Novel Challenges of Safety, Security and Privacy in Extended Reality

Jan Gugenheimer
Telecom-Paris/LTCI (IP-Paris)
Paris, France

Wen-Jie Tseng
Telecom-Paris/LTCI (IP-Paris)
Paris, France

Abraham Mhaidli
University of Michigan
Ann Arbor, United States

Jan-Ole Rixen
Ulm University
Ulm, Germany

Mark McGill
University of Glasgow
Glasgow, Scotland

Michael Nebeling
University of Michigan
Ann Arbor, United States

Mohamed Khamis
University of Glasgow
Glasgow, Scotland

Florian Schaub
University of Michigan
Ann Arbor, United States

Sanchari Das
University of Denver
Denver, United States

ABSTRACT

Extended Reality (AR/VR/MR) technology is becoming increasingly affordable and capable, becoming ever more interwoven with everyday life. HCI research has focused largely on innovation around XR technology, exploring new use cases and interaction techniques, understanding how this technology is used and appropriated etc. However, equally important is the investigation and consideration of risks posed by such advances, specifically in contributing to new vulnerabilities and attack vectors with regards to security, safety, and privacy that are unique to XR. For example perceptual manipulations in VR, such as redirected walking or haptic retargeting, have been developed to enhance interaction, yet subversive use of such techniques has been demonstrated to unlock new harms, such as redirecting the VR user into a collision. This workshop will convene researchers focused on HCI, XR, Safety, Security, and Privacy, with the intention of exploring safety, privacy, and security challenges of XR technology. With an HCI lens, workshop participants will engage in critical assessment of emerging XR technologies and develop an XR research agenda that integrates research on interaction technologies and techniques with safety, security and privacy research.

CCS CONCEPTS

• **Human-centered computing → Human computer interaction (HCI)**; **Virtual reality**; • **Security and privacy → Usability in security and privacy**.

KEYWORDS

Virtual Reality, Augmented Reality, Mixed Reality, MR, AR, VR, XR, Safety, Security, Privacy

ACM Reference Format:
Jan Gugenheimer, Wen-Jie Tseng, Abraham Mhaidli, Jan-Ole Rixen, Mark McGill, Michael Nebeling, Mohamed Khamis, Florian Schaub, and Sanchari Das. 2022. Novel Challenges of Safety, Security and Privacy in Extended Reality. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '22 Extended Abstracts), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3491101.3503741

1 INTRODUCTION

Extended Reality (XR) technology (referring to Augmented Reality, Virtual Reality, Mixed Reality), is rapidly reaching sufficient technological maturity to see adoption in a plethora of fields, such as education [6] or productivity [19]. However, the larger vision behind XR technology is that it becomes an everyday consumer device, supplementing and eventually supplanting smartphones and other physical display-based devices to become our main gateway to access digital information [14, 15]. Whilst XR technology undoubtedly has the potential to improve the lives of users, it will also inevitably contribute to novel risks and attack vectors – for XR users, bystanders, and society as a whole [20, 26, 27].

While Security, Safety and Privacy research are well-established fields inside of Computer Science, the field of Usable Security has only been exploring the intersection with Human-Computer Interaction for the last 15 years [11]. XR technology uniquely poses new cross-cutting challenges, particularly given the rapid advancement in XR technology, and its associated research and applications. One such novel issue are so-called *immersive attacks* [5] or other such *perceptual manipulations* [20]. The core idea of these attacks is that the target for attack vectors and vulnerabilities is not a hardware or software system, but the human that is using this technology with the intend of inflicting physical or psychological harm. While such threats may exist in other domains (e.g., autonomous driving cars), their occurrence in everyday consumer devices is still rare. These *immersive attacks* are frequently using techniques and methods that are often altering the human multi-sensory perception to nudge the user's physical movements. Examples of such methods that could be abused to manipulate a users actions are researched in redirected walking [24, 29, 30], redirected touch [3, 17], or action prediction [10]. While *immersive attacks* are only one example of these novel types of issues that occur at the intersection of Security, Privacy, Safety research, Human-Computer Interaction research and XR research, they demonstrate clearly how these disciplines are

CHI '22 Extended Abstracts, April 29-May 5, 2022, New Orleans, LA, USA

becoming increasingly interwoven, necessitating a joint agenda to tackle these pressing challenges. In particular, it highlights that the field of XR and HCI research, which is often focused on innovation, has to take a more critical perspective on their own creations.

