IEEE SA
STANDARDS ASSOCIATION

INDUSTRY CONNECTIONS REPORT

THE IEEE GLOBAL INITIATIVE ON ETHICS OF EXTENDED REALITY (XR) REPORT

EXTENDED REALITY (XR) AND THE EROSION OF ANONYMITY AND PRIVACY

Authored by

Mark McGill

Chapter Leader

IEEE

TRADEMARKS AND DISCLAIMERS

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The ideas and proposals in this specification are the respective author's views and do not represent the views of the affiliated organization.

ACKNOWLEDGEMENTS

Special thanks are given to the following contributors of this paper:

Kent Bye

Michael Middleton

Monique J. Morrow

Samira Khodaei

The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA

PDF: STDVA25065 978-1-5044-8131-1

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE SA INDUSTRY CONNECTIONS DOCUMENTS

This IEEE Standards Association ("IEEE SA") Industry Connections publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the IEEE SA Industry Connections activity that produced this Work. IEEE and the IEEE SA Industry Connections activity members expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the IEEE SA Industry Connections activity members disclaim any and all conditions relating to: results; and workmanlike effort. This IEEE SA Industry Connections document is supplied "AS IS" and "WITH ALL FAULTS."

Although the IEEE SA Industry Connections activity members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE OR IEEE SA INDUSTRY CONNECTIONS ACTIVITY MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder. The policies and procedures under which this document was created can be viewed at https://standards.ieee.org/about/bog/iccom/.

This Work is published with the understanding that IEEE and the IEEE SA Industry Connections activity members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

TABLE OF CONTENTS

EXTENDED REALITY (XR) AND THE EROSION OF ANONYMITY AND PRIVACY

ABSTRACT

This report is the result of work within the IEEE Global Initiative on Ethics of Extended Reality (XR), a multidiscipline group of industry practitioners, ethicists, academics, researchers, educators, and technology enthusiasts. It has been written to focus on a wide range of ethical issues related to XR and the erosion of anonymity and privacy. This report builds on work outlined in the "Extended Reality" chapter of the IEEE's seminal ethics-focused publication, *Ethically Aligned Design*. XR is a term used to broadly refer to a suite of immersive technologies including virtual reality, augmented reality, and spatial computing. The scope of this report is the exploration of ethics-related issues in terms of anonymity and privacy of XR applications; the aim is to initiate expert-driven, multidiscipline analysis of the evolving XR Ethics requirements, with a vision to propose solutions, technologies, and standards in future updates. The set of recommendations within this report will hopefully contribute to industry conceptualization of socio-technological issues, highlight concreted recommendations, and lay the groundwork for future technical-standardization activities.

MONIQUE J. MORROW & MATHANA

CHAIR & VICE CHAIR

IEEE GLOBAL INITIATIVE FOR ETHICAL EXTENDED REALITY

1. INTRODUCTION

Extended reality (XR) technologies, referring in combination to augmented, virtual, and mixed reality, will see pervasive and widespread adoption by both consumers and industry in the coming decades. This technology will revolutionize many aspects of everyday life: enhancing productivity through mobile and virtual workspaces ([1],[2]); supporting new immersive media experiences [3]; augmenting and enhancing intelligence and perception [4]; enabling telepresent communication and collaboration [5]; and fundamentally transposing digital artificial intelligence (AI) assistants and applications from heads-down smartphones toward heads-up spatial virtual experiences.[1]

To unlock these XR experiences, devices will pack sophisticated hardware to sense the world around them (e.g., LiDAR, camera arrays, microphone arrays) and the XR user (e.g., physiological sensing, EEG)—all features that are fundamentally necessary to drive key functionality. However, this breadth of sensing also means that XR applications and platforms will have the capacity to process captured data toward unanticipated and unintended ends. Furthermore, XR applications and platforms will be able to instrument the actions, attitudes, and emotions not just of the wearer, but of all those within their sight or within the sensing range of their equipment and its networks. Combined with cloud computing and machine learning, both the benefits and drawbacks of this technology will be unleashed on a societal scale, which will instigate new potential digital harms for both users and bystanders, from violations of anonymity, privacy, and identity to mass distributed surveillance and behavior nudging. The scale of this potential for harm is such that the social and privacy issues exposed by XR adoption are considered one of the grand challenges in XR research [6].

In this paper, an overview is given of some of the key privacy challenges introduced by the anticipated widespread adoption of XR technologies, algorithms, and services. This paper also discusses where existing rights and legislation fall short in safeguarding users of, and bystanders to, this technology. Recommendations regarding fundamental protections and mitigations that could either diminish or prevent XR-enabled digital harm are also proposed. More broadly, the text reflects on the tension between a desire to maintain human rights to privacy and anonymity, versus the potential consensual or induced erosion of these rights in the haste to take advantage of the benefits these technologies offer to everyday life.

[1] Numbers in brackets refer to the references listed in Section 3.

