Privacy, Security, and UX Challenges in (Social) XR: An overview

Katrien De Moor

Norwegian University of Science and Technology

Special thanks to **Camille Sivelle**

8th of April, 2025

NORCICS

SFI Norwegian Centre for Cybersecurity in Critical Sectors

NTNU

Norwegian Centre for Research-based Innovation

Briefly about me

Background: PhD from Ghent University, Communication Science

Associate professor at NTNU, Trondheim

Co-Editor-in-Chief of *Quality and User Experience* (Springer)

Key interests: human-technology experiences, human-centered design and evaluation, QoE and UX, methodological and ethical implications, human-centered cybersecurity

Outline

Scope (and disclaimer)

Privacy and data collection challenges

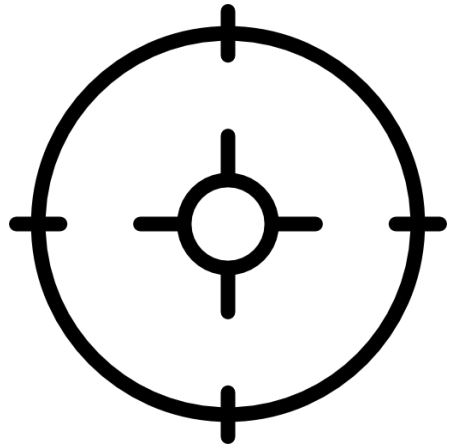
Security challenges

UX Challenges

Short case-study

Concluding thoughts

Illustrations credits: Flaticon



Scope (and disclaimer)

Illustrations credits: Flaticon

Reality-Virtuality Continuum

Real Environment (RE) — Virtual Environment (VE)

AR
AUGMENTED REALITY

Digital content from virtual world on top of real environment providing information

MR
MIXED REALITY

Real and virtual environment mix and interact with each other

VR
VIRTUAL REALITY

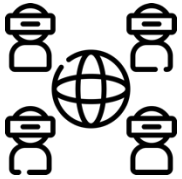
Immersive virtual environments shut out the real world

Source: https://www.dhl.com/us-en/home/innovation-in-logistics/logistics-trend-radar/augmented-and-extended-reality.html - based on Milgram and Colquhoun Jr, 1999).

Entertainment, gaming

....

Health and wellbeing



Marketing, Communication

increasing adoption of XR in range of sectors

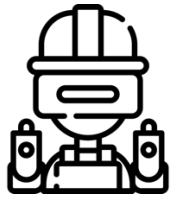
....

Military; emergency response and preparedness

....

Education

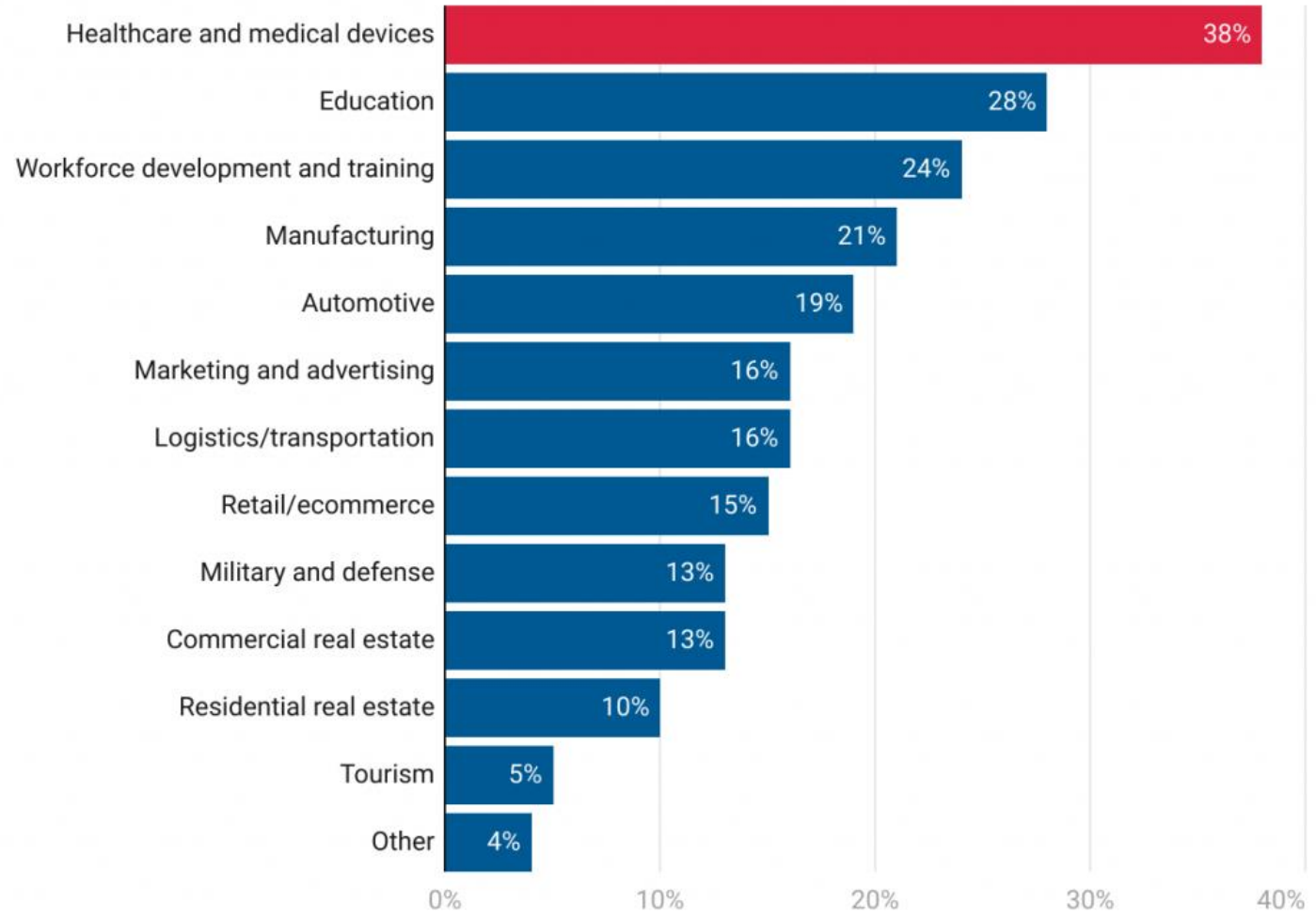
Industry; remote maintenance; manufacturing



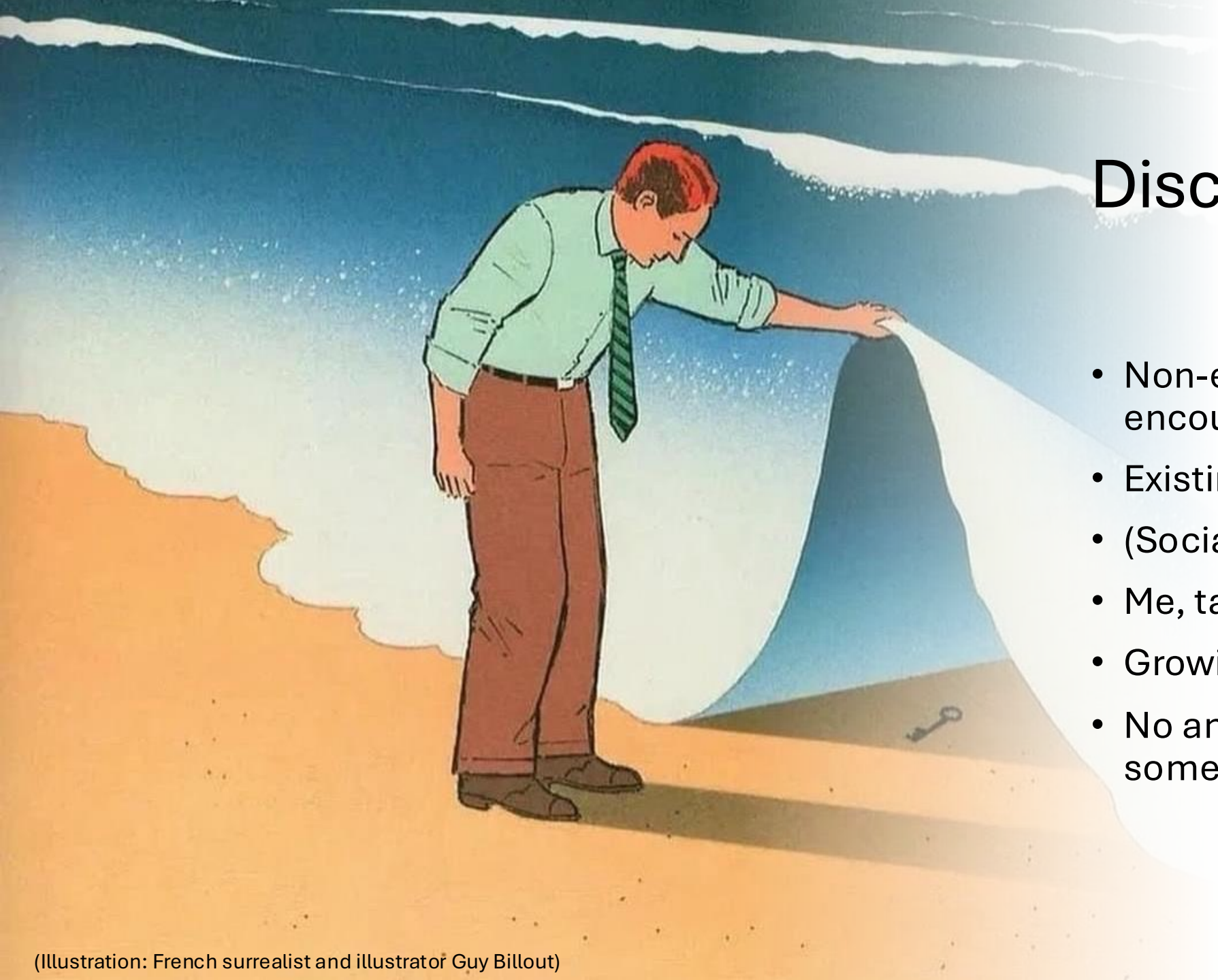
Illustrations credits: Flaticon

Industries Expected to Face the Most Disruption by Immersive Technologies

Besides Gaming and Entertainment



Source: Perkins Coie, 2020 Survey on AR/VR technology



Disclaimer

- Non-exhaustive overview (rather encouraging to explore further)
- Existing literature
- (Social) XR
- Me, talking about S&P?!
- Growing tensions
- No answers/the key; but maybe some food for thought

(Illustration: French surrealist and illustrator Guy Billout)

Privacy and data collection challenges in (social) XR

Illustrations credits: Flaticon

Or go to menti.com
Code: **8284 0995**

Self-representation and digital identity

A

B

C

Various **digital self-representation** possibilities, e.g.,

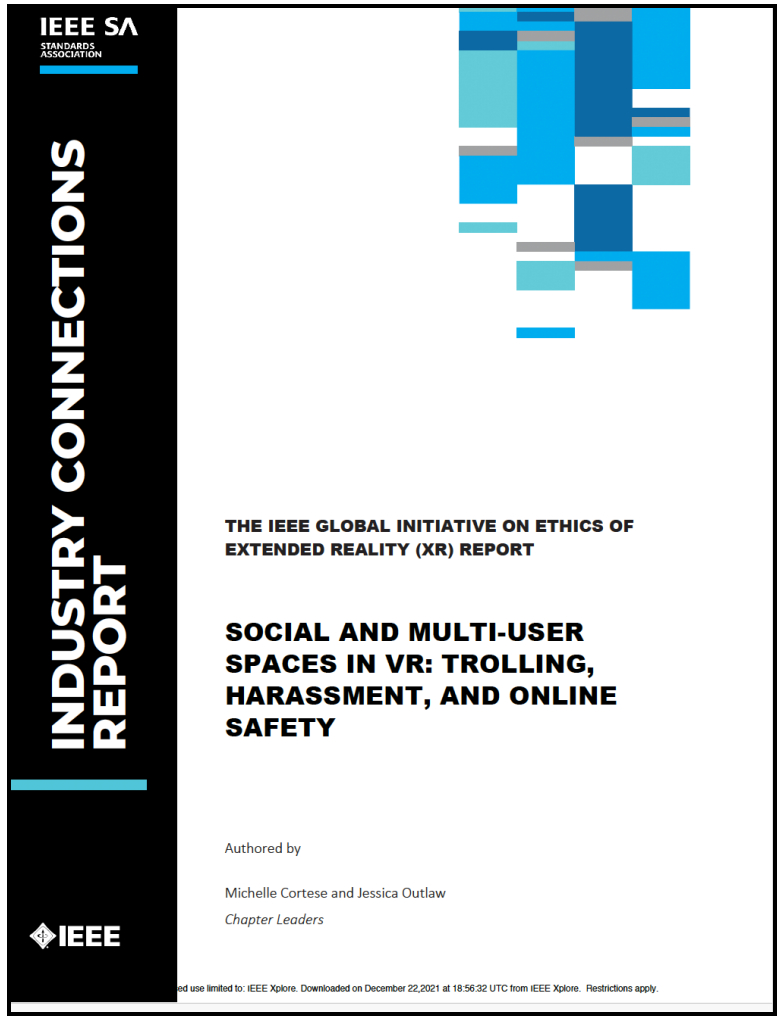
- Select or upload
- Customized avatars
- Photorealistic avatars (“superrealism”)

“**Digital bodies**” and interpersonal interaction

- Authenticity, naturalness, trustworthiness
- Social XR: stronger identification with digital body

Lin and Latoschik (2022). Digital body, identity and privacy in social virtual reality: A systematic review. Frontiers in Virtual Reality. Vol 3., 2022.