This workshop aims to bring together researchers and practitioners from all three areas of research: *Safety, Security and Privacy*, *Human-Computer Interaction* and *Extended Reality* to engage in a discussion around new types of potential threats emerging in the XR context. The focus will be on engaging in group discussion/debate rather than on presenting individual results. Therefore, we divided the workshop into three session each focusing on topics in the field of *Safety*, *Security* and *Privacy*. Each session will consist of four short presentations of workshop submissions and end with an approximately 45-minute long panel discussion with the four authors/presenters (each from one submission), and one organizer and/or external expert (which will be additionally invited by the organizer of the panel). This format will emphasize discussion facilitated and structured by one of the organizers acting as panel moderator. We are particularly eager to have this workshop and its discussions at CHI 2022, since the field of HCI is becoming one of the core contributors and innovators in creating novel attack vectors.

2 BACKGROUND AND PRIOR WORKSHOPS

In the last years, the intersection of XR advances and emerging risks and threats has received significant attention, with workshops being organized at major conferences in the security domain (e.g., "VR4Sec: Security for XR and XR for Security" at SOUPS 2021 [2]) and conferences in the field of XR (e.g., "PrXR: Towards a roadmap for privacy and security research for mixed reality applications" at IEEE VR 2021 [1]). While these topics are getting more attention and discussion inside these two communities (XR and Security, Security and Privacy), there has been little overlap and interaction with the HCI community. We argue that the HCI community, which has become a strong innovator in the field of XR [26, 27], can play an important role and responsibility in integrating these discussions and shaping the discussion and reflection on the creations and innovations of XR. As an example, "The Elements of Computer Credibility" by B. J. Fogg was a foundational work for persuasive computing [9], and persuasive design was published at CHI 99 and became the basis for growing research around Dark Design Patterns [13] which nudge users against their personal interests. As a community we need to be more cognizant of the risks posed by our research contributions, and how we might discover, disclose, and mitigate against them. Such an approach necessitates that we work closely across disciplines, in particular across HCI and privacy and security. The workshop organizers already started to engage in a more critical perspective with innovation in the field of XR and HCI by organizing a workshop at CHI 2020 on "Exploring Potentially Abusive Ethical, Social and Political Implications of Mixed Reality Research in HCI" [15]. While the prior workshop explored overall negative implications of XR research through an HCI lens, the here proposed workshop will emphasize in particular novel topics around Security, Privacy and Safety.

3 NOVEL ISSUES AROUND SECURITY, PRIVACY AND SAFETY RESEARCH IN XR

In the following, we provide a short classification and give examples for novel security, privacy and safety topics that are currently arising in the XR context. They do not represent an exhaustive list but rather work as a guideline for the reader and authors of workshop submissions to understand our perspective on this arising field of research.

Privacy can be seen from two perspectives for XR technology: the user and the bystander. Privacy concerns around the user are often exploring what potential risks arise from the availability of processed data derived from XR sensing (e.g. optical, auditory, and physiological sensing, EEG for brain activity etc.). Such data has immediate implications for biometric identification and anonymity, for example being able to uniquely identify a user based on gait or movement alone [21, 22]. But this data can also contribute to much deeper violations of mental privacy [16], enabling the surveillance of behaviors, actions, attention etc. The other perspective is exploring how world-facing XR sensors (cameras, microphone arrays and so on) could potentially impact the bystander who is often a non-involved third party that did not agree to be surveiled or sensed by such technology. Rixen et al. presented at CHI 2021 one of the first works that explored how a bystander feels about the fact that an XR user has the potential to augmented and change their visual appearance as they please [25]. Both perspectives are raising new questions regarding the potential erosion of the concept of privacy in a future where always available XR technology sees mass adoption, and in what ways we might head off such an eventuality.