2. KEY ISSUES IN XR PRIVACY

2.1. XR SENSING AND COMPUTED DATA

At an individual level, the sensing found in XR headsets and their associated peripherals will enable the capture of a range of data regarding a user as follows:

- **Movements and physical actions:** Optical and inertial tracking of head/body/limb movements, EMG neuromotor input, sensing of facial expressions, auditory sensing of speech and non-speech activity, etc.
- **Neural activity:** EEG for brain-computer interfaces
- **Context:** Location tracking, Simultaneous Localization and Mapping (SLAM), and machine learning-driven analysis of optical data
- **Physiology:** Eye/gaze tracking, HRV sensing, and other biometrics

This pervasive capture of personal "sensitive" data is unique to XR relative to other consumer technologies [7], but fundamentally necessary. Such sensing underpins much of the core functionality that makes this technology, and the software that runs on it, so compelling to futurists. It drives the capability to create more usable spatial interactions, enables new applications that better address accessibility needs, and enhances the understanding of the user's context, behavior, and needs that drive better AI assistants. For example, an XR headset *without* sophisticated optical sensing would feature greatly degraded performance in all use cases. Many current consumer devices would lose the ability to accurately track its position and orientation in the world, meaning it would be unable to render the exocentric (world-fixed) spatial virtual content that underpins immersive virtual and augmented reality experiences. Moreover, this feature—among others—lowers the risk of cybersickness in VR by enabling visual perception of experienced motion. Consequently, for much of the sensing described previously, there is a need to understand how people can best live with the ubiquitous presence of this sensing in consumer XR technology.

Notably, the availability of this sensed user data, coupled with real-time local and edge-computing processing and sensor fusion, introduces and amplifies the risks posed to an XR user's anonymity and

privacy [8]. This is a result of “computed” data [7], whereby machine learning algorithms and AI-driven approaches can be trained and employed to predict/infer information about identity, behavior, activity, and internal state, and make decisions based on this computed data. These algorithms are often a “black box” whose processes are opaque to even their developers, and the results of these processes are imperfect. Yet these algorithms are offered to developers as services that can trivially enhance the capability of an application to process sensed data (Microsoft Cognitive Services, Apple’s CoreML, Amazon’s AWS-driven AI/ML services, Google Cloud, etc.). The algorithms are subject to significant issues such as algorithmic bias [9], as well as false positives and other errors. This may lead to cases where algorithms interpret or “speak for” behavior or elements of a person’s identity that genuinely do not match their identity (e.g., if an XR application insists a person's data speaks to a sexual identity other than their own). This influx of data is yet to be matched by an equivalent transparency and mastery of the analysis.

Crucially, each data source offered by XR has the capacity to be exploited in a variety of anticipated and unanticipated ways. For example, eye tracker data conveys eye movements and basic pupil/iris properties (e.g., pupillometry), intended to enable some understanding of where, and what, a user is looking at. This can be used for indisputably beneficial reasons, for example creating gaze-based interactions for accessible interfaces. However, research has demonstrated that significantly more information can be inferred from just this limited set of features than might have been anticipated [10]—for example, making assessments of cognitive load, fatigue, drug consumption, physical health, etc. Computed data, sensor fusion, and estimation can also be used to fill in the gaps in what information is made available to an application. For example, it is possible to estimate eye gaze in VR based on a combination of less sensitive head and hand pose data [11].

2.2. IDENTITY AND ANONYMITY OF SELF

From the perspective of anonymity and identity, it has been demonstrated that based on simple captured positional tracking data, users could be personally identifiable with an accuracy of as much as 95% [12], with task-driven behavioral biometric data enhancing our capability to uniquely identify individuals [13]. And in time, it will be reasonable to expect that seemingly innocuous combinations of sensed data might enable a third party (e.g., an XR application) to not just uniquely identify a user, but also unlock information regarding characteristic and protected traits (gender expression, age, sexuality, accessibility needs, race, etc.), as well as other personally identifiable information without the user’s

knowledge or consent. The consequences of this could be significant and devastating for the individual concerned—for example this information could be used for the purposes of discrimination and profiling [14] in reality (e.g., further cementing stereotypes and biases), or open users up to blackmail if their anonymous activities in VR were linked to their real-world identity.

The advanced state of data capture and processing that is now occurring due to artificial intelligence, machine learning, and the vast increase in user and sensor input information has resulted in an excess of data being made freely and publicly available beyond the anticipated uses of those providing it. As such, this problem of anonymity is not limited to XR; however, XR stakeholders should put themselves at the forefront of supporting advanced research, development, and implementation of established or emerging fields of privacy that support the conclusions in this paper. One such field is "differential privacy" [15], which specifically focuses on the problem of sharing data about a group publicly but withholding information about individuals, such that any single individual's data is not enough to adjust the data set in a manner that would allow their identity to be inferred. These types of protections will be critical not only for maintaining appropriate privacy standards, but for developing a public trust that allows for the positive leveraging of mass-collected data in a manner that does not undermine the individual.

Recommendation #1	XR stakeholders should actively develop and/or support efforts to standardize differential privacy and/or other privacy protocols that provide for the protection of individual identities and data.

2.3. AUGMENTED INTELLIGENCE AND MENTAL PRIVACY

Beyond identity and personal traits, the treasure trove of sensed XR data will unlock the ability to develop a sophisticated, longitudinal understanding of an individual—from their behaviors, intentions, and actions to their mental and cognitive processes and phenomenological experiences; to stress/arousal and their affective state. This will effectively enable third parties to construct a digital twin or model of an individual's identity, giving them unique insights into intimate details of their lives, such as their likes, preferences, and attitudes. This class of processing is defined by Heller as "biometric psychography," whereby biometric data is used to instead identify a person's interests [16]. The

consequence of this is that it is not just the user's physical privacy and outward presentation that is potentially being eroded—their mental privacy [17] is as well, from low-level brain activity data to inferred behavior and intent.

