Safeguarding Privacy in the Age of Everyday XR

PEJMAN SAEGHE, MARK MCGILL, and MOHAMED KHAMIS, University of Glasgow, UK

ACM Reference Format:
Pejman Saeghe, Mark McGill, and Mohamed Khamis. 2022. Safeguarding Privacy in the Age of Everyday XR. 1, 1 (March 2022), 4 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

As augmented, mixed, and virtual reality technologies and devices—together, typically referred to as extended reality (XR)—tend towards everyday form factors, commentators are conceptualising a future where, for instance, "we won't be able to opt out from wearing AR glasses in 2035 any more than we can opt out of owning smartphones today." [3] While XR technology has the capacity to revolutionise personal computing—heralding new capabilities in augmented intelligence [20] and perception [5, 15, 16], telepresence [1], productivity [9], accessibility [10] and entertainment [13, 14, 19]—it also introduces significant privacy risks [2, 7].

In this position paper, we discuss the rational behind our recently funded award from the UK's National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (REPHRAIN), that sets out to explore:

(1) the ways in which XR technology can have an adverse effect on the users' and bystanders' privacy, and
(2) the ways in which such adverse effects could be mitigated, for instance, by raising users' and bystanders' awareness and providing practical mechanisms for consent.

Furthermore, by constraining our exploration to a regonised privacy taxonomy (i.e., Solove's [2005] taxonomy of privacy) we aim to emphasise novel issues surrounding everyday XR.

2 PRIVACY IN THE AGE OF EVERYDAY XR

In 2005 Solove recognised that "privacy [was] a concept in disarray" [18]. To address the new types of harm introduced by novel technologies, Solove developed a taxonomy of privacy by identifying and organising a set of related harmful activities that impinge on people in related ways. Considering an individual who is most directly affected by harmful activities—the data subject—as the centre of the conceptual model, Solove suggested four categories: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion.

While the principles that underpin Solove's [2005] taxonomy of privacy remain relevant today, the technological landscape has progressed considerably since 2005; suggesting there may be a need for an update in the taxonomy to capture novel risks and harms introduced by novel technologies, such as everyday XR. For instance, when considering information collection, new types of (contextual) data can be collected using state-of-the-art XR headsets' sensors (e.g., via wide angle depth/LiDAR-type sensing that enables the sensing of the data subject's environment, body and

Authors' address: Pejman Saeghe; Mark McGill; Mohamed Khamis, University of Glasgow, Glasgow, UK.

Manuscript submitted to ACM

actions [11, 12, 17], including information regarding the presence and actions of others in the vicinity of the data subject [6, 8]). Furthermore, the amount of data collected about an individual is likely on a scale that was previously unimaginable. Similarly, when considering information processing, the types of processing enabled by emerging computing paradigms (e.g., machine learning and artificial intelligence), and the speed with which the processing can take place, will likely exacerbate privacy challenges.

It is only logical then to assume, given the types and amount of data collection and processing enabled in the context of everyday XR, the types and the severity of the invasion towards individuals will likely be on a much larger scale with higher impact on the individual and consequently on the society as a whole.

We present three specific instances where Solove's [2005] taxonomy may need updating.

2.1 Privacy in public spaces

Historically, there has been a contrast in how public and private spaces are treated with regards to privacy. For instance, in the legal context, typically an individual only has *reasonable expectation of privacy* in a private space. In other words, there is no reasonable expectation of privacy in a public space [18].

This interpretation of privacy may have been sufficient in the past, where individuals did not have easy access to surveillance devices. However, given the sensing capabilities of everyday XR, users will be equipped with state-of-the-art sensors enabling them to record others, continuously and persistently in public spaces. This raises legal challenges that need to be addressed to safeguard the privacy of an individual in a public space.