Safety For XR technology we divide Safety into two perspectives: *physical safety* and *psychological safety*. Dao. et al., presented in their recent CHI 2021 publication [7] a structured analysis of why fails and breakdowns in VR are happening and how the safety mechanisms of current VR systems could be improved (which in itself became to get a field of interest for HCI and XR researchers [8]). O'Hagan et al. uncovered the unique contribution that bystanders have to VR safety – having significant, and potentially abusive, power over the VR user [23]. The psychological perspective of safety is focusing on how immersive experience and perceptual realism [28] could potentially traumatize and harm the user long term and how we could avoid it. While a large amount of research has explored how XR (or here in particular VR) can be used to positively impact user's mental health (e.g., being used in trauma therapy [4]), more research started to explore how the same benefits of presence could lead to potentially more traumatic experiences [31]. Relatedly, manipulation of reality through XR may lead to societal implications, for instance, when XR users are presented with scenes of prosperity hiding signs of poverty [20]

Security in the field of Computer Science focuses traditionally on protecting some forms of computing systems from malicious actors. These topics are still relevant and important in the age of XR technology [12, 18, 26, 27]. However, one very important new aspect starts to arise at the intersection between Safety and Security which feels quite unique to XR and HCI research: *immersive attacks*.

Immersive attacks have the goal to negatively impact the users physiological and psychological safety but are doing so by creating a directed attack towards the user and their perception rather than focusing on the underlying hardware or software. These types of attacks are leveraging perceptional thresholds towards certain types of illusions that are published within the field of HCI and XR [3, 30] to imperceptibly manipulate an immersed user towards harm [5]. These types of attacks are only recently gaining interest and can be expected to grow in relevance with an even further distribution of the technology. One important realization of these types of security threats is that unlike traditional security issues, the human perception can not be easily patched. Once we understand what type of illusions or "tricks" we are able to apply to manipulate an immersed user without their knowledge, we need to start to create a new layer on top of the users perception that is able to detect and prevent such manipulations.

4 WORKSHOP GOALS

This workshop will bring together scientists and industry attendees from multiple disciplines to discuss and reflect on these problems and challenges of XR adoption and usage. We will focus on engaging the HCI community more in this discussion and try to understand its role and responsibility in the future of XR research. The community we will form through this workshop, and insights of the day, could serve as a foundation to start to define more clearly what types of challenges are novel at this intersection of three fields and how can we start addressing them. We will start working towards a joint definition of these novel challenges. The deeper exploration of privacy, security, and safety issues arising in XR will facilitate the development of an integrative research agenda for XR.

5 WORKSHOP AREAS OF INTEREST

We will focus on fundamental challenges of Safety, Security and Privacy research which are arising with XR technology, using an HCI lens. This means that the topics are grounded in three fields we presented in Section 3 but are not limited to them. Since this intersection is only very recently becoming part of the scientific discussion, we expect a multitude of topics which will arise that we were not able to predict. We will especially encourage participation from members of the research and practitioner communities working at the intersection of these areas.

- Privacy implications for XR users
- Privacy implications for bystanders in XR
- Safety concerns around physiological harm to the XR user
- Safety concerns around psychological harm to the XR user
- Security challenges for future XR technology
- Security challenges on manipulating the XR user
- Societal implications of XR technology

6 PARTICIPANTS AND EXPECTED INTEREST

We welcome participants from all fields of HCI, Extended Reality and Safety, Security and Privacy – researchers, designers and practitioners, social scientists, psychologists, ethicists, and philosophers – provided they have some understanding and background of XR technologies. The workshop is inclusive for a non-technical audience. Participants with basic knowledge in XR, HCI, and Safety, Security and Privacy research will be able to follow and participate in the discussions.

7 PRE-WORKSHOP PLANS

We will distribute a Call for Papers in all relevant communities, announcing the CfP on popular mailing lists, e.g. ACM, CHI-announcements, Safety Security and Privacy mailing lists) and social media. We will also directly contact researchers and practitioners who are likely to be interested in the workshop and write to relevant institutions and research labs. The workshop website, located at https://wenjietseng.com/sspxr/, will act as an public repository for materials and outcomes of the workshop. Additionally, we plan to create a Slack channel where participants are able to connect and discuss asynchronously before and throughout the workshop.