However, again, there are valid reasons why such technology might be employed on personal consumer XR devices. One of the primary selling points on the necessity of this is in enabling contextually aware AI and augmented intelligence/mental augmentation (i.e., supplementing memories and enhancing cognition [4]). For example, consider the use of brain activity sensing to detect perceived user errors [18]. This capability was transposed to VR to enable assistance and intervention when users conducted errors in a given task [19]—effectively a basic form of augmented intelligence where the XR system could assist the user to avoid or correct detected errors. Brain activity sensing can be used to infer a variety of information about the user, including physical activity, attention, and affective state [20]. This, in turn, can enhance the systems understanding of the user and their context, providing missing insight into what the user feels or how they react to a given situation.

Brain activity is just one route toward developing this insight. For example, optical tracking provides the ability to detect both personal features (e.g., body language, facial expressions, micro gestures) as well as contextual information (instrumenting everyday actions and behavior); physiological sensing provides insight into arousal and fatigue; and eye gaze can be used to infer cognitive load and instrument attention amongst other features [21]. In this way, a detailed multi-sensory model of a user's mental state, personality, and decision-making behaviors could be constructed based on the availability of XR-requisite sensing. Moreover, this model will not be static—it will be refined and improved over time, with research unlocking new ways of processing and fusing this data to reveal additional unconsidered insights. And, crucially, this model will not be perfect. For example, determining affective states based on facial movements has been demonstrated to be a deeply flawed approach [22], on occasion bordering on pseudoscience [23] with AI-driven approaches likely to introduce additional uncertainty and error [24].

The consequences of having this deep, intimate, evolving, persistent, and potentially flawed understanding of an individual are only just beginning to be understood. This understanding could be used to peoples benefit, assisting in their everyday lives; however, combined with XR's capacity to alter a user's perception of reality, it also opens the possibility of real-time manipulation, nudging, and abuse—both of individuals and at a societal level. For example, user behaviors or thoughts could be

anticipated and consequently manipulated to the benefit and desire of a third party (the XR platform, applications on that platform, governments, etc.), which undermines the right to agency, or reverse-engineering fixed action patterns. This might take the mundane form of redirecting attention to purchase a different product. Or it might take a more extreme form, such as reinforcing existing bias toward "othered" groups or manipulating how we think about a politician or political party.

Moreover, once this data has been captured by said third parties, further processing and insight into users lives and behaviors might be generated far into the future, constantly refining a digital twin of their identity. What are the constraints regarding how this data is kept and used in the future? In picking apart how people think and behave without guidelines on how this data can be used, it risks further misuse of this data in the future. Such propositions have led to calls for "neuro-rights" [25], referring to human rights set within neuro-technologies, aiming to enshrine protections regarding identity, agency, mental privacy, exposure to algorithmic bias, and access to augmented intelligence/mental augmentation. It is likely that the need for such rights will become increasingly apparent in the coming years.

Recommendation #2	XR platforms should seek to adopt voluntary proposals such as "neuro-rights" to help ensure that the mental privacy of users is not violated.

Recommendation #3	XR platforms should disclose (in plain language) and give users agency over what personal data is being captured, how this data is processed and to what ends, and for how long it (and its processed outputs) is retained.

Recommendation #4	Individuals should have the right to decide how their identity (or representations/modifications thereof, such as digital twins or augmented appearance) is perceived and appropriated by others in XR.

2.4. IDENTITY AND PRIVACY OF BYSTANDERS

By necessity, XR devices commonly have sophisticated world-facing environmental sensing built-in, such as stereo camera arrays, LiDAR sensing, and directional microphones. This sensing is what, in part, drives the Simultaneous Localization and Mapping (SLAM) algorithms that allow XR devices to position

themselves in the world and render experiences from the perspective of the user. But the availability of such sensing in wearable, distributed technology opens a host of capabilities beyond positional tracking.

Perhaps the most immediate risk enabled by such sensing is in the ability to trivially observe and track bystanders—people within sensing range of the XR user. Driven by advances in machine learning and computer vision, it will be trivial for an XR device to segment, classify, and track these proximate others. It can be assumed that a device will be able to volumetrically capture the bystander and generate a 3D mesh of their body and likeness. At the most basic level, this data will unlock the ability to pseudo-anonymously identify and track nearby individuals whenever they are within sight of the XR user. When combined with social media platforms, publicly available data sets (e.g., facial ID sets of celebrities), and cloud computing applications will have all the necessary data to strip these bystanders of their anonymity and identify them to the XR user in real-time. As Facebook recently acknowledged, such platforms are likely to incorporate facial recognition due to its obvious benefits in business, noting for example that it "might be the thorniest issue, where the benefits are so clear, and the risks are so clear, and we don't know where to balance those things." They suggested it would be supported only "if it could be done in a way the public and regulators were comfortable with," such as enabling bystanders to "mark their faces as unsearchable" [26]. This capacity for photorealistic volumetric capture will also have significant implications for how people can safeguard, control, and augment their own identities as perceived by others, and how others might augment or appropriate their identities in turn [27].

However, identity is just one aspect of a bystander's privacy that will be trivially violated by pervasive, public use of XR. The visual and auditory data captured by an XR device will enable sensing and processing activities largely in line with what was previously discussed for individual XR users. For example, near-IR cameras can be used to sense physiological signals such as heart rate variability at-a-distance [28], while any optical and auditory capture obviously suggests a wealth of data that could be used for biometric psychography, identifying affective state (using facial expressions, speech, etc.), and behavior/activity tracking. Consequently, the same risks that an individual XR user is exposed to regarding mental and physical privacy are carried over to all bystanders in their proximity. The key difference is that where an XR user may have reasonably consented to such data capture, in this case bystander data may be captured, processed, retained, and longitudinally refined, all without the bystander's knowledge or consent, and all within the time it takes for a surreptitious glance.

