Privacy-certification standards for extended-reality devices and services

Jassim Happa*
Royal Holloway, University of London

Anthony Steed
University College London

Mashhuda Glencross
University of Queensland

Abstract

In this position paper, we discuss the need for, and potential requirements for privacy certification standards for extended-reality devices and related services. We begin by presenting motivations, before discussing related efforts. We then review the issue of certification as a research problem and identify key requirements. Finally, we outline key recommendations for how these might feed into a grander roadmap for privacy and security research.

Index Terms: Privacy—Extended-Reality—Certification—

1 Introduction

Personal data has become a valuable commodity for tech companies in recent years. It is becoming increasingly challenging for data subjects (individuals whose data exist on digital systems) to understand how software and hardware services process their data, and trust that it is treated according to what has been consented. These challenges spans a wide range of devices such as phones, TVs, home assistants, smart energy monitors and many more devices and services.

The disconnect between understanding the myriad of ways in which devices operate and how applications collect data across developers, data subjects and legal teams means that the implementation or services may not sufficiently reflect the intentions of the developer, company or data subjects. There is likely to be nuanced data and processes that has not been captured suitably, simply because business models, policies and practices are decoupled from the implementation. Software and hardware bugs may also be present that result in data exposure for which there is means to protect data subjects.

As new software and hardware becomes available, in particular: Extended-Reality (XR) devices, we argue that it will be necessary to re-think what concepts such as privacy and trust are in this space, and what they can and should be. In the context of XR, it is possible to now collect a variety of new data types, including observed or inferred bio-metric data about users, real-scene information (and relate this to other data sources). Some examples of this type of data can include gait, eye or head movements, body appearance, domicile information, heart rate, inferred emotional states and potentially many more. Domicile data for instance, may include a record of household objects to build a psychological profile about individuals.

In order to improve trust and understanding between end-users, data subjects and companies, and ensure that personal data will be processed as expected, we postulate it is necessary to develop a privacy model that developers can adhere to regardless if their XR device or service. This could take the form of an XR privacy certification standard that developers comply with to improve security, privacy, and ethics in the products and platforms they build. The purpose of this paper is to investigate and outline what such an approach might look like. The key research question we explore in this paper is therefore: **What requirements ought to exist for a privacy-certification scheme of extended-reality devices and services?**

*e-mail: jassim.happa@rhul.ac.uk

2 Related Work

Applying for any type of certification is often voluntary, but companies are encouraged to demonstrate compliance to specific standards, either by regulators, collaborators or even competitors in the interest of a healthy industry. Compliance means that stakeholders have assurances that a company or product will behave according to specification and that the specification is in part guided by a reference (i.e. standard). To the best of our knowledge, there is no privacy certification standard that exists specific to XR devices and services, however, a significant body of work exists is moving in that direction. We outline key efforts towards establishing privacy in systems. ISO 27701 for instance is a standard for Privacy Information Management[1]. It is a privacy extension to ISO/IEC 27001 Information Security Management and ISO/IEC 27002 Security Controls, and provides guidance on the protection of privacy.

Privacy-by-design is a set of seven key principles aimed at respecting privacy in a system's design [2]. The *Privacy Management Reference Model* (PMRM) [3] is a methodology for understanding and analysing privacy policies and their privacy management requirements in defined use cases. The National Institute of Standards and Technology (NIST) [1] discuss the concepts of privacy engineering and risk management for federal systems and aims to establish the basis for a common vocabulary to better facilitate understanding and communication of privacy risk within federal systems. MITRE's Privacy Engineering Framework [7] outlines how privacy engineering activities map to stages of a system's engineering life cycle.

The XR Safety Initiative[2] is in process of establishing a standard approach to communicating any data/resource stewardship, policy-based, regulatory, contractual and financial obligations related to the access to and use of XR technologies. An important aspect of this is privacy.

Emami-Naeini et al. [4] interviewed a group of security and privacy experts, and have proposed as set of security and privacy labels for IoT devices. The purpose of this is to enable users to understand how their data will be used in a standardised form. A similar approach to communicating what privacy standards can apply to XR systems could be beneficial to XR users.

Happa et al. [6] make the assumption it is impossible to identify all ethical and legal issues that can emerge from IoT research, and propose that through aggressive peer-review of conceivable data processing and decision-making in novel technologies, it is possible to tackle ethical and legislative concerns proactively and reactively in more well-informed ways. Such a methodology could be applied within an XR privacy context as well.

Our previous work [5] outlined key cyber security challenges posed to Collaborative Mixed-Reality (CMR) systems, including threat detection and possible harms from actuated threats in mixed-reality systems. We use this work as well as the aforementioned work as a starting point for our research into proposing key requirements for XR privacy-certification standards.