8 WORKSHOP STRUCTURE

The workshop will revolve heavily around interactive discussions which will be facilitated within three panel sessions, each focusing on topics and themes that are representing the submissions. Participants will be invited to submit either a 2-page position statement or a 4-page research statement and will each get the opportunity to present their work in a 5 minute talk as part of their panel session. Each panel session will start with introductions and short paper presentations, followed by a panel discussion, including audience questions. The panel will consist of one author of each submission, and one organizer and or external expert. The external experts will be invited to add further expert perspectives to the discussion. Organizers will moderate the panel and facilitate the discussion. The workshop will end with a final discussion panel consisting of volunteers of the former sessions and a subset of organizers and external experts.

The workshop is planned as a one-day virtual event. This helps us to be able to engage and lead a discussion with attendees that will not travel to CHI 2022. As an infrastructure we will use the streaming service provided by CHI 2022 or alternatively setup own instances of Big Blue Button or Zoom. The discussion during the panels will work as the main form of engaging with the individual topics. All participants will be able to contribute to the discussion by raising hands or writing in the chat. Throughout the panel discussion, multiple organizers will monitor the chat and help participants raise questions and participate in the discussion.

The tentative schedule for the workshop is as follows:

09:00 - 09:15	Welcome
09:15 - 10:00	Opening Keynote by Prof. Dr. Franziska Roesner
10:00 - 10:15	Break
10:15 - 11:45	Session 1 (4 Talks) + Panel
11:45 - 12:45	Lunch
12:45 - 14:15	Session 2 (4 Talks) + Panel
14:15 - 14:30	Break
14:30 - 16:00	Session 3 (4 Talks) + Panel
16:00 - 16:15	Break

16:15 - 17:00 Reflection and Overall discussion with panelists and workshop participants
17:00 Wrap Up

9 CALL FOR PARTICIPATION

We invite two types of submissions: a 2-page position statement or a 4-page research statement. The 2-page position statement can be a motivation of interest and present an opinion piece or critical position that fits into the larger discussion and topics of the workshop (contribution type "Opinion" as defined by Wobbrock and Kienz [32]). The 4-page research statement can be a presentation of already ongoing or planned research work in the topics of the workshop.

Exemplar topics might come from within the field of, but are not limited to:

- Privacy implications for the user of XR
- Privacy implications for bystanders in XR
- Safety concerns around physiological harm to the XR user
- Safety concerns around psychological harm to the XR user
- Security challenges for future XR technology
- Security challenges on manipulating the XR user
- Immersive Attacks and Human Perceptual Hacking
- Societal implications of XR technology

Once accepted, one author will have the chance to present their work in a 5-minute talk, followed by participation in a 45 minute panel discussion around the topic of the submission. The workshop will consist of three panel session, each consisting of four authors, one organizer and one external expert. We are highly encouraging submissions that are presenting new perspectives on XR, HCI and Safety, Security and Privacy. Submissions are not expected to be finished research projects but should be seen more as motivational and/or provocative piece. The workshop organizers aim for a mix of participants in terms of experience and research topics to maximize diversity of interests and viewpoints at the workshop.

Please note that one author of each accepted position paper must attend the workshop. Attendance can be either in person or remote. All workshop participants must register for both the workshop and for at least one day of ACM CHI 2022. For more information and submitting your contributions, please visit: https://wenjietseng.com/sspxr/

10 EXPECTED OUTCOMES AND POST-WORKSHOP PLANS

The strong focus on discussions will result in three highly-focused panels around a certain topic of novel challenges of Safety, Security and Privacy in XR. Since we aim to arrange the panels to each have on external expert and represent a cross section of three fields, we hope that this material will find interest in all three research domains and could be able to gather new researchers starting to work on these particular topics.

11 ORGANIZERS

Jan Gugenheimer (www.gugenheimer.com) is an Assistant Professor at the Institute Polytechnique de Paris. His research focuses around upcoming social challenges for mixed reality technology and how to embed XR into the fabric of our daily lives.

Wen-Jie Tseng (www.wenjietseng.com) is a 2nd year PhD student at Telecom Paris, Institute Polytechnique de Paris. His research explores safety issues in XR, particularly focusing on physical harm in VR.

Abraham Mhaidli (www.mhaidli.github.io) is a PhD Candidate at the School of Information at the University of Michigan. His research explores ethical issues in Extended Reality (XR) contexts, with a particular focus on XR advertising.

Jan-Ole Rixen (https://www.uni-ulm.de/in/mi/institut/mitarbeiter/jan-rixen/) is a 3rd year PhD student at Ulm University in Germany. His research focuses on exploring how the introduction of XR and the ability to augment people can impact interpersonal communication.