Digital identity management in XR



- Violence, harassment, racism, …
- Digital body modification
- Identity theft / hacking, identity misappropriation, …
- Ethical challenges and social norms
- Legal implications

https://standards.ieee.org/wp-content/uploads/import/governance/iccom/social-multi-user-spaces-vr.pdf
Lin and Latoschik (2022). Digital body, identity and privacy in social virtual reality: A systematic review. Frontiers in Virtual Reality.

Illustrations credits: Flaticon

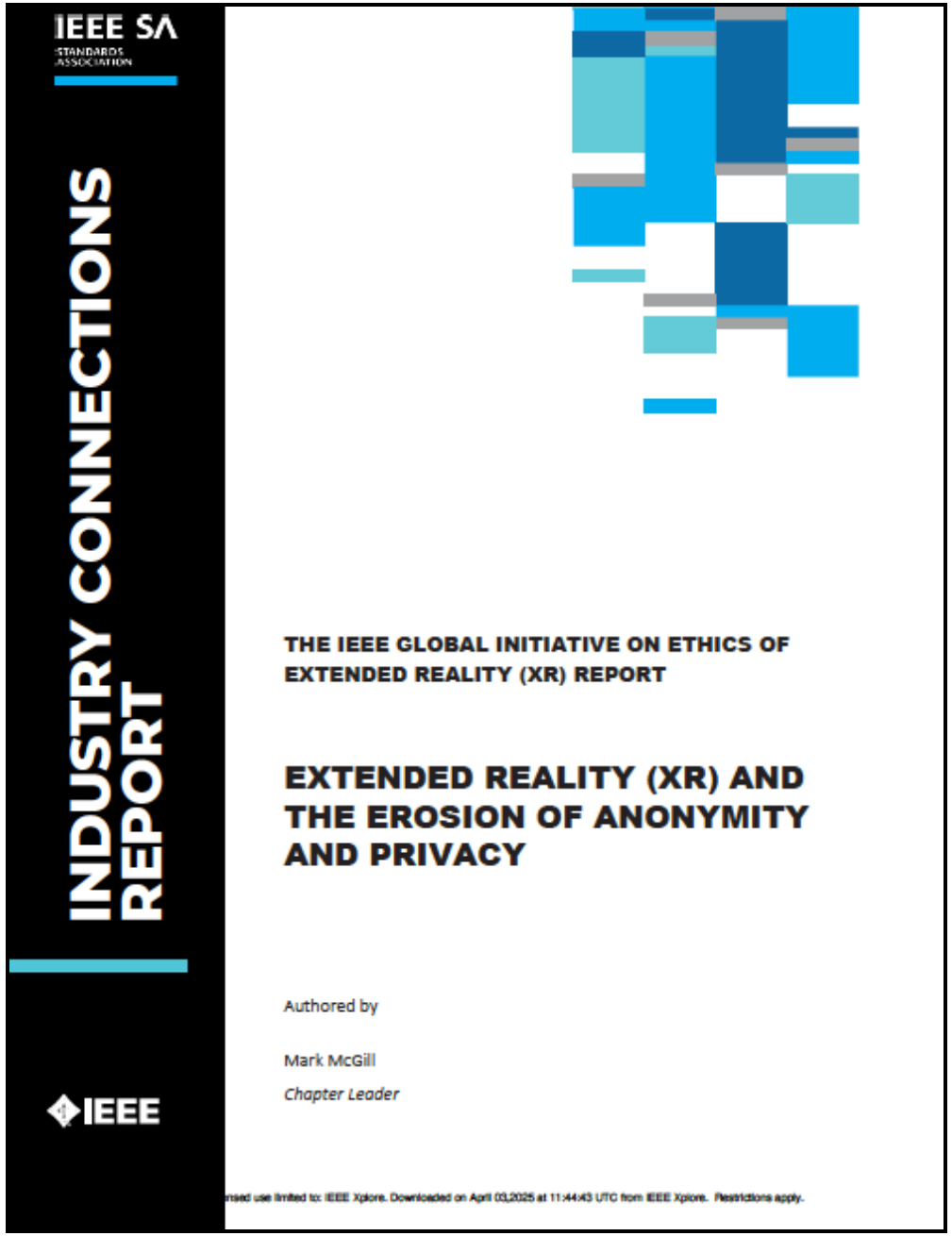
*"**Existing privacy regulations** that address virtual or real-world privacy issues **fail to adequately address the convergence of realities that exists in XR"*** (Pahi & Schroeder, 2022).

Pahi, S. and Schroeder, C. (2023). Extended Privacy for Extended Reality: XR Technology Has 99 Problems and Privacy is Several of Them. 4 Notre Dame J. Emerging Tech.

"*The desire to* ***maintain human rights to privacy*** *and* ***anonymity***

vs.

the ***potential*** *consensual or induced* ***erosion of these rights in the haste to take advantage of the benefits*** *these technologies offer to everyday life*"



https://standards.ieee.org/wp-content/uploads/import/governance/iccom/extended-reality-anonymity-privacy.pdf

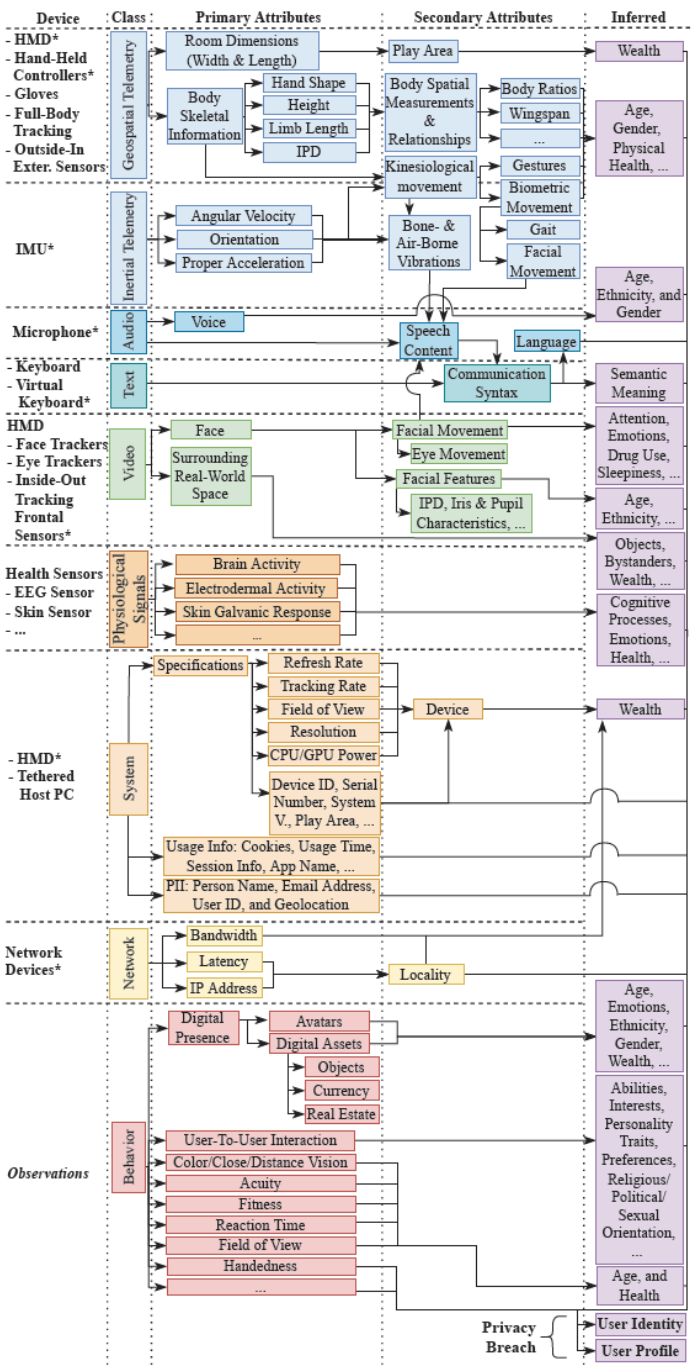


Figure 2: Taxonomy of VR data attributes. * Primary devices.

Inferred information:

- wealth
- age
- health
- gender
- ethnicity
- attention
- affective state
- medication use
- attention
- bystanders
- ...

Garrido GM, Nair V, Song D. SoK: Data Privacy in Virtual Reality. Proceedings on Privacy Enhancing Technologies. 2024.

Illustrations credits: Flaticon

Privacy breaches and types of attacks

User identity

- HMDs
- Hand-held controllers

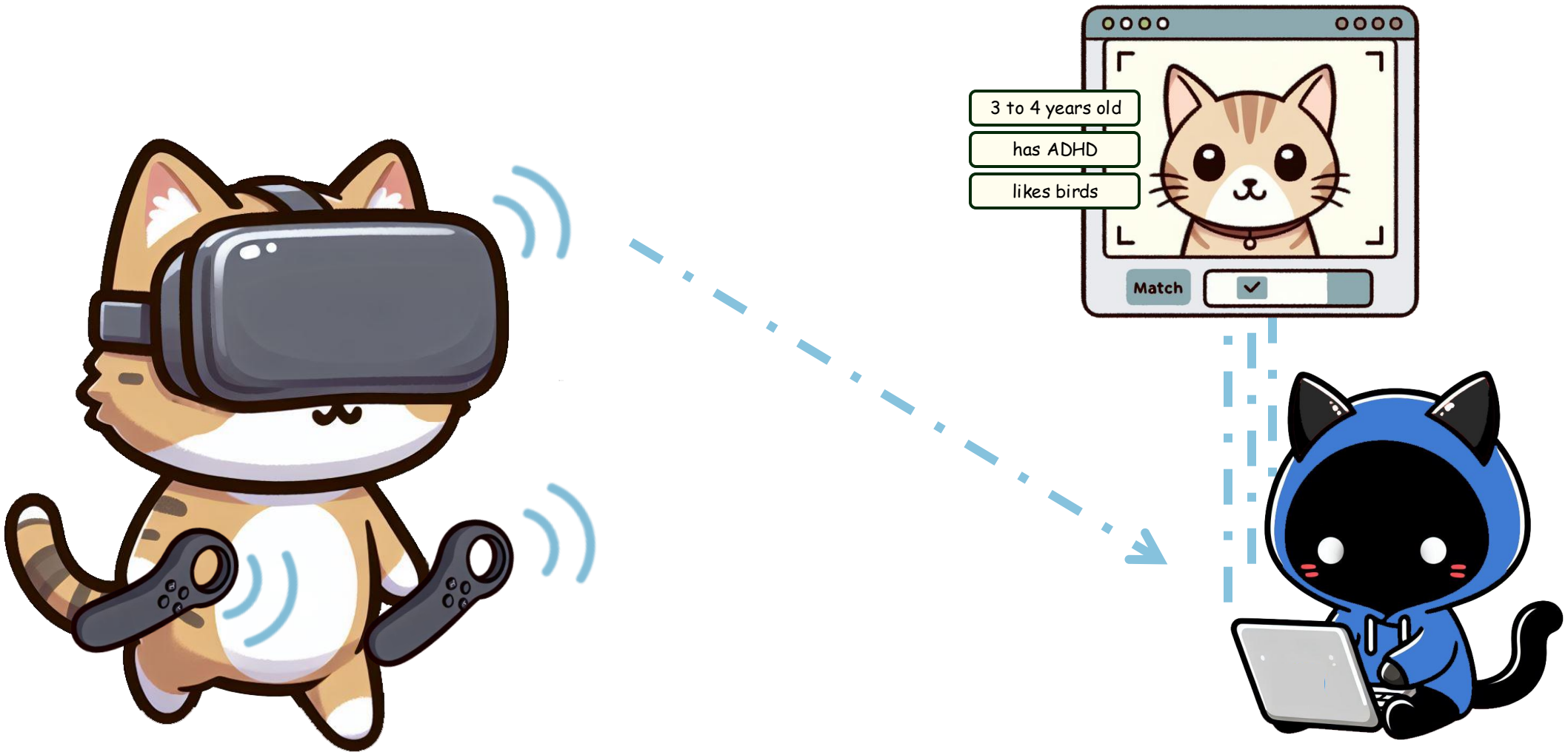
User profile

- Health sensors
- Direct vs. indirect leakages

Different countermeasures

Garrido GM, Nair V, Song D. SoK: Data Privacy in Virtual Reality. Proceedings on Privacy Enhancing Technologies. 2024.