Recommendation #5	Where some aspect of bystander data is legally permissible to be captured and processed, bystanders should be made aware that this capture is occurring and should have the capacity to revoke implicit or assumed consent for capture.

Recommendation #6	Platforms should refrain from enabling the persistent pseudo-anonymous identification or tracking of bystanders and their associated data. Where there is a risk that requested sensor streams enable such tracking and violation of bystander privacy, such streams should be obfuscated by default (e.g., making bystanders unrecognizable).

2.5. WORLDSCRAPING, "LIVE MAPS", AND DISTRIBUTED SURVEILLANCE

A single XR headset has the capacity to surveil a space only to the extent that it can sense that space, with there being physical limitations on the range, field of view, resolution, and accuracy of any single user's device. However, in conjunction, multiple headsets or other devices, including embedded XR-capable sensors, can surveil a space from multiple angles. At a saturation point where most of the public are wearing XR devices in their everyday lives, this capacity to surveil reality becomes ever present. XR sensing has the ability to surveil not just bystanders, but every aspect of virtuality and reality, supporting the capability for "persistent, ubiquitous recording" [29] by XR applications and platform owners. Previously the "natural limits of human memory" ensured a degree of privacy; "electronic devices, however, can remember perfectly, and collect these memories in a centralized database to be potentially used by corporate and state actors" [30], enabling cybersurveillance in VR [31], and surveillance/sousveillance in reality through AR, of the behavior and actions of ourselves and others.

When considered *en masse*, distributed XR devices have the potential to completely surveil and capture the ever-changing state of real spaces as well as their inhabitants. For example, Facebook's Project Aria specifically notes the ability to generate a "live map of 3D spaces" [32], a concept Hon termed "worldscraping" [33]. Facebook is not unique in chasing this aim of capturing Big Data regarding the world and its inhabitants. The creators of Pokémon Go, Niantic, have formed a "Planet-Scale AR" consortium (including Deutsche Telekom, EE, Globe Telecom, Orange, SK Telecom, SoftBank Corp., TELUS, and Verizon) with the intent to create distributed AR sensing that will allow for anyplace/anytime multi-user AR experiences [34], boasting the capability to crowdsource mesh data for environment capture [35]. Key AR APIs and services from Microsoft (Mixed Reality ToolKit), Apple (ARKit), and Google

(ARCore) varyingly contain capabilities for topological mapping, scene understanding, classification, world positioning, and geometry generation/capture that represent the first steps toward making worldscraping a feasible reality. Consequently, XR has the potential to facilitate a "global panopticon society of constant surveillance in public or semi-public spaces. In this dystopia, the possibility of being recorded looms over every walk in the park, every conversation in a bar, and indeed, everything you do near other people" [30].

Recommendation #7	The right to privacy should be extended to protecting real-time surveillance of homes, businesses, and public spaces.

Recommendation #8	Capture and processing of non-personal real-time data regarding public and private spaces needs to be regulated in the same way that personal data is through e.g., GDPR.

2.6. AUGMENTED PERCEPTION AND PERSONAL SURVEILLANCE

XR enables users not just to capture reality, but also to alter, augment, and diminish their perception of reality. One of the key anticipated use cases of XR technology, and particularly AR, is the facilitation of augmented intelligence (i.e., supplementing memories and enhancing cognition, driven by AI [4]) and augmented perception ([36],[37],[38]) (i.e., extending users sensorial range, amplifying their existing sensing, and overcoming impairments). In both cases, XR technology's sensing either supplements or extends users capabilities, for example being used to provide "superhearing" (e.g., enhancing the perceived contrast of audio [39], or more generally selectively enhancing and suppressing audio to improve speech perception [40]) or "supersight" (e.g., using head-mounted cameras as a magnification aid [41], visualizing out-of-view objects [10], or even changes in the environment over time [42]). As a consequence, these technologies offer significant benefits for overcoming situational, temporary, and permanent impairments—however, they also pose a significant security risk ([43],[44],[45]), potentially bestowing individuals with super-sensory capabilities and memories that could be used for personal surveillance e.g., supporting sophisticated "shoulder-surfing" type observation attacks [46].

Recommendation #9	Where there is a risk of infringing on the privacy of others, any augmented intelligence or perception application should require the consent of the sensed others or provide mechanics such that others in the environment are made aware of, or can automatically opt-out of, such activity.

Recommendation #10	Where there is a genuine need for powerful augmented perception approach that introduces a privacy concern (e.g., for accessibility reasons such as a situational, temporary, or permanent impairment), use of this capability should be sufficiently visible to bystanders that it cannot trivially be misused/abused

2.7. RIGHTS AND PROTECTIONS

If privacy alone is considered, XR-driven sensing opens up a Pandora's box of potential violations of privacy—from the perspective of individual users, bystanders, and society as a whole. It is pertinent at this point to consider what existing legal protections exist to prevent such violations from occurring. While this paper will discuss existing rights and areas where legislation goes some way toward safeguarding against the privacy concerns presented thus far, in summary: **the current system of digital privacy protection is no longer tenable in an extended reality world**. Laws are jurisdictional in nature and often do not apply in extended reality that can be borderless by nature. There must be a focus on defining harms within extended reality that result when personal digital privacy is breached.