Mark McGill (www.markmcgill.co.uk) is a lecturer (assistant professor) in the School of Computing Science at the University of Glasgow. His research explores the future of XR productivity (e.g. virtual workspaces, ergonomics, augmented peripherals) and XR-enabled passenger experiences.

Michael Nebeling (www.michael-nebeling.de) is an Assistant Professor at the University of Michigan. In his prior research, he developed novel XR prototyping methods and tools with the goal of empowering novice XR content creators. In his current work, he studies how to best guide XR designers in creating safe and inclusive XR experiences.

Mohamed Khamis (www.mkhamis.com) is an Assistant Professor at the University of Glasgow. His research is at the intersection of Human-Computer Interaction and Security. He is interested in understanding the privacy, security and ethical challenges in XR and proposing novel solutions to mitigate said challenges.

Florian Schaub (https://www.si.umich.edu/people/florian-schaub) is an Assistant Professor at the University of Michigan. His research is at the intersection of privacy, security, human-computer interaction, and public policy. He is interested in understanding the privacy and safety implications of emerging technologies such as XR and advance human-centric solutions for safe user experiences.

Sanchari Das (https://www.drsancharidas.com/) is an Assistant Professor at the department of Computer Science in the Ritchie School of Engineering and Computer Science at University of Denver. Her research lab - Security and Privacy Research in New-Age Technology (SPRINT) focuses on computer security, privacy, education, human-computer interaction, social computing, accessibility, and sustainability of new-age technologies.

REFERENCES

[1] [n. d.]. PrXR: towards a roadmap for privacy and security research for mixed reality applications. https://jainlab.cise.ufl.edu/PrXR_2021.html

[2] [n. d.]. Security for XR and XR for security (soups'21 workshop). https://www.afxr.org/articles/74443-security-for-xr-and-xr-for-security-soups-21-workshop-cfp

[3] Mahdi Azmandian, Mark Hancock, Hrvoje Benko, Eyal Ofek, and Andrew D. Wilson. 2016. Haptic Retargeting: Dynamic Repurposing of Passive Haptics for Enhanced Virtual Reality Experiences. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 1968–1979. https://doi.org/10.1145/2858036.2858226

[4] Poppy Brown, Felicity Waite, Aitor Rovira, Alecia Nickless, and Daniel Freeman. 2020. Virtual reality clinical-experimental tests of compassion treatment techniques to reduce paranoia. *Scientific Reports* 10, 1 (2020), 1–9.

[5] Peter Casey, Ibrahim Baggili, and Ananya Yarramreddy. 2021. Immersive Virtual Reality Attacks and the Human Joystick. *IEEE Transactions on Dependable and Secure Computing* 18, 2 (2021), 550–562. https://doi.org/10.1109/TDSC.2019.2907942

[6] Alan Cheng, Lei Yang, and Erik Andersen. 2017. Teaching language and culture with a virtual reality game. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 541–549.

[7] Emily Dao, Andreea Muresan, Kasper Hornbæk, and Jarrod Knibbe. 2021. *Bad Breakdowns, Useful Seams, and Face Slapping: Analysis of VR Fails on YouTube*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445435

[8] Sarah Faltaous, Joshua Neuwirth, Uwe Gruenefeld, and Stefan Schneegass. 2020. SaVR: Increasing Safety in Virtual Reality Environments via Electrical Muscle Stimulation. In *19th International Conference on Mobile and Ubiquitous Multimedia*. 254–258.

[9] B. J. Fogg and Hsiang Tseng. 1999. The Elements of Computer Credibility. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Pittsburgh, Pennsylvania, USA) *(CHI '99)*. Association for Computing Machinery, New York, NY, USA, 80–87. https://doi.org/10.1145/302979.303001

[10] Nisal Menuka Gamage, Deepana Ishtaweera, Martin Weigel, and Anusha Withana. 2021. So Predictable! Continuous 3D Hand Trajectory Prediction in Virtual Reality. In *The 34th Annual ACM Symposium on User Interface Software and Technology* (Virtual Event, USA) *(UIST '21)*. Association for Computing Machinery, New York, NY, USA, 332–343. https://doi.org/10.1145/3472749.3474753

[11] Simson Garfinkel and Heather Richter Lipford. 2014. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust* 5, 2 (2014), 1–124.