Illustrations credits: Flaticon

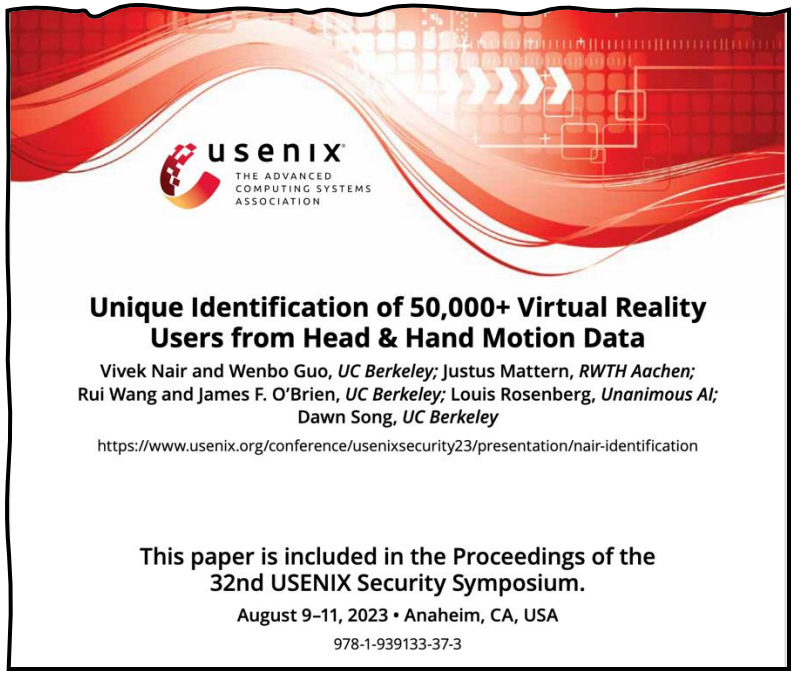


Icons generated with Microsoft CoPilot by Camille Sivelle

- **Key Finding:** Users (N=55 541 real users) can be uniquely identified with 94.33% accuracy using 100 seconds of motion data from XR devices (after training a classification model on 5 min/person)
- **Data Collected:** From sensors tracking head and hand movements in VR
- **Game:** Beat Saber (VR rhythm game)

Implications for Privacy:

- Motion patterns are as unique as fingerprints, posing serious risks if misused
- XR platforms can expose users to unauthorized tracking or profiling


usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data

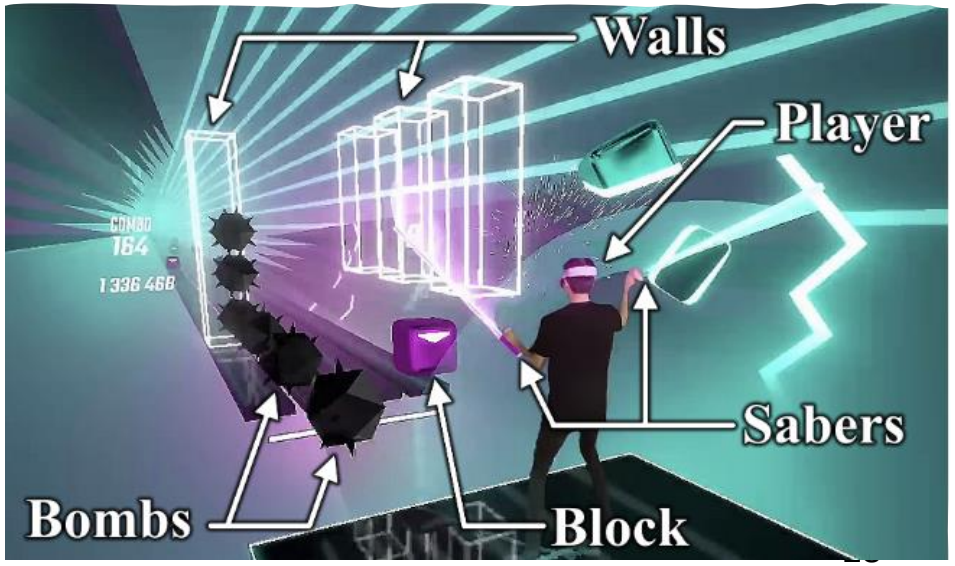
Vivek Nair and Wenbo Guo, *UC Berkeley;* Justus Mattern, *RWTH Aachen;* Rui Wang and James F. O'Brien, *UC Berkeley;* Louis Rosenberg, *Unanimous AI;* Dawn Song, *UC Berkeley*

https://www.usenix.org/conference/usenixsecurity23/presentation/nair-identification

This paper is included in the Proceedings of the 32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3



V. Nair et al., 32nd USENIX Conference on Security Symposium, 2023. "Unique identification of 50,000+ virtual reality users from head & hand motion data"

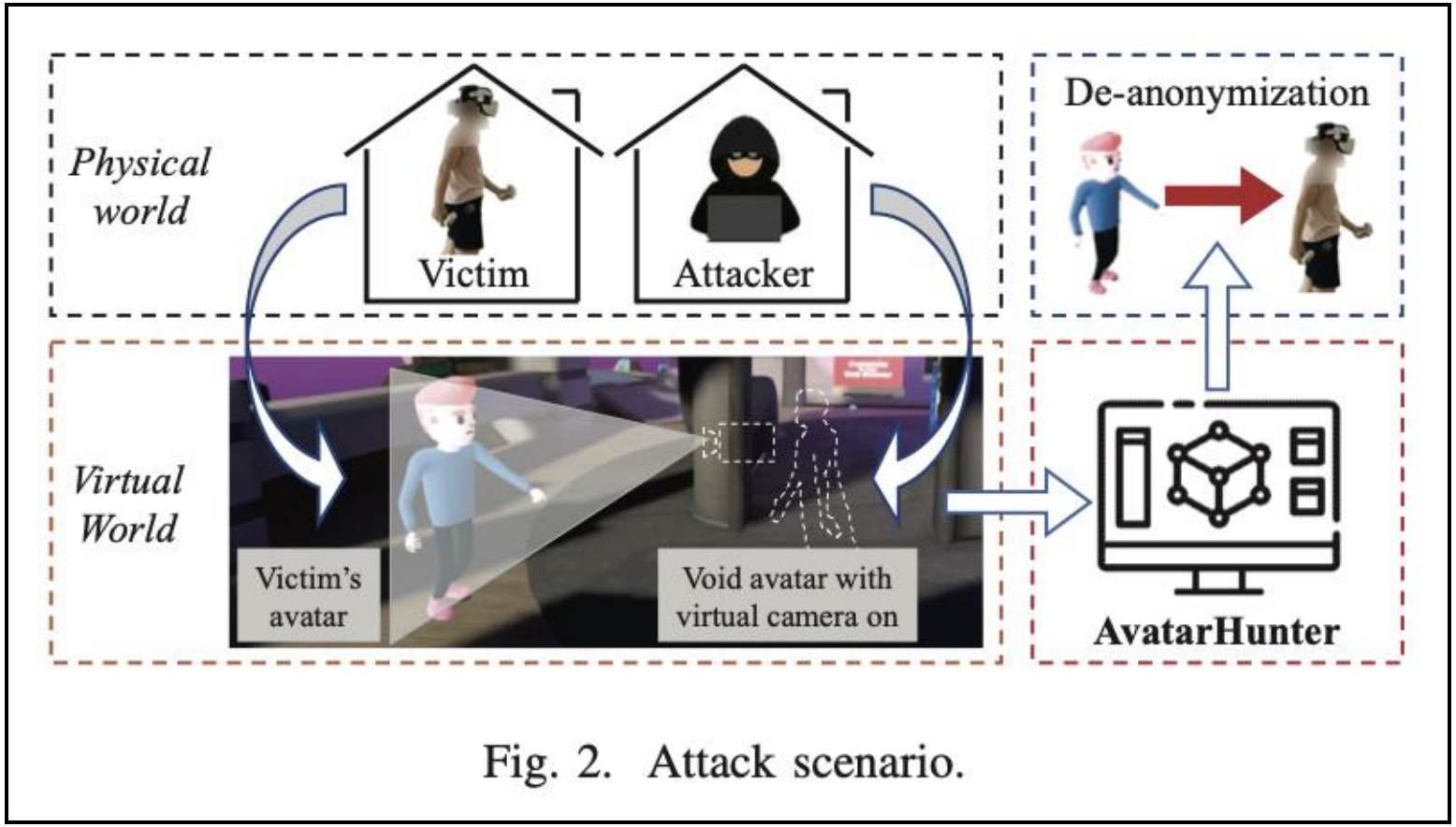
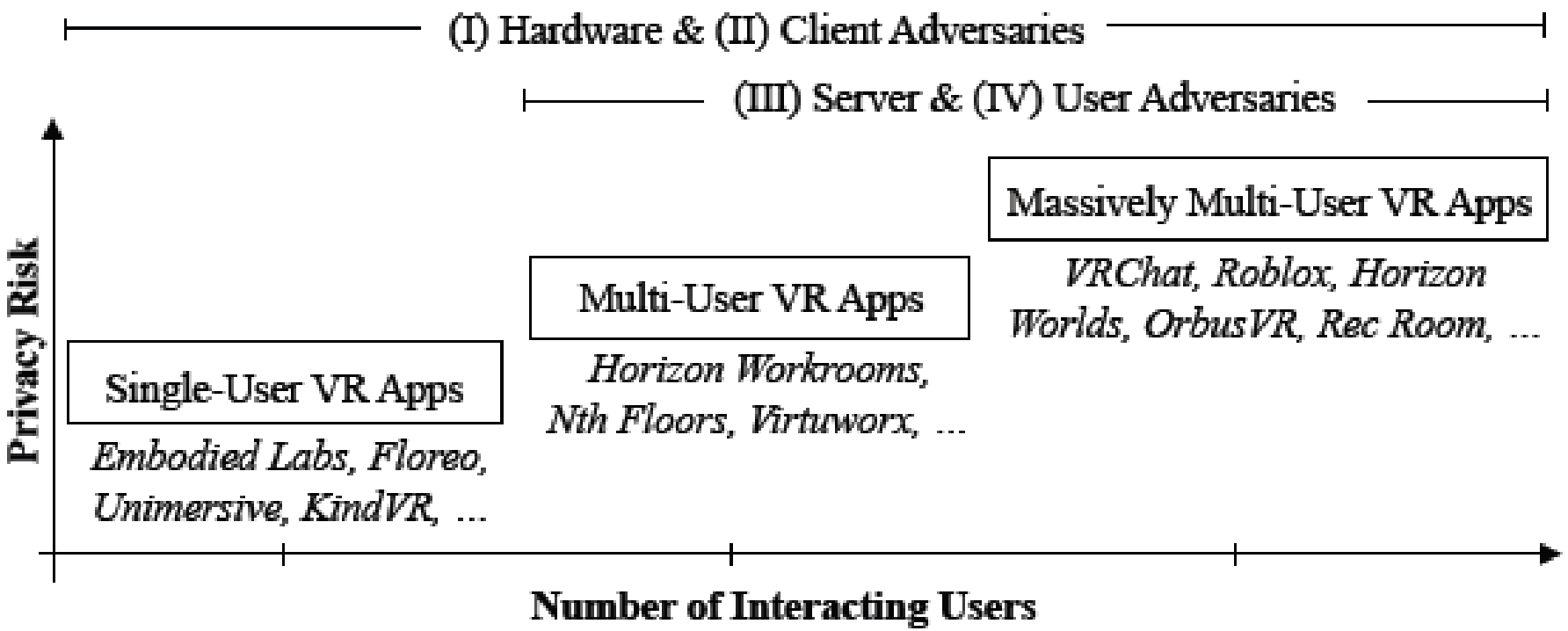


Fig. 2. Attack scenario.

Meng Y, Zhan Y, Li J, Du S, Zhu H, Shen XS (pp. 1-10). IEEE. . De-anonymization attacks on metaverse. In IEEE INFOCOM 2023-IEEE Conference on Computer Communications 2023 May 17

Illustrations credits: Flaticon

Increasing privacy risks with increasing exposure to adversaries



Garrido GM, Nair V, Song D. SoK: Data Privacy in Virtual Reality. Proceedings on Privacy Enhancing Technologies. 2024.

