may not receive any personal benefits from being in this study. However, others may benefit from the knowledge gained from this study with the broader XR community as a report.

5. Who can I contact about this study?
For questions regarding this study, please contact:

Principal Investigator: Joshua Tooker
Email: jtooker@umich.edu

Faculty Advisor: Dr. Florian Schaub

Email: fschaub@umich.edu

You can also contact the University of Michigan Compliance Hotline at 1-866-990-0111.

6. Consent/Assent to Participate in the Research Study

By clicking 'Yes' and continuing belo, you are agreeing to be in this study. However, continuing with this survey does not guarantee you will be in an interview. Make sure you understand what the study is about before you move forward. The team will give you a copy of this document for your records and the team will keep a copy with the study records. If you have any questions about the study after you sign this document, you can contact the study team using the information above.

I understand what the study is about and my questions so far have been answered. I agree to take part in this study.

- ◯ Yes
- ◯ No

Do you have a professional or personal interest in Extended Reality (i.e., XR, Augmented Reality, Mixed Reality, Virtual Reality) -- optional

- ◯ I have a professional interest
- ◯ I have a personal interest
- ◯ I have both a professional and personal interest
- ◯ I am not interested

What is your professional or personal involvement in Extended Reality (i.e., XR, Augmented Reality, Mixed Reality, Virtual Reality) -- optional

Please choose the answer that best describes your experience

- ◯ Hardware Developer
- ◯ Software Developer
- ◯ Business/Product/Program Manager
- ◯ Journalist
- ◯ Legal/Public Affairs
- ◯ Non-Profit
- ◯ Investor
- ◯ Technology enthusiast
- ◯ Technology Influencer
- ◯ Privacy Advocate
- ◯ [ ] Other

Please expand on your personal or professional experience... -- optional

Block 1

Are you interested in participating in an interview with the research team?

- ◯ Yes
- ◯ No

Please enter your email address, so we can schedule a time to meet with you.

Age

- ◯ 18-24
- ◯ 25-34
- ◯ 35-44
- ◯ 45-54
- ◯ 55-65
- ◯ >65

Geographic Location

- ◯ United States - Northeast
- ◯ United States - Mid-Atlantic
- ◯ United States - Midwest
- ◯ United States - Mountain
- ◯ United States - Southeast
- ◯ United States - South
- ◯ United States - West
- ◯ Europe -Western
- ◯ Europe - Eastern
- ◯ Europe - UK/Ireland
- ◯ Africa
- ◯ Middle East
- ◯ Asia
- ◯ Australia

What is your gender?

- ◯ man
- ◯ woman
- ◯ non-binary
- ◯ prefer not to disclose
- ◯ _____ prefer to self-describe

What are your pronouns?

- ◯ He/Him/His
- ◯ She/Her/Hers
- ◯ They/Them/Theirs
- ◯ _____ Other

Occupation

Industry

Block 2

Is there someone with a personal or professional interest (i.e., XR, Augmented Reality, Mixed Reality, Virtual Reality) that you think I should speak with? If so, please provide their email address or share the survey link.

Is there anything else you'd like to share?

- ◯ Yes
- ◯ No

Please share your additional feedback below:

Joshua Tooker
UMID#: 31778252

What questions am I trying to answer?

The research questions that I hope to gain insight into through these interviews are based off of the XRSI Privacy Framework:

- How do organizations understand/view XRSI's (more information below) proposed minimum, desired, and ideal privacy requirements (in lieu of federal law)?
- What's most important?
    - How easy/difficult it is for companies to implement even this minimal baseline?
    - What are the hurdles and/or incentives for organizations to adopt more comprehensive privacy design/policies?

The XRSI Privacy 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. Its goal is to provide initial guidance to members of the XR community for how to incorporate privacy considerations into the development and deployment of their work in the XR space. The above research questions for the Master's thesis are born out of gaps between the guidance provided in the XRSI framework and previous research that has been completed by the Academy and privacy professionals throughout history, but primarily during the digital age (i.e., since 1990). The XRSI 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:

- **Leave no one behind**
- **Be accessible**: Everyone must be able to participate in the digital society
- **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
- **Keep everyone safe and secure**: Shape rules and practices to enable a secure and resilient immersive environment
- **Build new rules to promote trust**: Develop new, flexible, participatory governance mechanisms to complement traditional policy and regulation in a constantly evolving domain

Joshua Tooker
UMID#: 31778252

Interview

Style of Interview

This will be a semi-structured Zoom default video with audio-only option to interview. The decision to meet with video or audio-only will be determined by the interviewee. Depending on the flow of the interview, some questions may not be asked, some questions will be adapted based on what the interviewee says/does, and additional probing questions may be added if necessary.

