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

Documents
Document Sharing Hub

Full document details: IEEE Extended reality (XR) and the erosion of anonymity and privacy 2021

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

Copyright © 2021 by The Institute of Electrical and Electronics Engineers, Inc.

All rights reserved. November 2021. Printed in the United States of America.

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

IEEE is a registered trademark in the U. S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated. All other trademarks are the property of the respective trademark owners.

IEEE prohibits discrimination, harassment, and bullying. For more information, visit http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html.

No part of this publication may be reproduced in any form, in an electronic retrieval system, or otherwise, without the prior written permission of the publisher.

Find IEEE standards and standards-related product listings at: http://standards.ieee.org.

Copyright © 2021 IEEE. All rights reserved.
AVA Documents Document Sharing Hub

Full document details: IEEE Extended reality (XR) and the erosion of anonymity and privacy 2021

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.

Copyright © 2021 IEEE. All rights reserved.
AVA Documents Document Sharing Hub

Full document details: IEEE Extended reality (XR) and the erosion of anonymity and privacy 2021

TABLE OF CONTENTS

ABSTRACT 5

1. INTRODUCTION 6

2. KEY ISSUES IN XR PRIVACY 7

- 2.1. XR Sensing and Computed Data 7
- 2.2. Identity and Anonymity of Self 8
- 2.3. Augmented Intelligence and Mental Privacy 9
- 2.4. Identity and Privacy of Bystanders 11
- 2.5. Worldscraping, "Live Maps" and Distributed Surveillance 13
- 2.6. Augmented Perception and Personal Surveillance 14
- 2.7. Rights and Protections 15
  - 2.7.1. Existing Rights 15
  - 2.7.2. Consensual and Induced Erosion of Rights 17
  - 2.7.3. Non-Consensual Erosion or Circumvention of Rights 17
  - 2.7.4. Suitability of Existing Legislation 18
  - 2.7.5. Non-Legislative Protections, and the need for Transparency and Consent 18

3. REFERENCES 20

Documents
Document Sharing Hub

Full document details: IEEE Extended reality (XR) and the erosion of anonymity and privacy 2021

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

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

Copyright © 2021 IEEE. All rights reserved.

AVA Documents Document Sharing Hub

Full document details: IEEE Extended reality (XR) and the erosion of anonymity and privacy 2021

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.

Copyright © 2021 IEEE. All rights reserved.
IEEE Documents Document Sharing Hub
Full document details: IEEE Extended reality (XR) and the erosion of anonymity and privacy 2021

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

Copyright © 2021 IEEE. All rights reserved.
AVA Documents Document Sharing Hub
Full document details: IEEE Extended reality (XR) and the erosion of anonymity and privacy 2021

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

Copyright © 2021 IEEE. All rights reserved.
AVA Documents Document Sharing Hub
Full document details: IEEE Extended reality (XR) and the erosion of anonymity and privacy 2021