“Processing of **bystander data** poses a crucial **unaddressed privacy risk**, because a **bystander does not have awareness** that their information is being collected and cannot opt out” (Suchismita et al, 2023).

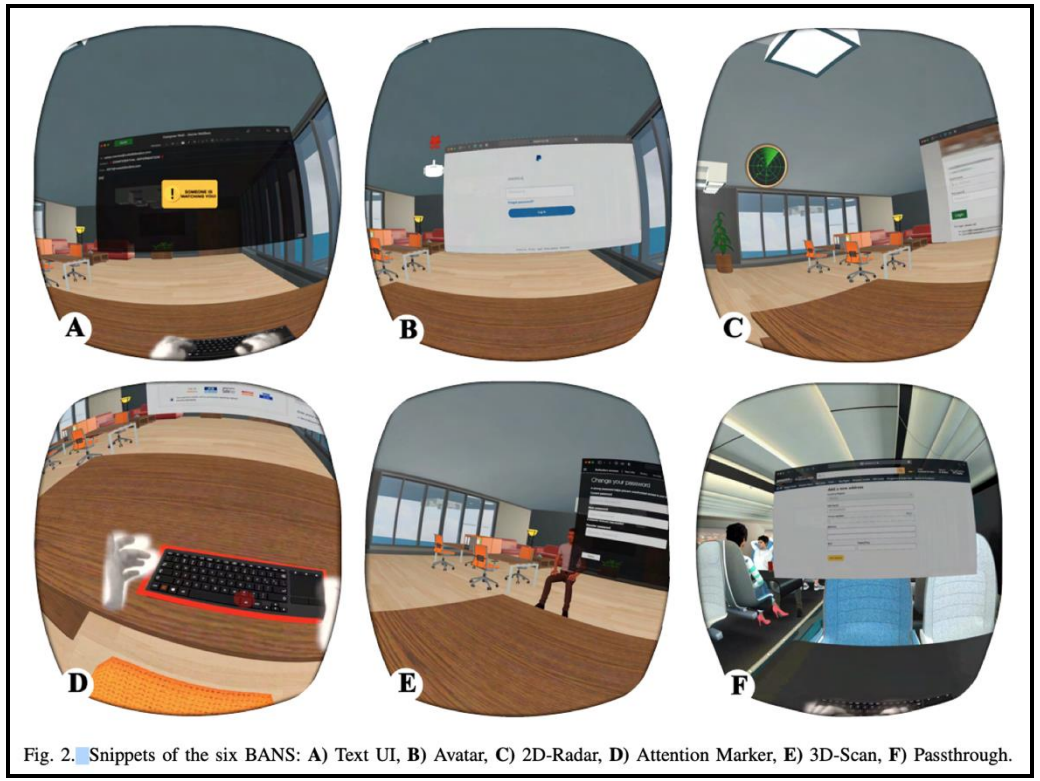
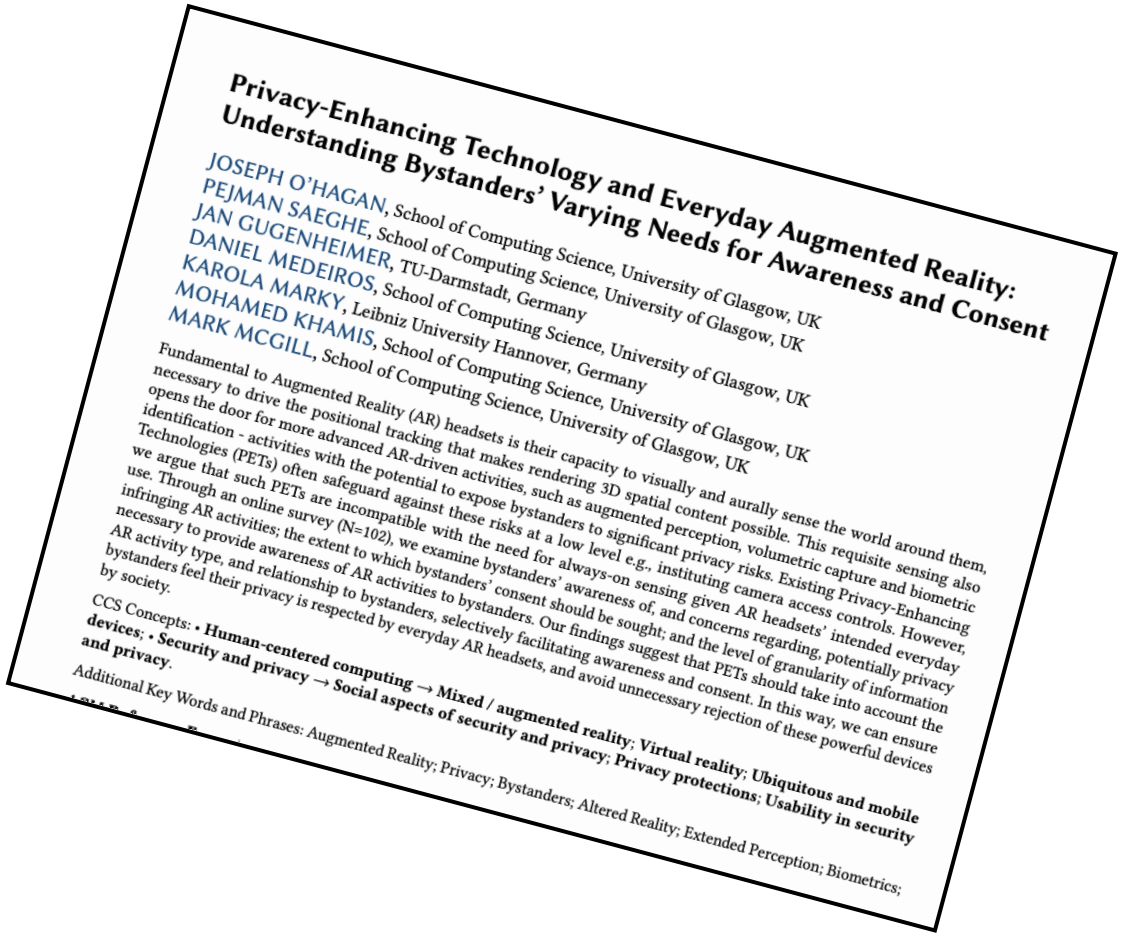


Fig. 2. Snippets of the six BANS: **A)** Text UI, **B)** Avatar, **C)** 2D-Radar, **D)** Attention Marker, **E)** 3D-Scan, **F)** Passthrough.

Bystander **A**wareness **N**otification **S**ystems (BANS), Mansour et al., 2023.



Privacy-Enhancing Technology and Everyday Augmented Reality: Understanding Bystanders' Varying Needs for Awareness and Consent

JOSEPH O'HAGAN, School of Computing Science, University of Glasgow, UK
PEJMAN SAEGHE, School of Computing Science, University of Glasgow, UK
JAN GUGENHEIMER, TU-Darmstadt, Germany
DANIEL MEDEIROS, School of Computing Science, University of Glasgow, UK
KAROLA MARKY, Leibniz University Hannover, Germany
MOHAMED KHAMIS, School of Computing Science, University of Glasgow, UK
MARK MCGILL, School of Computing Science, University of Glasgow, UK

Fundamental to Augmented Reality (AR) headsets is their capacity to visually and aurally sense the world around them, necessary to drive the positional tracking that makes rendering 3D spatial content possible. This requisite sensing also opens the door for more advanced AR-driven activities, such as augmented perception, volumetric capture and biometric identification - activities with the potential to expose bystanders to significant privacy risks. Existing Privacy-Enhancing Technologies (PETs) often safeguard against these risks at a low level e.g., instituting camera access controls. However, we argue that such PETs are incompatible with the need for always-on sensing given AR headsets' intended everyday use. Through an online survey (N=102), we examine bystanders' awareness of, and concerns regarding, potentially privacy infringing AR activities; the extent to which bystanders' consent should be sought; and the level of granularity of information necessary to provide awareness of AR activities to bystanders. Our findings suggest that PETs should take into account the AR activity type, and relationship to bystanders, selectively facilitating awareness and consent. In this way, we can ensure bystanders feel their privacy is respected by everyday AR headsets, and avoid unnecessary rejection of these powerful devices by society.

CCS Concepts: • **Human-centered computing** → **Mixed / augmented reality**; **Virtual reality**; **Ubiquitous and mobile devices**; • **Security and privacy** → **Social aspects of security and privacy**; **Privacy protections**; **Usability in security and privacy**.

Additional Key Words and Phrases: Augmented Reality; Privacy; Bystanders; Altered Reality; Extended Perception; Biometrics;

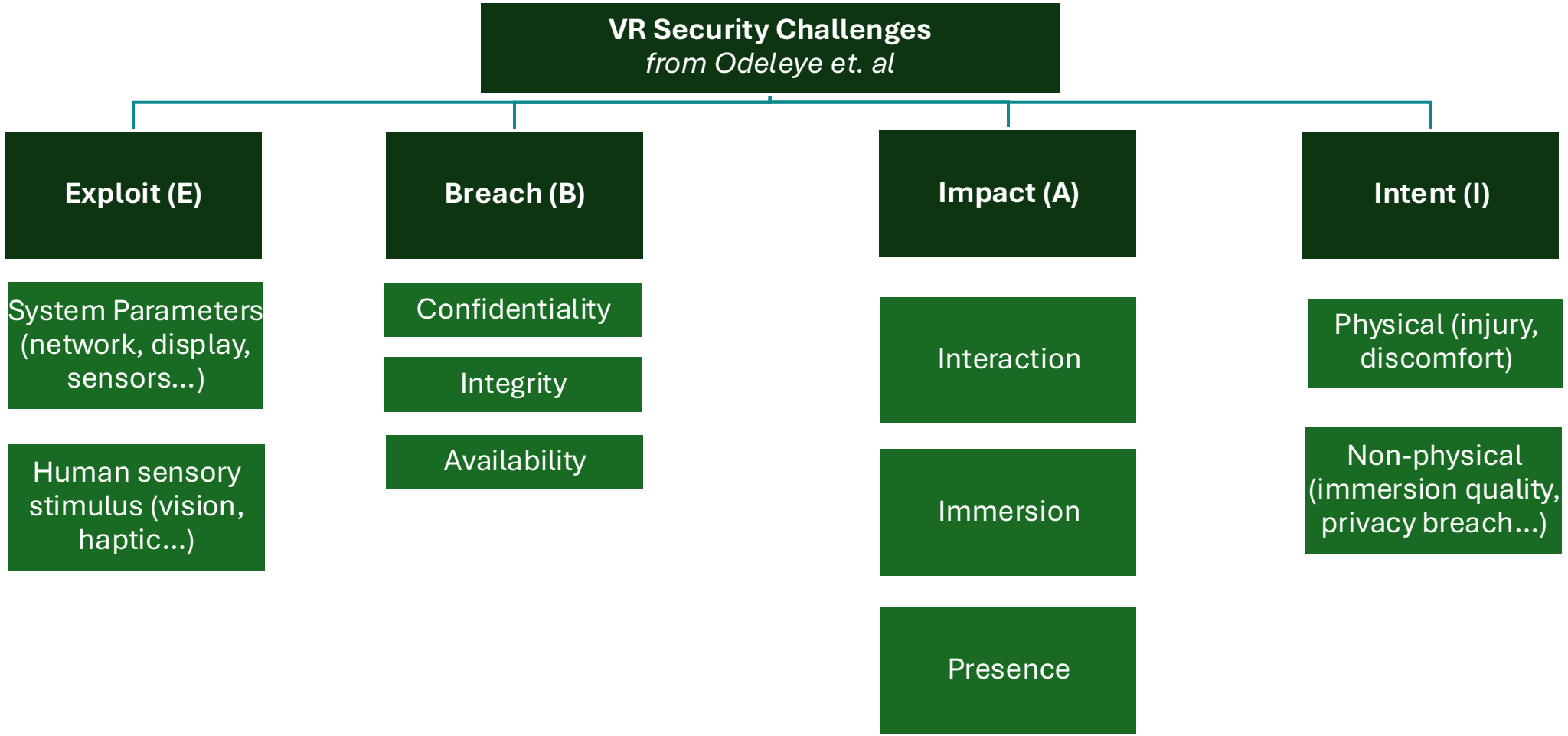
Suchismita, P. and Schroeder, C. (2023). Extended Privacy for Extended Reality: XR Technology Has 99 Problems and Privacy is Several of Them. 4 Notre Dame J. Emerging Tech.
Mansour S, Knierim P, et al. (2023). Bans: Evaluation of bystander awareness notification systems for productivity in VR. InNetwork and Distributed Systems Security (NDSS) Symposium 2023 (Vol. 2).