2.7.1. EXISTING RIGHTS

XR technology introduces challenges to rights and protections for both end users of this technology, as well as those non-users whose personal data is potentially captured and processed by an XR user's device. In Europe the General Data Protection Regulation (GDPR) governs how personal data can be captured, stored, and processed, with a particular focus on special categories of personal data, such as biometric data (when used for identification) and data regarding racial or ethnic origin, health, sexual orientation, and political opinions. These data types are closely linked to enshrined freedoms such as freedom of thought, conscience and religion, and freedom from discrimination. GDPR also enshrines additional data rights for individuals, emphasizing data protection by design and by default; user access to captured data; the right to data portability; the right to be forgotten; and the right to know when there has been a data breach [47].

GDPR requires a “lawful basis” for processing personal data, typically by seeking consent, or determining “legitimate interest” in processing (i.e., assessing the balance between intent and an individual's interests). As such, many of the potential privacy violating activities suggested in this report are not ruled out by default by GDPR, but rather the activities would have to be justified through garnering user consent or building a legal case for the allowance of said activity. For example, consent may be a basis for usage if enabling some form of interaction (as Facebook suggested in considering facial identification [26]), or again legitimate interest would need to be established [48] with an emphasis on reducing the inherent privacy intrusion. By design, GDPR is a generic framework that must be applied and interpreted, balancing “the right to be seen versus the right to be recognized” [49]. Currently, there exists no interpretation of GDPR considering the breadth of challenges discussed herein. For example, it is uncertain how GDPR would hold up against careful application of biometric psychography or worldscraping approaches.

United State’s law is focused predominantly on personally identifiable information (PII) and biometric data, with no equivalent of the EU’s GDPR currently in place. While there are some common data protection regulations across states [e.g., the Health Insurance Portability and Accountability Act (HIPAA)], the burden of data protection has fallen largely to individual states to address [e.g., California’s Consumer Privacy Act (CCPA)]; these states in turn have been predominantly concerned with PII and biometric identifiers [16], rather than some of the more sophisticated processing activities outlined herein. For example, see “Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law” [16] for a discussion on the variations in state law in the U.S. regarding biometric data, which has been varyingly described with respect to user privacy as “a patchwork of national- and state-level legislation addressing various concerns” [7].

Around the world, privacy legislation has played catch-up with digital reality, with only a few countries having protections of similar scope and reach as GDPR [50]. For example, Brazil has legislation broadly equivalent to GDPR, in the form of Lei Geral de Proteçao de Dados (LGPD); Japan has the Act on Protection of Personal Information; South Korea’s Personal Information Protection Act has similar protections to GDPR in terms of requirements for consent; India’s Personal Data Protection Bill (PDPB) and South Africa’s Protection of Personal Information Act (POPIA) are both reportedly modeled after GDPR; and countries such as Switzerland and Canada are in the process of introducing equivalent legislation. Consequently, privacy protections in XR will vary significantly from country to country, and even the foremost protections such as GDPR remain largely untested with respect to the multitude of processing activities discussed thus far.

2.7.2. CONSENSUAL AND INDUCED EROSION OF RIGHTS

Critically, where there is a mechanism for consent for lawful processing of personal data, there exists the scope for consensual erosion of existing rights, effectively legal loopholes whereby access to/usage of an XR platform or application requires that the user agrees to terms of service or privacy policies that permit extensive capture and processing activities. While these would typically need to be justified, nonetheless users may find themselves willingly giving permission to capture and processing activities because of the perceived low cost to themselves (e.g., not appreciating the privacy implications, or receiving subsidized access to hardware, software, or virtual spaces or experiences such as the metaverse), balanced against the high perceived potential benefits (e.g., access to the latest AR headset and its associated augmented intelligence capabilities)—assuming that users even read the terms to which they are agreeing. In effect, companies will be aided in this activity by users eager to gain access to the latest XR experiences and hardware, who have become accustomed to blindly agreeing to conditions to use the latest digital technology. The tension here is in balancing a legitimate interest in the use of XR sensing against users (and bystanders) rights and freedoms.

2.7.3. NON-CONSENSUAL EROSION OR CIRCUMVENTION OF RIGHTS

Weighing heavily on this balance will be the capability of well-resourced technology companies to either lobby for changes or omissions in legislation or bend the interpretation of existing legislation in their favor immediately and address the consequences later (e.g., Facebook reportedly set aside €302 million for anticipated fines in the EU [51] and $650 million for fines in the U.S. in 2021). While such efforts may in fact be pro-consumer (e.g., legitimizing processing required for new functionality or capability, anticipating novel and emergent risks), they nonetheless open the possibility of abuse by those companies that are directing the future of XR technology.

While the main endeavor is to safeguard users from privacy and anonymity infringements, third parties will also inevitably attempt to circumvent such protections. User attitudes toward sharing their personal or captured data can be manipulated. Erickson [52] noted that the stated use of data can influence a user's decision to permit access (e.g., being used to ambiguously “improve the experience”)—a “dark pattern” [53], referring to exploitative approaches that aim to either trick users into actions, or exploit gaps in permissions and legislation to capture and process data toward an unintended end. XR technology may enable new forms of dark patterns, specifically in how they manipulate behavior. Gaps

in legislation can also be exploited to similar ends. For example, consider “creepy technology,” where there is no “breach of any of the recognized principles of privacy and data protection law. They include activity that is not exactly harmful; does not circumvent privacy settings; and does not exceed the purposes for which data were collected”—yet pushes the boundaries of social norms to an uncomfortable degree [54].