Intended plan for interviews

An ideal method of interviewing: Set up the interview via a Zoom audio or video call The Zoom audio or video call will only be audio recorded.

Joshua Tooker
UMID#: 31778252

Consent/Introduction Section (start from here)

Introductory:

Hello, my name is Josh. I want to thank you in advance for your time and your participation. I am a current graduate student at the University of Michigan pursuing my MBA and Masters in Information with a focus on Human Computer Interaction in Extended Reality (XR). One of my program requirements is to complete a Masters Thesis for which I am focusing on understanding what privacy and consent looks like in XR. It's my goal to speak with business leaders, academics, privacy advocates, and policymakers like yourself to understand where there is the potential for collaboration and compromise in developing XR technologies.

What questions am I trying to answer?

The research questions that I hope to gain insight into through these interviews are based off of the XRSI Privacy Framework:

- How do organizations understand/view XRSI's (more information below) proposed minimum, desired, and ideal privacy requirements (in lieu of federal law)?
- What's most important?
    - How easy/difficult it is for companies to implement even this minimal baseline?
    - What are the hurdles and/or incentives for organizations to adopt more comprehensive privacy design/policies?

This interview will take about 30 to 45 minutes, during which time we'll go through some questions.

- Whose responsibility is it to determine what privacy is required and provide it?
- The XRSI Privacy Framework lists providing "disclosures that satisfy CCPA and GDPR requirements" as a minimum expectation. Generally, the minimum expectation is that the "organizations should have legally compliant privacy policies."
    - Is this sufficient as a minimum expectation in XR? Why or why not?
    - How might these laws need to be adapted to meet the specific needs of XR?
- The XRSI Privacy Framework raises the question of "'real choice' to refuse the processing and a question of whether it is possible to draw the line between necessary and unnecessary data."
    - What, in your opinion, ensures "real choice" and/or valid permission is granted in the context of XR?
- What are the complexities (i.e., hurdles and/or incentives) for businesses and/or technologists to adopt more comprehensive privacy design/policies?

Do you have questions about the consent form? If so, the interviewer will answer those questions

Voluntary Participation: Your participation is entirely voluntary. You can choose to skip any portion of the questions you wish not to answer and can withdraw your consent or discontinue participation at any time without consequence.

Confidentiality: Before we start, I want to mention that your comments will be confidential. Your name and personal information will not be recorded with the answers you give. Though we plan to use what we learn from this interview in my Master's Thesis, and potentially a publication of this work, none of these will reveal participants' name or organizational affiliation (e.g., person working as executive for VR company; etc.).

Audio recording: One final thing, in order to guarantee that we have properly documented everything, do you mind if we take an audio recording? As a reminder, no one outside of our team will have access to the recording. Once the project has concluded, all audio recordings will be destroyed.

Is this okay? ***(if so, turn on the Zoom recorder, otherwise put recorder away)***

Do you have any questions for us before we begin? *(**wait several seconds to make sure interviewee has time to process and ask any questions they may have**)*

All right then, let's proceed.

Joshua Tooker
UMID#: 31778252

Questions for interviewees -- DO NOT LEAD OR BIAS THE INTERVIEWEE

Warm-up questions about XR and their roles *(the goal is to build a little rapport and get the interviewee talking in the beginning)*

- How long have you been in the position <INSERT JOB ROLE HERE>?
    - **Can you share how you became <JOB TITLE>?** Why did you want to be <JOB TITLE>?

- What is the most recent project/programs that you are in charge of and/or have worked on?

- Can you explain some of your primary interactions with Extended Reality (i.e., XR)?
    - How does XR factor into your work/personal life?
    - What's going well?
    - What are your main challenges/hurdles when adopting/building XR tech? Do these differ from what you see as the challenges facing the XR industry?

Transition to discussion about privacy in XR

(Note: it may require that I bring up privacy issues as a concern if the interviewee doesn't identify it as a main challenge)

Questions about privacy in XR

- **What are your thoughts on privacy in the context of XR?**
- **How do you think about privacy and XR in your role?**
    - What does this look like day-to-day?
    - Where is privacy in your XR hierarchy of needs?