Security challenges in (social) XR

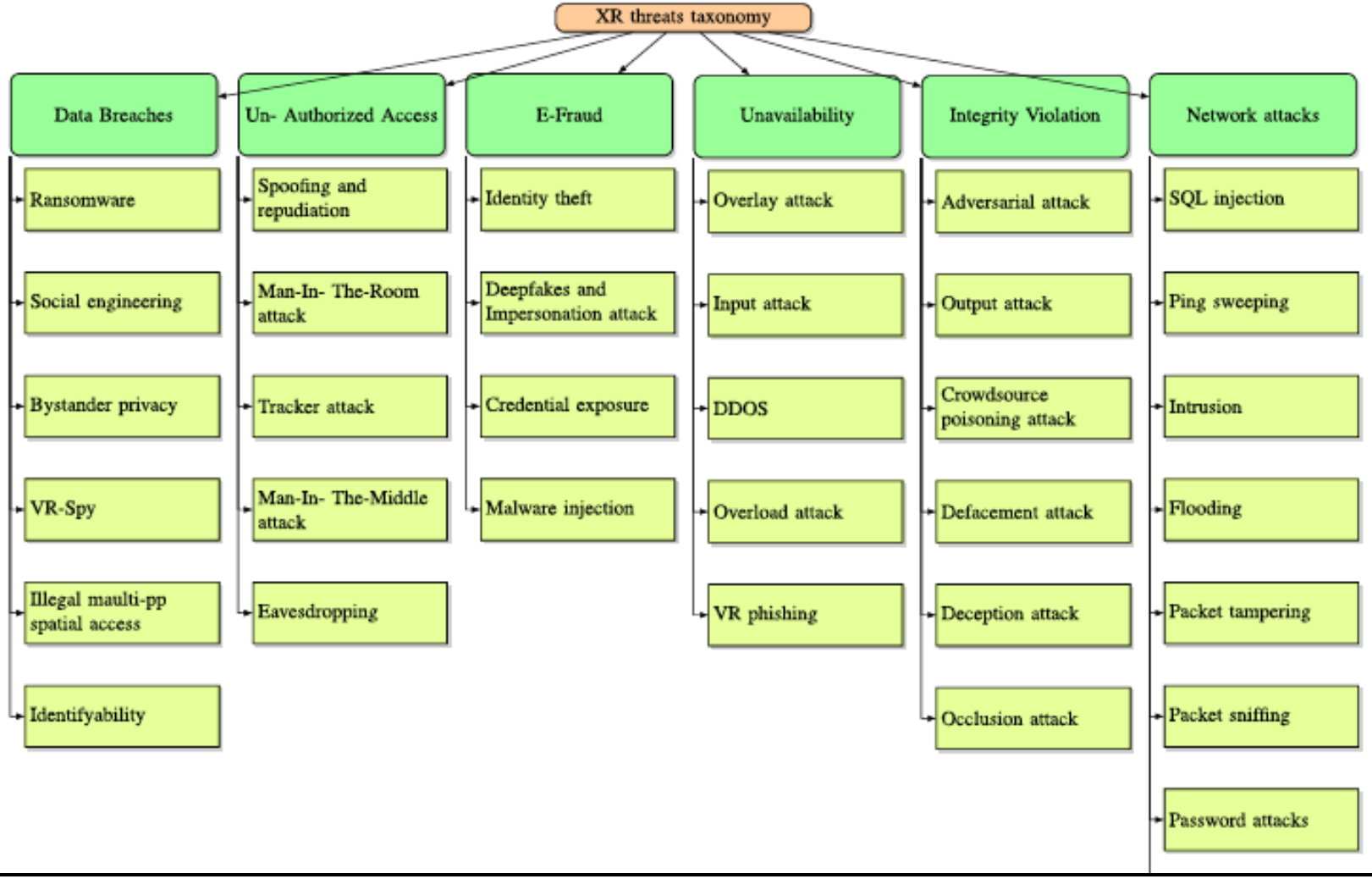
Illustrations credits: Flaticon

Or go to menti.com
Code: **8284 0995**

Confidentiality
Integrity
Authenticity
Availability
Non-repudation



B. Odeleye et al. Virtually secure: A taxonomic assessment of cybersecurity challenges in virtual reality environments. Computers & Security, 2022.

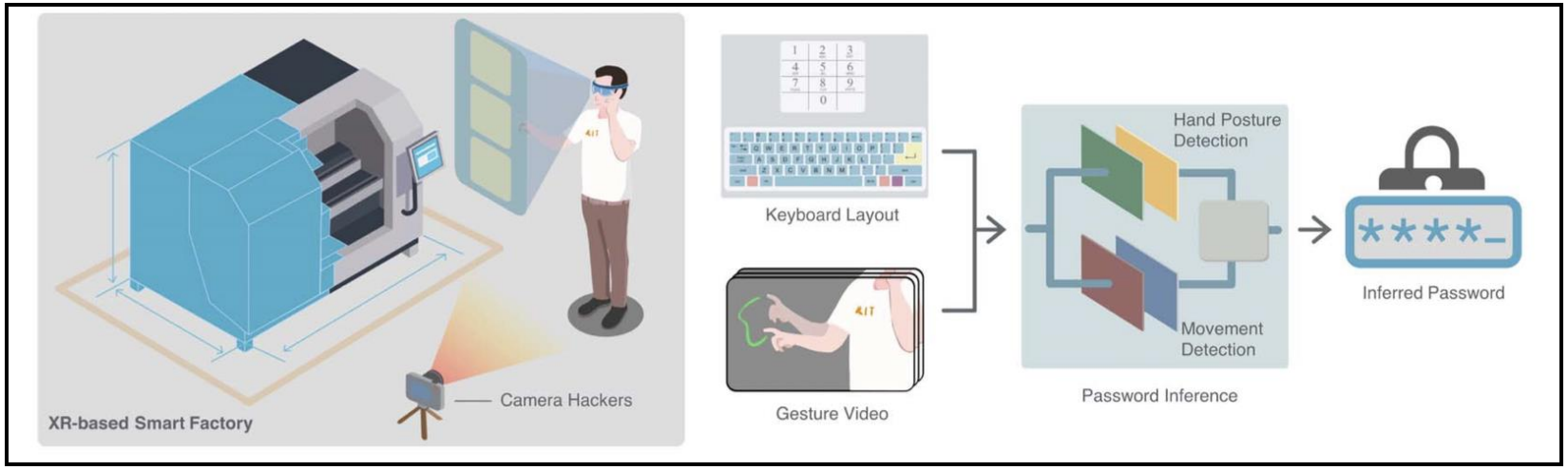


- Broad threat landscape, new dimensions
- AR and VR: Distinct challenges in terms of privacy and security

Qamar, S., Anwar, S., Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems, Computers & Security, Volume 128, 2023, 103127

Yang, W et al. (October 10, 2023). ""I Can See Your Password": A Case Study About Cybersecurity Risks in Mid-Air Interactions of Mixed Reality-Based Smart Manufacturing Applications."

Icons generated with Microsoft CoPilot by Camille Sivelle

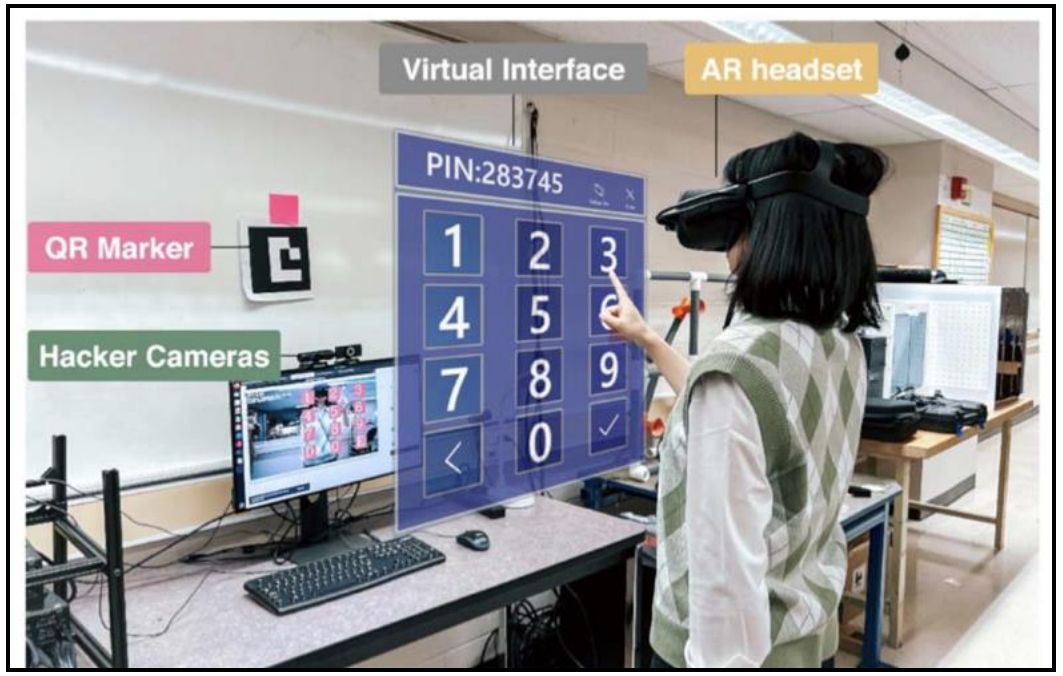


Accuracy in estimating the password

97.03% (2 digit passwords)

94.06% (4 digit passwords)

83.83% (6 digit passwords)



Yang, W et al. (October 10, 2023). "“I Can See Your Password”: A Case Study About Cybersecurity Risks in Mid-Air Interactions of Mixed Reality-Based Smart Manufacturing Applications."