2.7.4. SUITABILITY OF EXISTING LEGISLATION

Where existing legislation may pertain to XR technology, there are also significant loopholes covering personal data and biometric psychography. For example, in many cases “these frameworks do not reflect the development of immersive technology when considering what features are available with hardware, how those features function, what information about users is available, and how that information could be used” [16]. At what point data is considered personally identifiable/biometric data, under what circumstances, and in what ways can this data be processed or computed from other sources, can play a significant role in whether or not an activity is covered by existing legislation. Future research will be needed to build upon existing efforts in this space, for example exploring privacy frameworks [55], contextual integrity [56], neuro-rights [25], and extensions to human rights [57]. Moreover, specific legislation will likely be needed to target privacy protections for public spaces and vulnerable groups such as children. In time, it is to be hoped that a global **Extended Reality Privacy Rights Framework** will be established. That considers, and protects against, digital harms resulting from the capability of XR-driven technology to instrument, process, and act upon people’s everyday actions, physiology, brain activity, behaviors, thoughts, and attitudes.

2.7.5. NON-LEGISLATIVE PROTECTIONS, AND THE NEED FOR TRANSPARENCY AND CONSENT

There are also a host of other routes by which pressure can be exerted to create safer, more privacy-respecting XR platforms and applications. As XR sees mass adoption, cultural norms will inevitably evolve around usage in practice, and how human usage might vary in different public or private contexts. Accordingly, society has a part to play in rejecting socially unacceptable or irresponsible use cases. Emergent ethical guidelines around XR technology [58] employing methodology such as participatory design [59] will help to steer public opinions and attitudes toward the need for stronger privacy protections. This, in turn, will influence the standards and codes of conduct that XR platforms propose or voluntarily choose to adopt around privacy concerns—standards that could be enforced on all

application software running on these platforms if they are adopted [10]. At a low level, the design of more granular sensor APIs can provide a route for preventing misuse of sensor data by XR applications and malicious parties [9]; incorporating stronger [60] data access protections (selective obfuscation [61], differential privacy [62], etc.); privacy-certification standards [63]; transparency, comprehension and consent into their very operation; keeping XR users and bystanders informed and in control as to how, and when, their personal sensed data is being used [63], [64].

Recommendation #11	XR Platforms need to adopt rigorous control over what sensor APIs applications can utilize, and how said data is protected from unintended or unanticipated processing. Where "risky" requests for access occur (e.g., requesting data that, in composite, could enable additional biometric processing), these risks should be mitigated against (e.g., informing users, denying access).

Recommendation #12	Users should be given the tools they need to retain agency over their device, its sensing activity, and client applications using this data. This includes requiring informed consent for risky sensor data and providing continual awareness and feedback regarding device activity.

Recommendation #13	Companies should strive to adopt leading guidelines regarding XR privacy protections and standards and enforce those standards on their app stores and platforms.

Recommendation #14	Industry, legislators, and researchers need to define an Extended Reality Privacy Rights Framework that can inform future legislation and provide voluntary standards for XR privacy protections as a stopgap.

Recommendation #15	Given there will be shortcomings in legislation and guidelines, the rights of victims of digital harms and privacy violations should also be addressed.

3. REFERENCES

The following list of sources either has been referenced within this paper or may be useful for additional reading:

[1] M. McGill, J. Williamson, A. Ng, F. Pollick, and S. Brewster, "Challenges in passenger use of mixed reality headsets in cars and other transportation," *Virtual Real.*, 2020, doi: 10.1007/s10055-019-00420-x.

[2] M. McGill, A. Kehoe, E. Freeman, and S. Brewster, "Expanding the Bounds of Seated Virtual Workspaces," *ACM Trans. Comput. Interact.*, 2020, doi: 10.1145/3380959.

[3] C. Handler Miller, *Digital Storytelling: A creator's Guide to Interactive Entertainment*. 2004.

[4] N. ning Zheng *et al.*, "Hybrid-augmented intelligence: collaboration and cognition," *Frontiers of Information Technology and Electronic Engineering*. 2017, doi: 10.1631/FITEE.1700053.

[5] S. Orts-Escolano *et al.*, "Holoportation: Virtual 3D teleportation in real-time," 2016, doi: 10.1145/2984511.2984517.

[6] M. Billinghurst, "Grand Challenges for Augmented Reality," *Front. Virtual Real.*, 2021, doi: 10.3389/frvir.2021.578080.

[7] E. Dick, "Balancing User Privacy and Innovation in Augmented and Virtual Reality," *Information Technology Innovation Foundation*, 2021.

[8] K. Bye, D. Hosfelt, S. Chase, M. Miesnieks, and T. Beck, "The ethical and privacy implications of mixed reality," 2019, doi: 10.1145/3306212.3328138.

[9] J. Buolamwini, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," *Proc. Mach. Learn. Res.*, 2018.

[10] U. Gruenefeld, A. El Ali, W. Heuten, and S. Boll, "Visualizing out-of-view objects in head-mounted augmented reality," 2017, doi: 10.1145/3098279.3122124.

[11] K. J. Emery, M. Zannoli, L. Xiao, J. Warren, and S. S. Talathi, "Estimating gaze from head and hand pose and scene images for open-ended exploration in VR Environments," 2021, doi: 10.1109/VRW52623.2021.00159.

[12] M. R. Miller, F. Herrera, H. Jun, J. A. Landay, and J. N. Bailenson, "Personal identifiability of user tracking data during observation of 360-degree VR video," *Sci. Rep.*, 2020, doi: 10.1038/s41598-020-74486-y.

[13] J. Liebers *et al.*, "Understanding User Identification in Virtual Reality Through Behavioral Biometrics and the Effect of Body Normalization," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–11.