- **Who's responsibility it is to determine what privacy is required and provide it?** Whose role is it to create multiple profiles based on the NIST principles (e.g., the business)? Why?
- How familiar are you with the XR Safety initiative?
    - XRSI privacy framework?
    - Can you talk about a recent project where consent/privacy/etc. came up? How did you deal with that?

(Note: If the interviewee is unfamiliar with the XRSI privacy framework, I have to summarize it. If that is necessary, I will read the below statement)

- *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.*

Questions about the Specific Parts of the XRSI Privacy Framework

- The XRSI Privacy Framework lists providing "disclosures that satisfy CCPA and GDPR requirements" as a minimum expectation. Generally, the minimum expectation is that the "organizations should have legally-compliant privacy policies."
    - **Is this sufficient as a minimum expectation in XR? Why or why not?**
    - How might these laws need to be adapted to meet the specific needs of XR?
        - In its current form, are there gaps in protection (for whatever reason)? In other words, what does the minimum level of protection actually provide?
    - What is challenging to achieve desired or ideal?
    - What is easy or accessible that has not been done? Where could there be compromise?

- The XRSI Privacy Framework lists "the desired expectation for XR privacy policies should be that they: should include layered, just-in-time, and other contextual privacy communications."
    - How might these requirements fit into the minimum requirements for XR?
    - **What are some of the potential technological or business complexities that would prevent these from being adopted.**

  Note: Examples of Desired expectations from the XRSI Privacy Framework below:
    - *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.*

- **The XRSI Privacy framework lists that organizations "should provide clear indications to bystanders or other XR users through visual or audio indicators when data is being collected and recorded."**
    - **Does the ideal state go far enough, or too far, in protecting users (across the four components of the XRSI framework)?**
    - whether companies consider these levels practical or whether they go too far from their perspective, or maybe they might also want to do more

  Note: Examples of Desired expectations from the XRSI Privacy Framework below:
    - *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:*
- *Developing XR digital aides 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*

Questions to specific consent, choice, and context in XR

- The XRSI Privacy Framework raises the question of "'real choice' to refuse the processing and whether it is possible to draw the line between necessary and unnecessary data."
  - What, in your opinion, ensures "valid permission" is granted in the context of XR?
  - Should this 'real choice' be freely given? If so, how? Why?
- **What are the hurdles and/or incentives for organizations to adopt more comprehensive privacy design/policies? What's most important?**

Questions to specific professional groups (e.g., Industry, Academy, Public-Sector, Non-profit)

- **Industry:**
  - How can academics, non-profit groups, and policymakers make prioritizing privacy and consent easier for you?
  - For XR, two aspects that should be considered according to the framework is making them immersive and comfortable. What does that mean to you? XRSI privacy framework 1.6.5
  - Bystander privacy?!
    - Do we use the physical world's definition of 'freely given' or Web 2.0?
    - How do you adequately address varying degrees of consumer/user consent?
- **Academy:**
  - Should companies pause commercialization until questions around transparency, awareness, accountability, and trust are sorted out?
    - How might this impact 'right' incentives for organizations to prioritize consumer privacy?
- **Public-Sector:**
  - What must be true for legislatures to prioritize the recommendations in the XRSI Privacy Framework as legislation is created?

- **Non-profit (privacy advocates):**
  - What are the most important reasons for a different application/understanding of privacy and consent in XR?
    - What do you think do/don't consumers understand about the data being collected and its use?
    - What's the risk and repercussions to bystanders in public?
    - What is your perspective on consent be provided directly or indirectly?
      - Is there precedent, ever, for ignoring non-consenting parties ?
  - Do you see challenges working with industry on privacy issues? What are they?
    - What are the top 3 (if many given)?
    - How might they be overcome?

Wrap-up Questions

- Is there anything else that you think I should know?
- Do you have any questions for me?

Conclusion/Debrief Section

That concludes our interview for today. Thank you again for taking the time out of your schedule to speak with us. As a reminder, we intend to code all data received to preserve confidentiality and anonymity. No one else will have access to the recording, and all audio recordings will be destroyed once the project has concluded.

Do you have any questions for us? *(**wait several seconds to make sure interviewee has time to process and ask any questions they may have**)*

At any point you have questions, please feel free to reach me at jtooker@umich.edu.