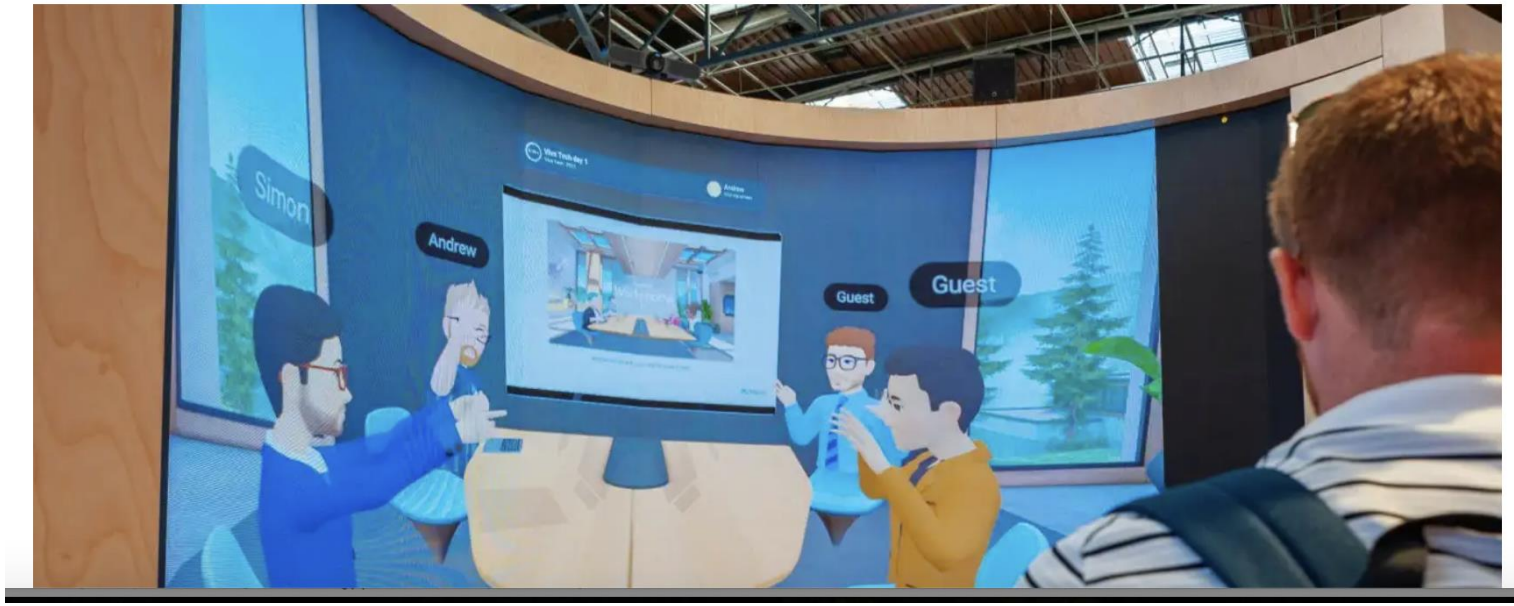
Technology

AI can steal passwords in virtual reality from avatar hand motions

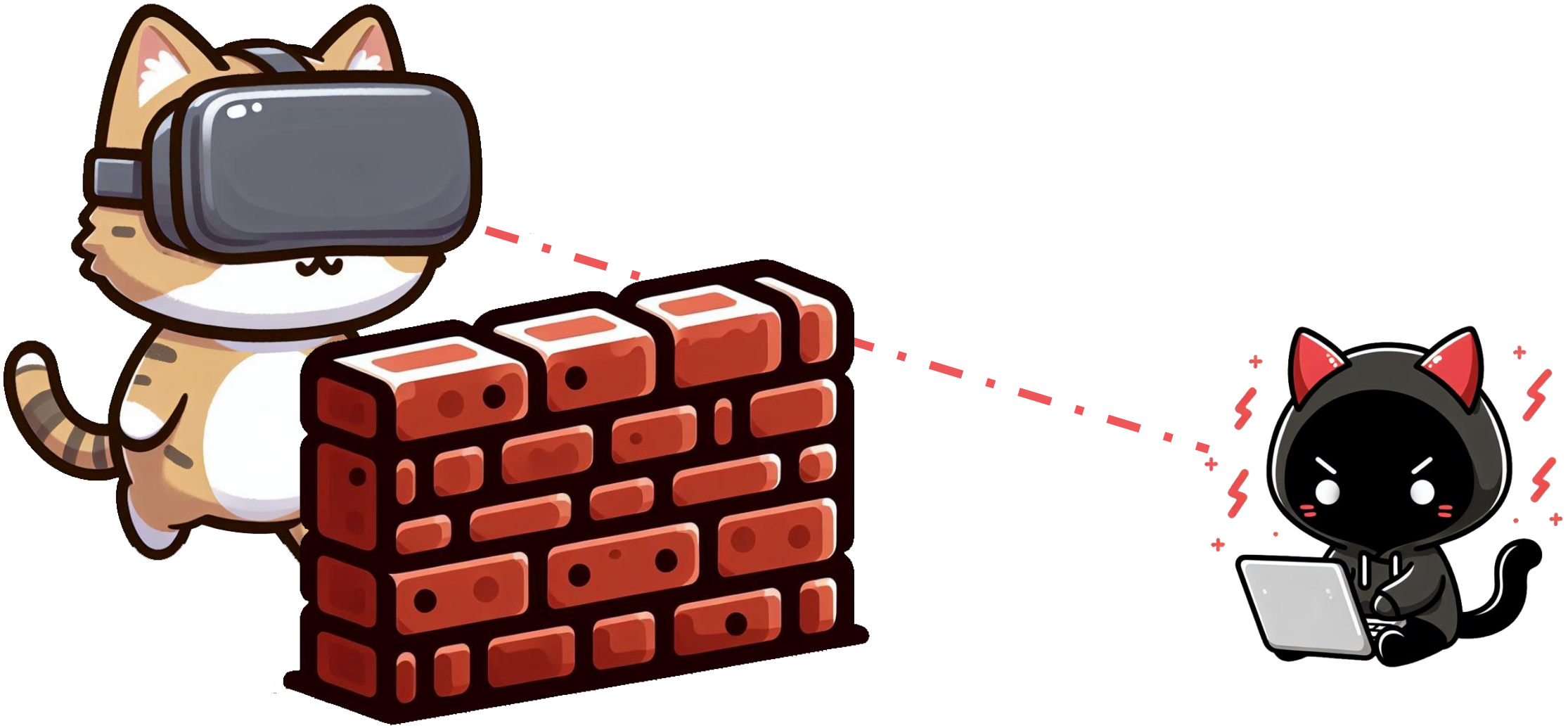
Artificial intelligence can work out what someone is privately typing in VR meetings in Meta Horizon Workrooms by looking at the way their avatar's hands move

By Jeremy Hsu

14 November 2023



https://www.newscientist.com/article/2401929-ai-can-steal-passwords-in-virtual-reality-from-avatar-hand-motions/



W.-J. Tseng et al., CHI Conference on Human Factors in Computing Systems, 2022. “The Dark Side of Perceptual Manipulations in Virtual Reality”

Icons generated with Microsoft CoPilot by Camille Sivelle

MIT Technology Review

Featured Topics Newsletters Events Audio SIGN

COMPUTING

VR headsets can be hacked with an Inception-style attack

Researchers managed to crack Meta's Quest VR system, allowing them to steal sensitive information, and manipulate social interactions.

By Melissa Heikkilä

Deceived by Immersion: A Systematic Analysis of Deceptive Design in Extended Reality

HILDA HADAN, Stratford School of Interaction Design and Business, University of Waterloo, Waterloo, Canada and Games Institute, University of Waterloo, Waterloo, Canada
LYDIA CHOONG, Cheriton School of Computer Science, University of Waterloo, Waterloo, Canada
LEAH ZHANG-KENNEDY, Stratford School of Interaction Design and Business, University of Waterloo, Stratford, Canada
LENNART E. NACKE, Stratford School of Interaction Design and Business, University of Waterloo, Waterloo, Canada

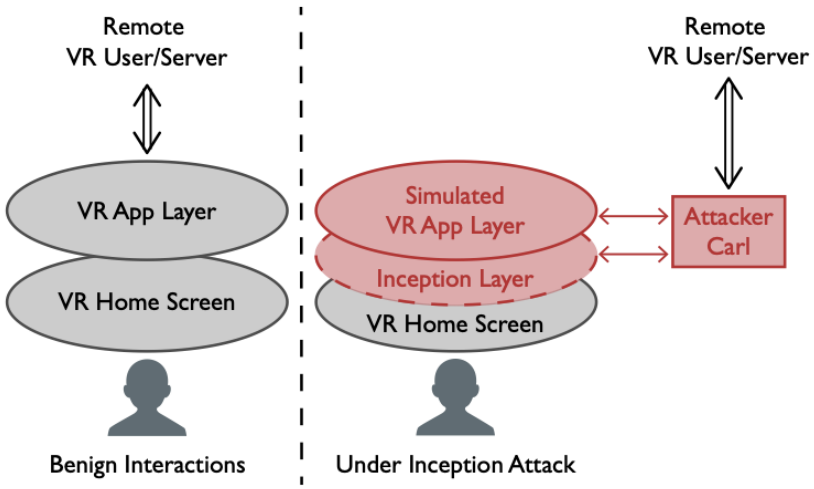
The well-established deceptive design literature has focused on conventional user interfaces. With the rise of extended reality (XR), understanding deceptive design's unique manifestations in this immersive domain is crucial. However, existing research lacks a full, cross-disciplinary analysis that analyzes how XR technologies enable new forms of deceptive design. Our study reviews the literature on deceptive design in XR environments. We use thematic synthesis to identify key themes. We found that XR's immersive capabilities and extensive data collection enable subtle and powerful manipulation strategies. We identified eight themes outlining these strategies and discussed existing countermeasures. Our findings show the unique risks of deceptive design in XR, highlighting implications for researchers, designers, and policymakers. We propose future research directions that explore unintentional deceptive design, data-driven manipulation solutions, user education, and the link between ethical design and policy regulations.

CCS Concepts: • **Human-centered computing → Mixed/augmented reality**; **Virtual reality**; **HCI theory, concepts and models**;

Additional Key Words and Phrases: Deceptive design, dark pattern, user manipulation, extended reality, virtual reality, augmented reality, mixed reality

ACM Reference Format:
Hilda Hadan, Lydia Choong, Leah Zhang-Kennedy, and Lennart E. Nacke. 2024. Deceived by Immersion: A Systematic Analysis of Deceptive Design in Extended Reality. *ACM Comput. Surv.* 56, 10, Article 250 (May 2024), 25 pages. https://doi.org/10.1145/3659945

This research was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery



Yang Z, Li CY, Bhalla A, Zhao BY, Zheng H. Inception attacks: Immersive hijacking in virtual reality systems. arXiv preprint arXiv:2403.05721. 2024 Mar 8.

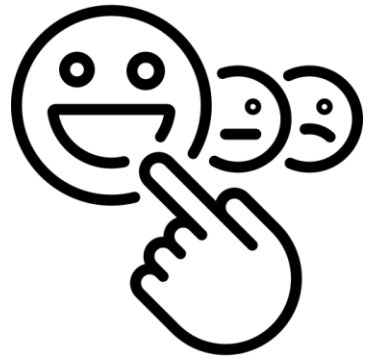
"*The **insecurity of XR systems** allows for all types of **deceptive design** that exploits XR design elements and users' false beliefs in the authenticity of XR content.*"
Hadan et al., (2024).

Hadan, H., et al. (2024). Deceived by Immersion: A Systematic Analysis of Deceptive Design in Extended Reality. ACM Comput. Surv. 56, 10, Article 250

1. New types of vulnerabilities and impacts

2. Traditional privacy and security measures are not sufficient.

3. Inherently intertwined with UX



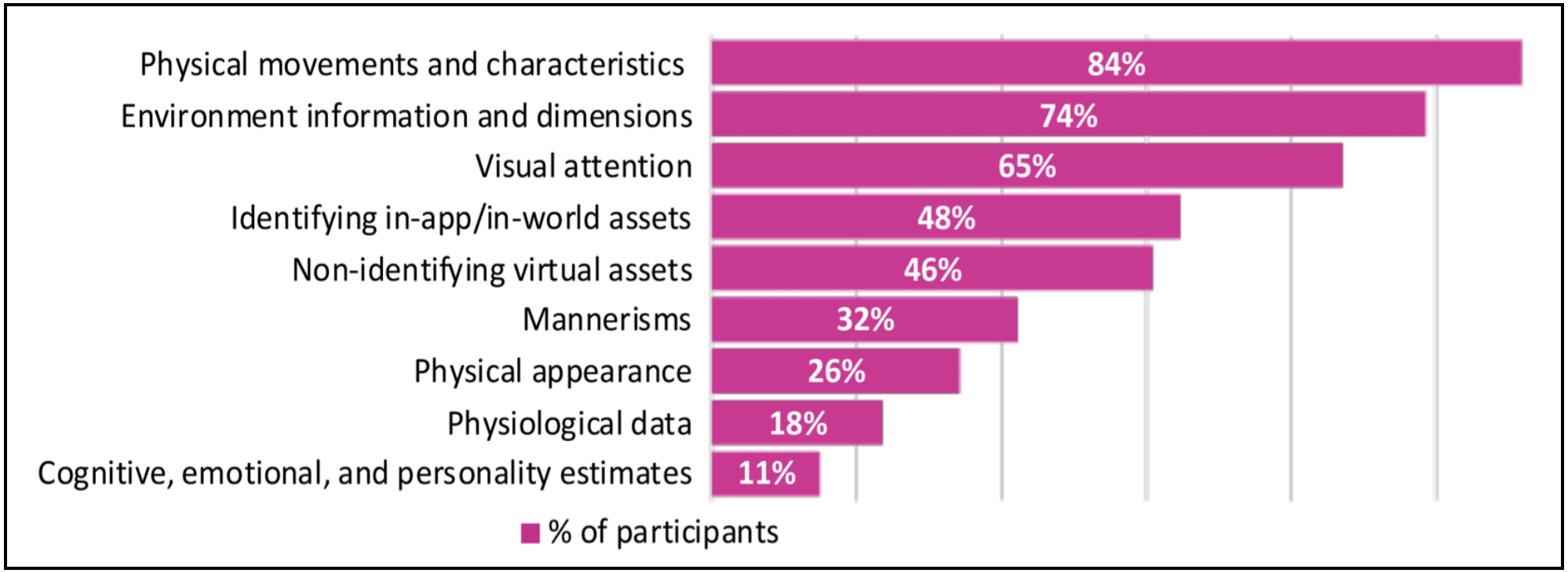
UX challenges

Illustrations credits: Flaticon

”Designing **secure social VR** applications that **protect users while enhancing their experience, acceptance and trust** remains a **challenge**”

(Lin et al. 2024).