2.2 Users *vs.* bystanders *vs.* passersby

While Solove's [2005] conceptual model captures important aspects of an individual's privacy, it fails to distinguish between various potential roles of the individual. This is particularly relevant in the context of everyday XR, where a different protocol—for data collection, processing, and dissemination—may be required, based on whether the individual is the primary user of a given XR device—with some degree of access to the device's sensors—a bystander, who may be to some degree engaged with and aware of the XR activities of the user—or a passerby, with potentially no knowledge of XR-related activities. Even in a scenario where a majority adopt everyday XR (e.g., [3]), there will remain a percentage of the population without access to such a technology (either by choice or e.g., because they are unable to afford it). This likely causes a gap in recording/surveillance capabilities of individuals. Furthermore, even a user of everyday XR will play the role of a bystander or a passerby in relation to another person's everyday XR equipment.

Given that use-cases of everyday XR likely involve wearing them in public spaces, the way in which consent regarding information collection, processing, and dissemination is negotiated, between a device user and their bystanders and passersby raises novel challenges.

2.3 Information dissemination with everyday XR

While dissemination of information, as described by [18], captures harmful activities regarding "the spreading or transfer of personal data or the threat to do so", the unique ways in which everyday XR can facilitate this is missing. For instance, while *distortion* generally consists of disseminating false or misleading information about individuals, in the context of everyday XR, distortion can consist of visually distorting an individual's facial and physical features, for instance using augmented reality, or diminished reality.

3 SAFELY UNLOCKING THE BENEFITS OF XR

Given the potential positive impact that XR can have on the individual and on the society, if privacy risks are identified and addressed early on, we propose two avenues to harden XR technology against violations of privacy:

(1) **Supporting resistance against surveillance and misuse** – bringing transparency and accountability to the use of XR sensing, and making it harder for applications to knowingly or unknowingly abuse XR's capacity for surveillance. To do this, we propose exploring novel XR sensing API architectures that facilitate both enhanced data access protections, and increased user awareness regarding how, when, and to what purpose personal sensing is being used.

(2) **Facilitating bystander awareness and consent** – We propose examining the ways in which bystanders' awareness can be raised regarding the activities of nearby XR headsets that result in bystanders' data being collected and processed. We further, propose exploring practical mechanisms by which bystanders can grant or deny consent to said activity.

In this project, our aim is to identify potential privacy risks introduced by everyday XR and to explore the ways in which these problems can be addressed before mass adoption takes place. We argue that by not identifying and addressing the privacy problems unique to XR devices, we run the risk of facilitating mis-use and abuse e.g., bestowing super sensory capabilities upon malicious actors and harming the security and privacy of individuals; which could lead once more towards societal rejection of this powerful technology [4].

ACKNOWLEDGMENTS

This paper was produced as part of *PriXR*, supported by REPHRAIN: The National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online, under UKRI grant: EP/V011189/1.

REFERENCES

[1] Artanim. 2020. *Creating an Interactive VR Experience with the VRTogether platform.* Retrieved February , 2022 from https://vrtogether.eu/2020/11/18/creating-an-interactive-vr-experience-with-the-vrtogether-platform/

[2] Raja Chatila and John C Havens. 2019. The IEEE global initiative on ethics of autonomous and intelligent systems. In *Robotics and well-being*. Springer, 11–16.

[3] Adrian Hon. 2020. *Digital Sight Management, and the Mystery of the Missing Amazon Receipts.* Retrieved February 18, 2022 from https://mssv.net/2020/08/16/digital-sight-management-and-the-mystery-of-the-missing-amazon-receipts/

[4] Matt Honan. 2013. *I, Glasshole: My Year With Google Glass.* Retrieved February 19, 2022 from https://www.wired.com/2013/12/glasshole/

[5] Olivier Hugues, Philippe Fuchs, and Olivier Nannipieri. 2011. New augmented reality taxonomy: Technologies and features of augmented environment. In *Handbook of augmented reality*. Springer, 47–63.