[14] "When bodies become data: Biometric technologies and free expression.," *Article19.Org*. https://www.article19.org/biometric-technologies-privacy-data-free-expression/ (accessed Jul. 14, 2021).

[15] C. Dwork and A. Roth, *The Algorithmic Foundations of Differential Privacy*. 2013.

[16] B. Heller, "Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law," *Vand. J. Ent. Tech. L.*, vol. 23, p. 1, 2020.

[17] M. Ienca, “Do We Have a Right to Mental Privacy and Cognitive Liberty?,” *Sci. Am.*, 2017.

[18] G. Schalk, J. R. Wolpaw, D. J. McFarland, and G. Pfurtscheller, “EEG-based communication: Presence of an error potential,” *Clin. Neurophysiol.*, 2000, doi: 10.1016/S1388-2457(00)00457-0.

[19] H. Si-Mohammed *et al.*, “Detecting System Errors in Virtual Reality Using EEG Through Error-Related Potentials,” 2020, doi: 10.1109/VR46266.2020.1581262194646.

[20] S. Gannouni, A. Aledaily, K. Belwafi, and H. Aboalsamh, “Emotion detection using electroencephalography signals and a zero-time windowing-based epoch estimation and relevant electrode identification,” *Sci. Rep.*, 2021, doi: 10.1038/s41598-021-86345-5.

[21] J. L. Kröger, O. H. M. Lutz, and F. Müller, “What does your gaze reveal about you? on the privacy implications of eye tracking,” 2020, doi: 10.1007/978-3-030-42504-3_15.

[22] L. F. Barrett, R. Adolphs, S. Marsella, A. M. Martinez, and S. D. Pollak, “Emotional expressions reconsidered: Challenges to inferring emotion from human facial movements,” *Psychol. Sci. public Interes.*, vol. 20, no. 1, pp. 1–68, 2019.

[23] “Emotion Recognition Technology Report,” *ARTICLE 19.Org*. https://www.article19.org/emotion-recognition-technology-report/ (accessed Jul. 14, 2021).

[24] K. Crawford, “Artificial Intelligence Is Misreading Human Emotion - The Atlantic,” *The Atlantic*, 2021.

[25] R. Yuste, J. Genser, and S. Herrmann, “It’s Time for Neuro-Rights,” *Horizons*, 2021.

[26] T. Hardwick, “Facebook Weighing Up Legality of Facial Recognition in Upcoming Smart Glasses,” *Macrumors.Com*, 2021. https://www.macrumors.com/2021/02/27/facebook-facial-recognition-smart-glasses-legal/ (accessed Mar. 01, 2021).

[27] K. Lyons, “Judge approves $650 million Facebook privacy settlement over facial recognition feature,” *TheVerge.com*, 2021. https://www.theverge.com/2021/2/27/22304618/judge-approves-facebook-privacy-settlement-illinois-facial-recognition (accessed Mar. 01, 2021).

[28] J. Kranjec, S. Beguš, G. Geršak, and J. Drnovšek, “Non-contact heart rate and heart rate variability measurements: A review,” *Biomedical Signal Processing and Control*. 2014, doi: 10.1016/j.bspc.2014.03.004.

[29] R. Chatila and J. C. Havens, “The IEEE global initiative on ethics of autonomous and intelligent systems,” in *Intelligent Systems, Control and Automation: Science and Engineering*, 2019.

[30] K. R. and K. Opsahl, “Augmented Reality Must Have Augmented Privacy,” 2020. https://www.eff.org/deeplinks/2020/10/augmented-reality-must-have-augmented-privacy (accessed Feb. 11, 2021).

[31] G. Yadin, “Virtual Reality Surveillance,” *Cardozo Arts Entertain. Law J.*, 2017.

[32] Oculus, “Facebook Reality Labs: LiveMaps | Oculus Connect 6,” *YouTube.Com*, 2019. https://www.youtube.com/watch?v=JTa8zn0RNVM (accessed Feb. 18, 2021).

[33] A. Hon, “Digital Sight Management, and the Mystery of the Missing Amazon Receipts.,” *mssv.com*, 2020. https://mssv.net/2020/08/16/digital-sight-management-and-the-mystery-of-the-missing-amazon-receipts/ (accessed Feb. 11, 2021).

[34] Niantic, “Introducing the Niantic Planet-Scale AR Alliance: Bringing the Mobile Industry Together Towards the 5G Future of Consumer A,” *NianticLabs.com*, 2020. https://nianticlabs.com/en/blog/niantic-planet-scale-ar-alliance-5g/ (accessed Feb. 11, 2021).

[35] Niantic, “Welcoming 3D Spatial Mapping Leader 6D.ai to Niantic: Accelerating Real-World AR Innovation,” *NianticLabs.com*, 2020. https://nianticlabs.com/en/blog/6d/ (accessed Feb. 11, 2021).

[36] O. Hugues, P. Fuchs, and O. Nannipieri, “New Augmented Reality Taxonomy: Technologies and Features of Augmented Environment,” in *Handbook of Augmented Reality*, 2011.

[37] H. K. Schraffenberger, “Arguably augmented reality: relationships between the virtual and the real.” Leiden University, 2018.

[38] S. Ligthart, G. Meynen, N. Biller-Andorno, T. Kooijmans, and P. Kellmeyer, “Is Virtually Everything Possible? The Relevance of Ethics and Human Rights for Introducing Extended Reality in Forensic Psychiatry,” *AJOB Neurosci.*, 2021, doi: 10.1080/21507740.2021.1898489.

[39] M. Weger, T. Hermann, and R. Höldrich, “Real-time Auditory Contrast Enhancement,” 2019, doi: 10.21785/icad2019.026.