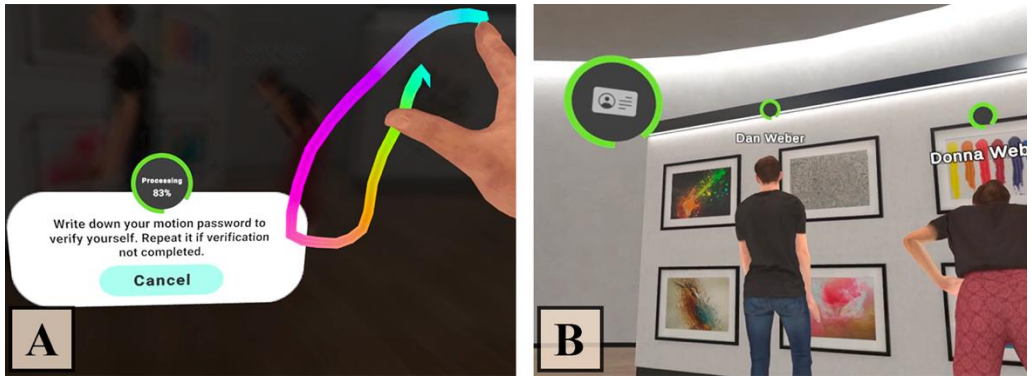
Need to **make users more aware** of data privacy threats in XR (Hadan et al., 2024)



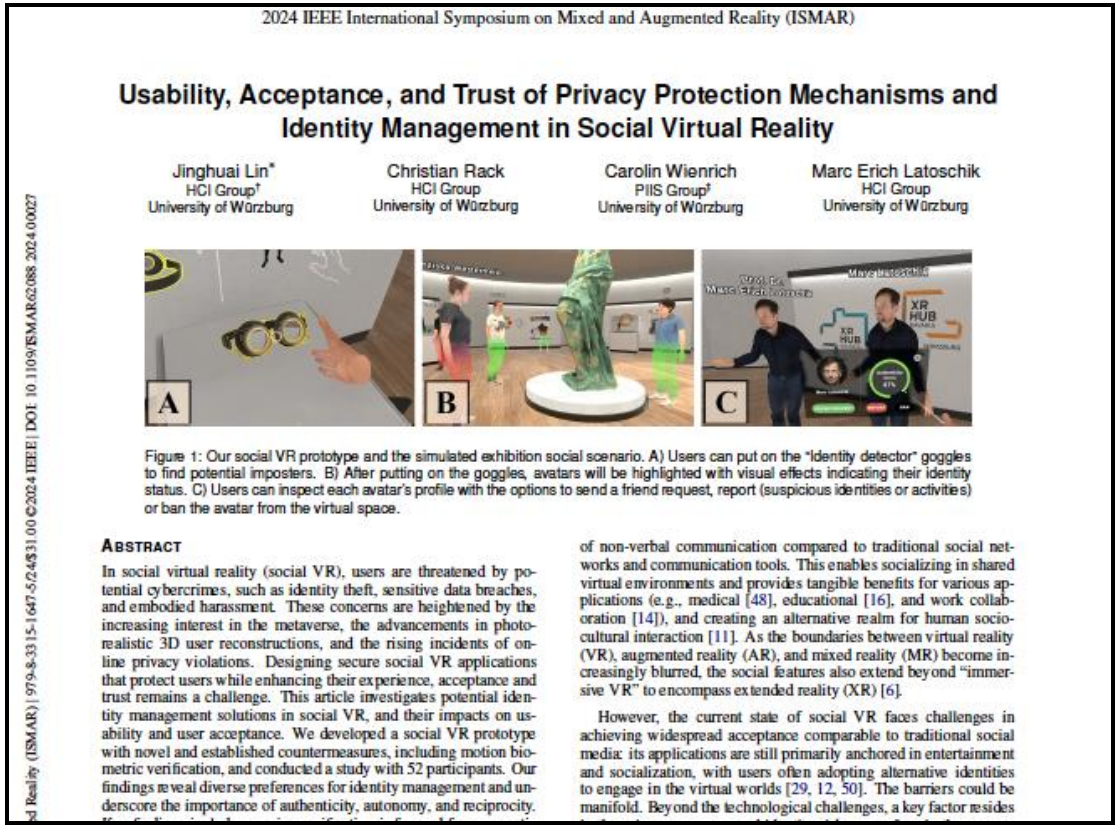
Hadan et al. (CHI 2024): "% of participants (N = 464) perceived the collection of different types of data through XR devices.

Hadan, H. Derrick M. Wang, Lennart E. Nacke, and Leah Zhang-Kennedy. 2024. Privacy in Immersive Extended Reality: Exploring User Perceptions, Concerns, and Coping Strategies. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI '24).

- Need for **design and evaluation approaches** that to a larger extent consider different **tensions**, from the off-set
- **Diversity** and **inclusion**



Active vs. passive verification (Lin et al., 2024)



2024 IEEE International Symposium on Mixed and Augmented Reality (ISMAR)

Usability, Acceptance, and Trust of Privacy Protection Mechanisms and Identity Management in Social Virtual Reality

Jinghuai Lin* HCI Group† University of Würzburg
Christian Rack HCI Group University of Würzburg
Carolin Wienrich PIIS Group‡ University of Würzburg
Marc Erich Latoschik HCI Group University of Würzburg

Figure 1: Our social VR prototype and the simulated exhibition social scenario. A) Users can put on the "Identity detector" goggles to find potential imposters. B) After putting on the goggles, avatars will be highlighted with visual effects indicating their identity status. C) Users can inspect each avatar's profile with the options to send a friend request, report (suspicious identities or activities) or ban the avatar from the virtual space.

ABSTRACT

In social virtual reality (social VR), users are threatened by potential cybercrimes, such as identity theft, sensitive data breaches, and embodied harassment. These concerns are heightened by the increasing interest in the metaverse, the advancements in photo-realistic 3D user reconstructions, and the rising incidents of online privacy violations. Designing secure social VR applications that protect users while enhancing their experience, acceptance and trust remains a challenge. This article investigates potential identity management solutions in social VR, and their impacts on usability and user acceptance. We developed a social VR prototype with novel and established countermeasures, including motion biometric verification, and conducted a study with 52 participants. Our findings reveal diverse preferences for identity management and underscore the importance of authenticity, autonomy, and reciprocity.

of non-verbal communication compared to traditional social networks and communication tools. This enables socializing in shared virtual environments and provides tangible benefits for various applications (e.g., medical [48], educational [16], and work collaboration [14]), and creating an alternative realm for human socio-cultural interaction [11]. As the boundaries between virtual reality (VR), augmented reality (AR), and mixed reality (MR) become increasingly blurred, the social features also extend beyond "immersive VR" to encompass extended reality (XR) [6].

However, the current state of social VR faces challenges in achieving widespread acceptance comparable to traditional social media: its applications are still primarily anchored in entertainment and socialization, with users often adopting alternative identities to engage in the virtual worlds [29, 12, 50]. The barriers could be manifold. Beyond the technological challenges, a key factor resides

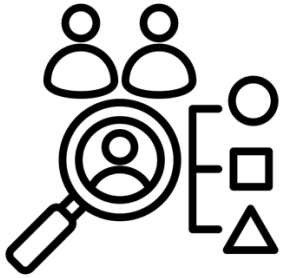
d Reality (ISMAR) | 979-8-3315-1647-5/24$31.00 ©2024 IEEE | DOI: 10.1109/ISMAR62088.2024.00027

Experimental evaluation of different privacy protection and identity management mechanisms (Lin et al., 2024)

Lin J, Rack C, Wienrich C, Latoschik ME. Usability, Acceptance, and Trust of Privacy Protection Mechanisms and Identity Management in Social Virtual Reality. In2024 IEEE International Symposium on Mixed and Augmented Reality (ISMAR) 2024 Oct 21 (pp. 130-139). IEEE.

*“Pursuing every possible or technically feasible option to enhance user experience in XR environments should **not** come at the cost of user data privacy”.* (Maddem, 2024)

K. Maddern (2024). https://news.exeter.ac.uk/faculty-of-humanities-arts-and-social-sciences/growth-of-extended-reality-tech-means-new-enhanced-regulation-needed-to-protect-peoples-privacy/ .



Short case study

C. Sivelle, D. Palma and K. De Moor (2025). Security and Privacy for VR in non-entertainment sectors: a practice-based study of the challenges, strategies and gaps. MASSXR workshop at IEEE VR.

Illustrations credits: Flaticon

NORCICS T3.13: Secure, ethical and human-centered technology experiences in critical sectors

Our team

Katrien De Moor, Associate professor (lead)

Kaja Ystgaard, Researcher, Ethical and secure digitalization in critical sectors

Camille Sivelle, PhD Student - Secure, Human-centered XR experiences in Critical Sectors

Julie Høgetveit, MSc student, XR in Norwegian Healthcare: Data Privacy and Security Concerns

Katrine Bjune, MSc student, XR in Norwegian Healthcare: Data Privacy and Security Concerns

Henriette Bjørnheim, Master student - Assessing Ethical Risks and Challenges in EdTech

Anna Storli Tveit, External collaborator – Mass surveillance and marginalized groups

Recent publications:

Sivelle, C., Palma, D. and De Moor, K. (2025). Security and privacy for VR in non-entertainment sectors: a practice-based study of the challenges, strategies and gaps. MASSXR-workshop at IEEE VR2025.

Ystgaard, K.T., Kuosa, T. and De Moor, K. (2025,forthcoming). Backcasting future human autonomy and ethics protection in smart health environments: a case study. IEEE Ethics 2025.

Storli Tveit, A., De Moor, K. (2025, forthcoming). Marginalised groups "under surveillance": a meta analysis. IEEE Ethics 2025.

Ystgaard, K.F., De Moor, K. (2025). Assessing Ethical Risks in Smart Environment Use Cases: A ForSTI Methodological Approach. HCI International 2024 – Late Breaking Papers. HCII 2024. Lecture Notes in Computer Science, vol 15380. Springer, Cham.

Sivelle, C., Palma, D. and De Moor, K. (2024). Extended Reality in critical sectors: Exploring the use cases and challenges, Nokobit 2024.

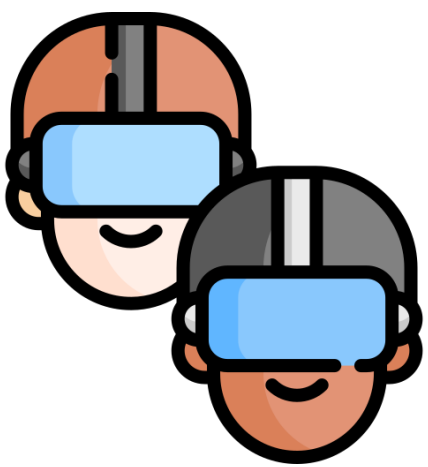
NORCICS

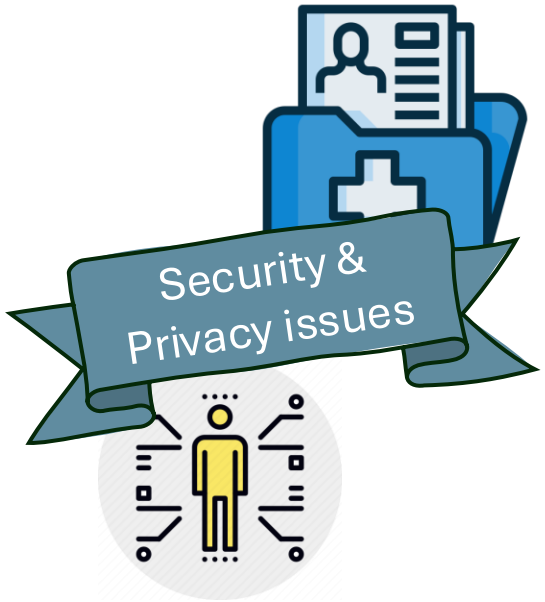
SFI Norwegian Centre for Cybersecurity in Critical Sectors

NTNU

Norwegian Centre for Research-based Innovation

What are the **relevant S&P challenges** for non-entertainment VR experiences, according to **the people who create them**?





C. Sivelle, D. Palma and K. De Moor (2025). Security and Privacy for VR in non-entertainment sectors: a practice-based study of the challenges, strategies and gaps. MASSXR workshop at IEEE VR.