[6] David Lindlbauer and Andy D. Wilson. 2018. *Remixed Reality: Manipulating Space and Time in Augmented Reality.* Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3173703

[7] Mark McGill. 2021. The IEEE Global Initiative on Ethics of Extended Reality (XR) Report–Extended Reality (XR) and the Erosion of Anonymity and Privacy. *Extended Reality (XR) and the Erosion of Anonymity and Privacy - White Paper* (2021), 1–24. https://ieeexplore.ieee.org/document/9619999

[8] Mark McGill, Daniel Boland, Roderick Murray-Smith, and Stephen Brewster. 2015. A Dose of Reality: Overcoming Usability Challenges in VR Head-Mounted Displays. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 2143–2152. https://doi.org/10.1145/2702123.2702382

[9] Mark Mcgill, Aidan Kehoe, Euan Freeman, and Stephen Brewster. 2020. Expanding the Bounds of Seated Virtual Workspaces. *ACM Trans. Comput.-Hum. Interact.* 27, 3, Article 13 (may 2020), 40 pages. https://doi.org/10.1145/3380959

[10] Mark McGill, Florian Mathis, Mohamed Khamis, and Julie Williamson. 2020. Augmenting TV Viewing Using Acoustically Transparent Auditory Headsets. In *ACM International Conference on Interactive Media Experiences* (Cornella, Barcelona, Spain) *(IMX '20)*. Association for Computing Machinery, New York, NY, USA, 34–44. https://doi.org/10.1145/3391614.3393650

[11] Ken Pfeuffer, Matthias J. Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300340

[12] Thammathip Piumsomboon, Gun Lee, Robert W. Lindeman, and Mark Billinghurst. 2017. Exploring natural eye-gaze-based interaction for immersive virtual reality. In *2017 IEEE Symposium on 3D User Interfaces (3DUI)*. 36–39. https://doi.org/10.1109/3DUI.2017.7893315

[13] Pejman Saeghe, Gavin Abercrombie, Bruce Weir, Sarah Clinch, Stephen Pettifer, and Robert Stevens. 2020. Augmented reality and television: Dimensions and themes. In *ACM International Conference on Interactive Media Experiences*. 13–23.

[14] Pejman Saeghe, Sarah Clinch, Bruce Weir, Maxine Glancy, Vinoba Vinayagamoorthy, Ollie Pattinson, Stephen Robert Pettifer, and Robert Stevens. 2019. Augmenting Television With Augmented Reality. In *Proceedings of the 2019 ACM International Conference on Interactive Experiences for TV and Online Video*. 255–261.

[15] Hanna Schraffenberger and Edwin Van der Heide. 2014. Everything augmented: On the real in augmented reality. *Journal of Science and Technology of the Arts* 6, 1 (2014), 17–29.

[16] Hanna Kathrin Schraffenberger. 2018. *Arguably augmented reality: relationships between the virtual and the real.* Ph. D. Dissertation. Leiden University.

[17] Toby Sharp, Cem Keskin, Duncan Robertson, Jonathan Taylor, Jamie Shotton, David Kim, Christoph Rhemann, Ido Leichter, Alon Vinnikov, Yichen Wei, Daniel Freedman, Pushmeet Kohli, Eyal Krupka, Andrew Fitzgibbon, and Shahram Izadi. 2015. Accurate, Robust, and Flexible Real-Time Hand Tracking. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 3633–3642. https://doi.org/10.1145/2702123.2702179

[18] Daniel J Solove. 2005. A taxonomy of privacy. *U. Pa. l. Rev.* 154 (2005), 477.

[19] Radu-Daniel Vatavu, Pejman Saeghe, Teresa Chambel, Vinoba Vinayagamoorthy, and Marian F Ursu. 2020. Conceptualizing augmented reality television for the living room. In *ACM International Conference on Interactive Media Experiences*. 1–12.

[20] Nan-ning Zheng, Zi-yi Liu, Peng-ju Ren, Yong-qiang Ma, Shi-tao Chen, Si-yu Yu, Jian-ru Xue, Ba-dong Chen, and Fei-yue Wang. 2017. Hybrid-augmented intelligence: collaboration and cognition. *Frontiers of Information Technology & Electronic Engineering* 18, 2 (2017), 153–179.