[40] “Hearables: Here come the: Technology tucked inside your ears will augment your daily life,” *IEEE Spectr.*, 2019, doi: 10.1109/MSPEC.2019.8701198.

[41] L. Stearns, L. Findlater, and J. E. Froehlich, “Design of an augmented reality magnification aid for low vision users,” 2018, doi: 10.1145/3234695.3236361.

[42] D. Lindlbauer and A. D. Wilson, “Remixed reality: Manipulating space and time in augmented Reality,” 2018, doi: 10.1145/3173574.3173703.

[43] J. A. D. E. Guzman, K. Thilakarathna, and A. Seneviratne, “Security and privacy approaches in mixed reality: A literature survey,” *ACM Computing Surveys*. 2019, doi: 10.1145/3359626.

[44] J. Happa, M. Glencross, and A. Steed, “Cyber security threats and challenges in collaborative mixed-reality,” *Front. ICT*, 2019, doi: 10.3389/fict.2019.00005.

[45] F. Roesner, T. O. Kohno, and D. Molnar, “Security and privacy for augmented reality systems,” *Commun. ACM*, 2014, doi: 10.1145/2580723.2580730.

[46] S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, “Design and evaluation of a shoulder-surfing resistant graphical password scheme,” 2006, doi: 10.1145/1133265.1133303.

[47] G. C. for Apps, “Privacy Policies,” *PrivacyPolicies.com*. https://www.privacypolicies.com/blog/gdpr-compliance-apps/ (accessed Jul. 14, 2021).

[48] H. Lovells, “International: Making facial recognition GDPR-compliant,” *DataGuidance.com*. https://www.dataguidance.com/opinion/international-making-facial-recognition-gdpr (accessed Mar. 01, 2021).

[49] C. Cuador, “From Street Photography to Face Recognition: Distinguishing Between the Right to Be Seen and the Right to Be Recognized,” *Nov. L. Rev.*, 2017.

[50] D. Simmons, “13 Countries with GDPR-like Data Privacy Laws,” *Insights.Comforte.com*. https://insights.comforte.com/13-countries-with-gdpr-like-data-privacy-laws (accessed Aug. 05, 2021).

[51] V. M. and M. Scott, “Facebook earmarks €302M for privacy fines,” *Politico.eu*, 2020. https://www.politico.eu/article/facebook-earmarks-e302m-for-privacy-fines/ (accessed Feb. 11, 2021).

[52] L. Erickson, “Exploring Digital Rights: Data Sovereignty in XR. Games for Change,” *YouTube.Com*, 2020. https://www.youtube.com/watch?v=H3tMiSzRHA0 (accessed Feb. 11, 2021).

[53] A. Mathur, M. Kshirsagar, and J. Mayer, “What Makes a Dark Pattern... Dark?,” 2021, doi:

10.1145/3411764.3445610.

[54] O. Tene and J. Polonetsky, “A Theory of Creepy: Technology, Privacy, and Shifting Social Norms,” *Yale J. Law Technol.*, 2014.

[55] A. Barth, A. Datta, J. C. Mitchell, and H. Nissenbaum, “Privacy and contextual integrity: Framework and applications,” 2006, doi: 10.1109/SP.2006.32.

[56] H. Nissenbaum, “Privacy as contextual integrity,” *Washington Law Review*. 2004.

[57] E. F. Foundation, “RightsCon: As AR/VR becomes a reality, it needs a human rights framework,” *EFF.com*, 2021. https://www.eff.org/event/rightscon-arvr-becomes-reality-it-needs-human-rights-framework (accessed Aug. 05, 2021).

[58] J. Lingane, “FPF Report: Mitigate the Privacy Risks of AR & VR Tech,” *FPF.org*, 2021. https://fpf.org/blog/fpf-report-outlines-opportunities-to-mitigate-the-privacy-risks-of-ar-vr-technologies/ (accessed Jun. 24, 2021).

[59] J. Slupska, S. D. Dawson Duckworth, L. Ma, and G. Neff, “Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity,” 2021, doi: 10.1145/3411763.3451731.

[60] E. Dick, “How to Address Privacy Questions Raised by the Expansion of Augmented Reality in Public Spaces,” *ITIF.org*, 2020. https://itif.org/publications/2020/12/14/how-address-privacy-questions-raised-expansion-augmented-reality-public (accessed Aug. 05, 2021).

[61] N. Richards and W. Hartzog, “Privacy’s Trust Gap: A Review,” *Yale LJ*, vol. 126, p. 1180, 2016.

[62] J. Steil, I. Hagestedt, M. X. Huang, and A. Bulling, “Privacy-aware eye tracking using differential privacy,” 2019, doi: 10.1145/3314111.3319915.

[63] J. Happa, A. Steed, and M. Glencross, “Privacy-certification standards for extended-reality devices and services,” 2021, doi: 10.1109/VRW52623.2021.00085.

[64] B. Heller, “Defining ‘Biometric Psychography’ to Fill Gaps in Privacy Law to Cover XR Data: Brittan Heller’s Human Rights Perspectives,” *Voices of VR*, 2021. https://voicesofvr.com/988-defining-biometric-psychography-to-fill-gaps-in-privacy-law-to-cover-xr-data-brittan-hellers-human-rights-perspectives (accessed Sep. 16, 2021).

RAISING THE WORLD'S STANDARDS

3 Park Avenue, New York, NY 10016-5997 USA http://standards.ieee.org

Tel.+1732-981-0060 Fax+1732-562-1571