Illustrations credits: Flaticon

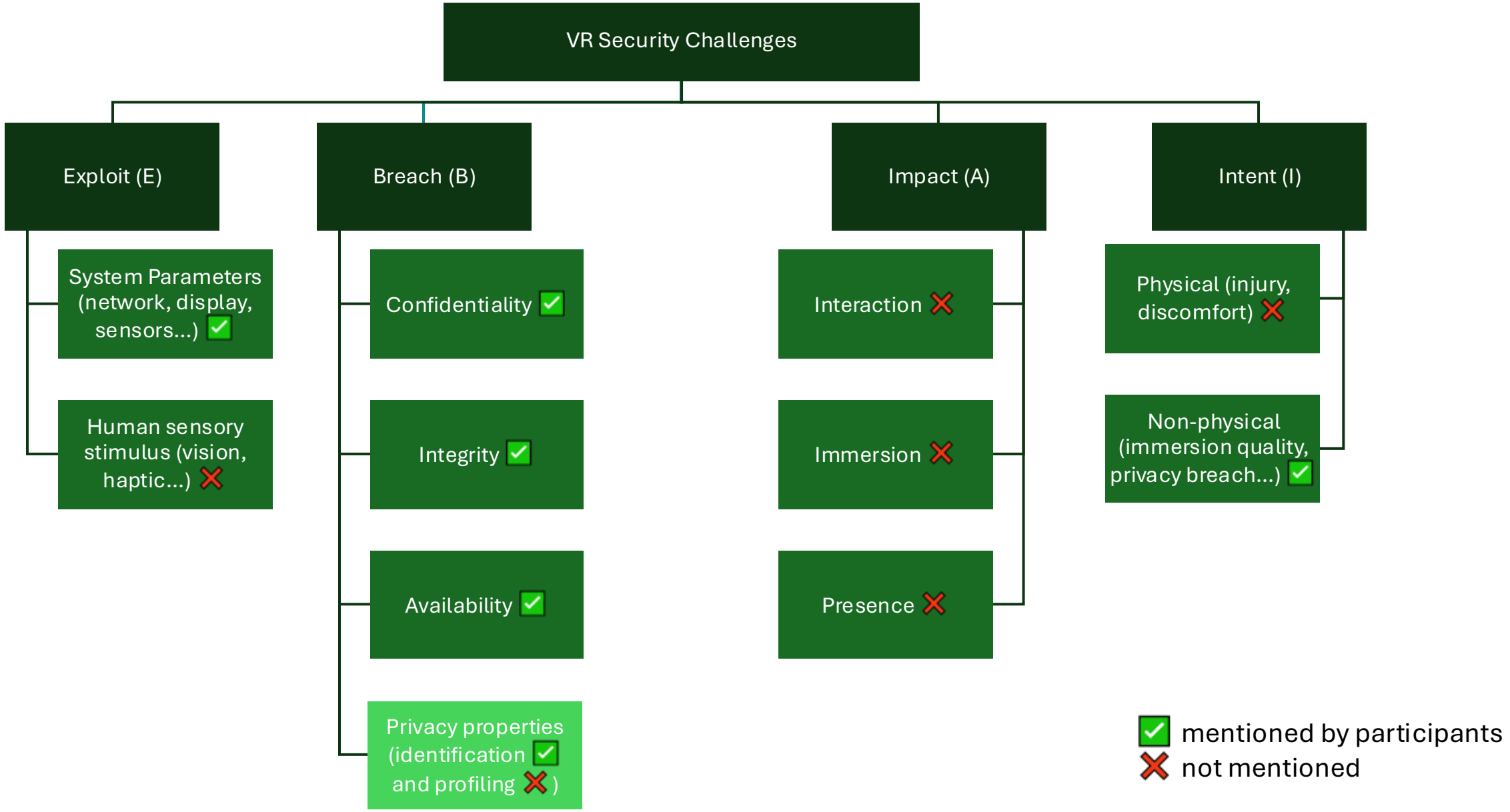
Semi-structured interviews (N=7) covering:
✅ the use case for VR
✅ Non-entertainment, developers,CTO/CEO's
✅ S&P perceptions
✅ security and data collection practices

Thematic analysis against a S&P threat framework for VR

Follow-up study ongoing (Interviews, N=17 experts) specifically focusing on XR in health

C. Sivelle, D. Palma and K. De Moor (2025). Security and Privacy for VR in non-entertainment sectors: a practice-based study of the challenges, strategies and gaps. MASSXR workshop at IEEE VR.

Illustrations credits: Flaticon



C. Sivelle, D. Palma and K. De Moor (2025). Security and Privacy for VR in non-entertainment sectors: a practice-based study of the challenges, strategies and gaps. MASSXR workshop at IEEE VR.

Observations

Stakeholders are concerned about S&P…*but only about the «traditional» threats?*

Gap in awareness

Gap literature vs. practice

Legal grey zone impacts how XR is used

C. Sivelle, D. Palma and K. De Moor (2025). Security and Privacy for VR in non-entertainment sectors: a practice-based study of the challenges, strategies and gaps. MASSXR workshop at IEEE VR.

Concluding thoughts

Illustrations credits: Flaticon

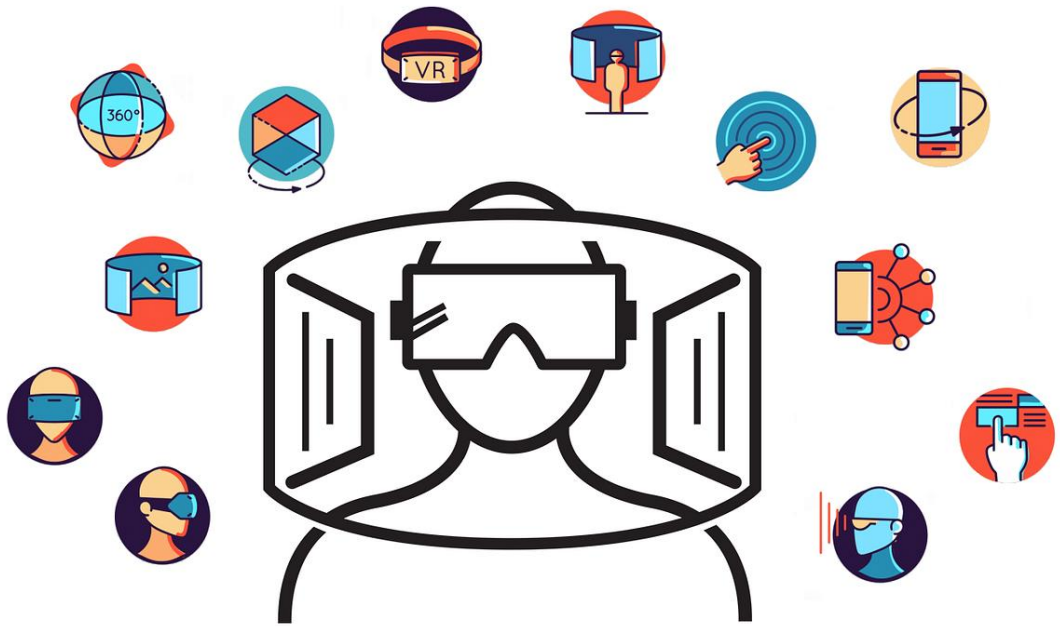
(Social) XR environments: vulnerable to (cyber)security threats

- XR Data introduces "*unprecedented risks*" (Abraham et al., 2022)
- New, XR-specific threats, further strengthened by AI (e.g., deepfakes)
- Focus on increasing awareness and robust countermeasures

Balancing privacy/anonymity and personalized experiences

- Data minimization, meaningful user control and autonomy over digital identity
- Importance of transparent XR data practices and standards
- Privacy-preserving techniques *by default*, privacy-choice interfaces, opt-out
- Considering users AND bystanders

Tollgart getty images, from https://www.wired.com/story/virtual-reality-accessibility-disabilities/



https://medium.com/@alex24dutertre/the-ethical-challenges-of-ar-vr-a5333594f909

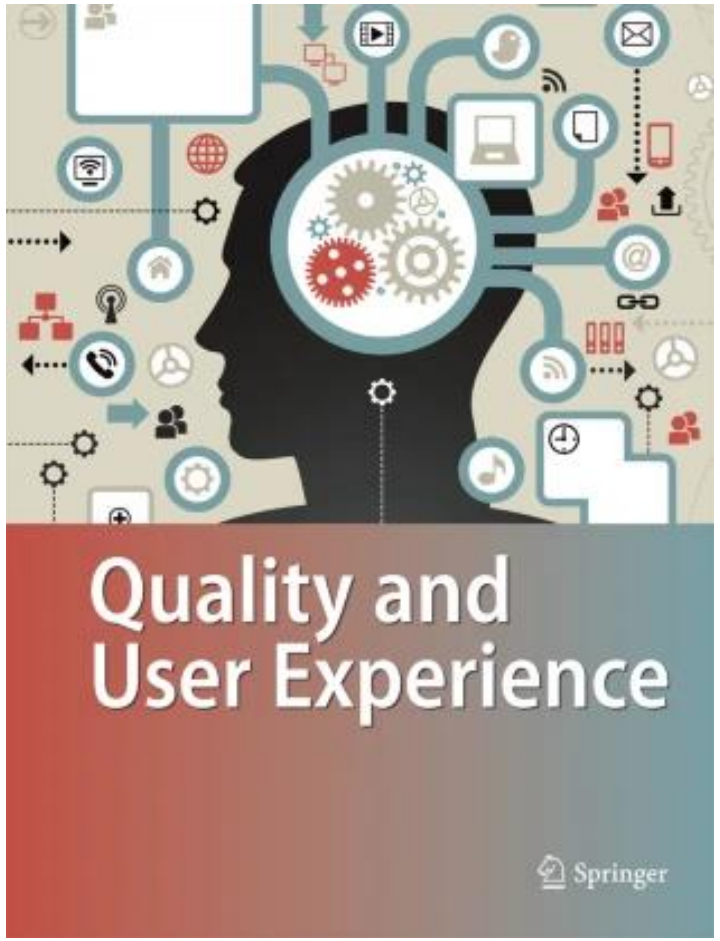
UX, security and privacy are inherently intertwined and need to be addressed **holistically** to create **human-centred**, ethical, safe, engaging XR environments "**by design**"

- Human-centred approach to S & P measures and defense strategies
- UX evaluation should also consider S & P concerns
- Trust

Extensive data collection poses novel legal and ethical challenges

- Bias, manipulation, discrimination, …
- High-risk use cases, e.g., automated profiling
- May impact further adoption in non-entertainment sectors

Or go to menti.com
Code: **8284 0995**



Interested in contributing to a “Spring School on Social XR” special issue as guest editor or author?

Come and talk to me!

Thank you!

linkedin.com/in/katriendemoor
katrien.demoor@ntnu.no

Illustrations credits: Flaticon, Copilot
Special thanks to Camille Sivelle

References / Recommended reading

Lin and Latoschik (2022). Digital body, identity and privacy in social virtual reality: A systematic review. Frontiers in Virtual Reality. Vol 3, 2022.

Pahi, Suchismita and Schroeder, Calli, Extended Privacy for Extended Reality: XR Technology Has 99 Problems and Privacy is Several of Them (August 28, 2022). 4 Notre Dame J. Emerging Tech (Forthcoming 2023). , http://dx.doi.org/10.2139/ssrn.4202913

Dick, E. (2021). Balancing user privacy and innovation in augmented and virtual reality. Information Technology and Innovation Foundation.

Garrido GM, Nair V, Song D. SoK: Data Privacy in Virtual Reality. Proceedings on Privacy Enhancing Technologies (PETS). 2024.

Qamar S, Anwar Z, Afzal M. A systematic threat analysis and defense strategies for the metaverse and extended reality systems. Computers & Security. 2023 May 1;128:103127.

Abraham M, Saeghe P, Mcgill M, Khamis M. Implications of xr on privacy, security and behaviour: Insights from experts. In Nordic Human-Computer Interaction Conference 2022 Oct 8 (pp. 1-12).

V. Nair et al., 32nd USENIX Conference on Security Symposium, 2023. “Unique identification of 50,000+ virtual reality users from head & hand motion data. https://www.usenix.org/system/files/usenixsecurity23-nair-identification.pdf

Lin J, Rack C, Wienrich C, Latoschik ME. Usability, Acceptance, and Trust of Privacy Protection Mechanisms and Identity Management in Social Virtual Reality. In2024 IEEE International Symposium on Mixed and Augmented Reality (ISMAR) 2024 Oct 21 (pp. 130-139). IEEE.

Hadan, H. Derrick M. Wang, Lennart E. Nacke, and Leah Zhang-Kennedy. 2024. Privacy in Immersive Extended Reality: Exploring User Perceptions, Concerns, and Coping Strategies. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI '24). Association for Computing Machinery, New York, NY, USA, Article 784, 1–24. https://doi.org/10.1145/3613904.3642104

Joseph O'Hagan, Pejman Saeghe, Jan Gugenheimer, Daniel Medeiros, Karola Marky, Mohamed Khamis, and Mark McGill. 2023. Privacy-Enhancing Technology and Everyday Augmented Reality: Understanding Bystanders' Varying Needs for Awareness and Consent. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 6, 4, Article 177 (December 2022), 35 pages. https://doi.org/10.1145/3569501

Hadan, H., et al. (2024). Deceived by Immersion: A Systematic Analysis of Deceptive Design in Extended Reality. ACM Comput. Surv. 56, 10, Article 250 (October 2024), 25 pages. https://doi.org/10.1145/3659945

Mansour S, Knierim P, O’Hagan J, Alt F, Mathis F. Bans: Evaluation of bystander awareness notification systems for productivity in vr. InNetwork and Distributed Systems Security (NDSS) Symposium 2023 (Vol. 2).