3 Key Considerations for Research

When identifying key requirements for any XR privacy-certification scheme, several concerns may not be immediately apparent, partly because companies and users do not fully explore the scope of

[1] https://www.iso.org/standard/71670.html
[2] https://xrsi.org/

potential harm that may arise from XR privacy misuse prior to deployment. This is in part because most evidence is anecdotal, and very little has been demonstrated empirically and experimentally. Given the complexity of the amount, and types of personal data that can be collected or inferred, it is difficult for data subjects to be able to really give (fully) informed consent in order to use these devices and access associated services. From the perspective of certification standards, for XR devices and services, we believe there are at least six important issues that need consideration:

- **Keeping privacy and security a priority**. Data subjects, especially end-users need to trust that a company will prioritise privacy of the data subjects for which they retain data – ideally this is core to their business model. This includes ensuring that protection mechanisms (security) are suitably applied and updated to the needs of the data subject.
- **Acting with data subjects' best interests in mind**. Companies will behave both legally and ethically responsible when changing their usage licenses, products and services. This is challenging if data subject and company interests are diametrically opposed.
- **Ability to monitor/audit personal data within systems**. Developers and legal teams need to be able to properly capture (and secure) the full scope of how personal data trails can be used.
- **Lack of transparency in first party system**. Data processing is opaque to data subjects, making it difficult to have confidence in that technology companies have their users best interests at heart.
- **Ability to understand how personal data can interact with third-party systems**. Devices and services may be provided by different companies, and can be misused by third-party actors.
- **Disconnect between legal documents and implementation**. Usage policy documents are written by legal teams, and not developers whose understanding of a systems is likely to be detached from the actual implementation.

End users rely on privacy polices in end-user licence agreements to use most devices or services and most people cannot (or have the time to) study, disassemble and monitor how their devices or services process their data. In fact, they often have to blindly trust that their devices and service providers will act according to the polices specified. In terms of trust, users may initially trust device and service providers, however usage licenses change and companies can choose to change they way in which they monetise the data and data trails they collect. They may also not fully understand the scope of the system in play, and thus make a well-informed decision w.r.t. consent. One scenario that is problematic is the inevitable "multi-app future"[3], in which users may wish to bring in their own apps (e.g. own virtual camera, virtual applications, etc.) into someone else's "environment". Driver chains for instance can be beneficial for accessibility, but unmoderated and insecure systems can be compromised by particularly motivated adversaries. Finally, there is also the usual problem of certification of applications, specifically graphics drivers (which are fragile), and overlaying apps (similar to smartphone phone grabbing permissions), present their own sets of security concerns.

4 Key Requirements for a Roadmap

Below follows some initial suggestions for requirements to feed into a roadmap. We believe this list should be considered a starting point, rather than an exhaustive list:

- **Vocabulary**. A vocabulary to meaningfully communicate information about data subjects, their data and stakeholders may become necessary. For XR devices and services, we argue that it will be necessary to re-define privacy threats and concerns, with XR devices and services in mind. Such a system will require a much wider view of social and technical harms and how to protect users from those harms.
- **Establishment of an interdisciplinary consortium** in order to exhaustively capture, categorise and discuss privacy threats in XR.
- **Tools to forensically examine cyber attacks specific to XR devices and services**. This may be achieved using a shared, peer-reviewed unified framework that can interface with a wide array of XR devices and services. Security analysts make use of technology-centric solutions to detect and combat threats posed to digital infrastructures. Present day Intrusion Detection and Prevention Systems (IDS/IPS) for instance aim to identify and limit misuse or anomalies from actuating into real-world harms. These systems have not been built with XR needs in mind. While, technology-centric tools will always remain important, no existing system is able to capture, take into account, mitigate or respond to social-level harms such as reputation, identify theft or mental health. We believe socio-technical threat detection systems will likely become vital in the future of XR.
- **Establish practices to identify and mitigate third-party misuse**. Any auditing tools, ought to also be able to monitor for misuse by trusted third parties. To what degree should these be available to all stakeholders remains an open question, but we suspect that any secure system should also allow, encourage and empower all parties to try and find misuse of their data using open-source and easy to use tools.
- **Development of privacy benchmarks to be met in order to be certified**. When monitoring for tampering, leaks or other attacks – an XR device attestation method or external auditing tool could output logs to e.g. an JSON schema format, either for research settings or production environments. We might be able to answer questions like: does the XR device meet a benchmark we have specified – if yes, this will be because we have the empirical or experimental evidence to demonstrate that.

5 Conclusion

We believe that a special interest group ought to be established to further refine privacy requirements for XR devices and services, and propose recommendations for a privacy certification scheme, particularly exploring how one might be implemented, whether tiers (of compliance) could exist for privacy models, which may lead to a formal specification, which can be met and tested by companies and data subjects.

[3] https://www.khronos.org/news/permalink/multi-app-the-next-evolution-in-spatial-computing

References

[1] S. Brooks, S. Brooks, M. Garcia, N. Lefkovitz, S. Lightman, and E. Nadeau. *An Introduction to Privacy Engineering and Risk Management in Federal Systems*. US Department of Commerce, National Institute of Standards and Technology, 2017.

[2] A. Cavoukian. Privacy by design. 7 foundational principles. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf, 2011.

[3] A. Cavoukian, D. Jutla, F. Carter, J. Sabo, F. Dawson, J. Fox, T. Finneran, and S. Fieten. Privacy by design documentation for software engineers version 1.0. *(PbD-SE) Burlington, MA: Organization for the Advancement of Structured Information Standards (OASIS)*, 2014.

[4] P. Emami-Naeini, Y. Agarwal, L. F. Cranor, and H. Hibshi. Ask the experts: What should be on an iot privacy and security label? In *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 447–464. IEEE, 2020.

[5] J. Happa, M. Glencross, and A. Steed. Cyber Security Threats and Challenges in Collaborative Mixed-Reality. *Frontiers in ICT*, 6, 2019.

[6] J. Happa, J. R. Nurse, M. Goldsmith, S. Creese, and R. Williams. An ethics framework for research into heterogeneous systems. 2018.

[7] S. Shapiro, N. Washington, K. Miller, J. Snyder, and J. McEwen. MITRE privacy engineering framework. MITRE Corporation Technical Report, 2014.