[12] Ceenu George, Mohamed Khamis, Daniel Buschek, and Heinrich Hussmann. 2019. Investigating the Third Dimension for Authentication in Immersive Virtual Reality and in the Real World. In *2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. 277–285. https://doi.org/10.1109/VR.2019.8797862

[13] Colin M Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L Toombs. 2018. The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–14.

[14] Jan Gugenheimer. 2016. Nomadic virtual reality: Exploring new interaction concepts for mobile virtual reality head-mounted displays. In *Proceedings of the 29th Annual Symposium on User Interface Software and Technology*. 9–12.

[15] Jan Gugenheimer, Mark McGill, Samuel Huron, Christian Mai, Julie Williamson, and Michael Nebeling. 2020. Exploring Potentially Abusive Ethical, Social and Political Implications of Mixed Reality Research in HCI. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3334480.3375180

[16] Brittan Heller. 2020. Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law. *Vand. J. Ent. & Tech. L.* 23 (2020), 1.

[17] Luv Kohli. 2010. Redirected touching: Warping space to remap passive haptics. In *2010 IEEE Symposium on 3D User Interfaces (3DUI)*. 129–130. https://doi.org/10.1109/3DUI.2010.5444703

[18] Florian Mathis, John H. Williamson, Kami Vaniea, and Mohamed Khamis. 2021. Fast and Secure Authentication in Virtual Reality Using Coordinated 3D Manipulation and Pointing. *ACM Trans. Comput.-Hum. Interact.* 28, 1, Article 6 (jan 2021), 44 pages. https://doi.org/10.1145/3428121

[19] Mark Mcgill, Aidan Kehoe, Euan Freeman, and Stephen Brewster. 2020. Expanding the bounds of seated virtual workspaces. *ACM Transactions on Computer-Human Interaction (TOCHI)* 27, 3 (2020), 1–40.

[20] Abraham Hani Mhaidli and Florian Schaub. 2021. *Identifying Manipulative Advertising Techniques in XR Through Scenario Construction*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445253

[21] Mark Roman Miller, Fernanda Herrera, Hanseul Jun, James A Landay, and Jeremy N Bailenson. 2020. Personal identifiability of user tracking data during observation of 360-degree VR video. *Scientific Reports* 10, 1 (2020), 1–10.

[22] Alec G. Moore, Ryan P. McMahan, Hailiang Dong, and Nicholas Ruozzi. 2021. Personal Identifiability of User Tracking Data During VR Training. In *2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. 556–557. https://doi.org/10.1109/VRW52623.2021.00160

[23] Joseph O'Hagan, Julie R Williamson, Mark McGill, and Mohamed Khamis. 2021. Safety, Power Imbalances, Ethics and Proxy Sex: Surveying In-The-Wild Interactions Between VR Users and Bystanders. *ISMAR '21: Proceedings of the 2021 IEEE INTERNATIONAL SYMPOSIUM ON MIXED AND AUGMENTED REALITY* (2021).

[24] Sharif Razzaque, David Swapp, Mel Slater, Mary C. Whitton, and Anthony Steed. 2002. Redirected Walking in Place. In *Proceedings of the Workshop on Virtual Environments 2002* (Barcelona, Spain) *(EGVE '02)*. Eurographics Association, Goslar, DEU, 123–130.

[25] Jan Ole Rixen, Teresa Hirzle, Mark Colley, Yannick Etzel, Enrico Rukzio, and Jan Gugenheimer. 2021. *Exploring Augmented Visual Alterations in Interpersonal Communication*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445597

[26] Franziska Roesner and Tadayoshi Kohno. [n. d.]. Security and Privacy for Augmented Reality: Our 10-Year Retrospective. ([n. d.]).

[27] Franziska Roesner, Tadayoshi Kohno, and David Molnar. 2014. Security and privacy for augmented reality systems. *Commun. ACM* 57, 4 (2014), 88–96.

[28] Mel Slater, Cristina Gonzalez-Liencres, Patrick Haggard, Charlotte Vinkers, Rebecca Gregory-Clarke, Steve Jelley, Zillah Watson, Graham Breen, Raz Schwarz, William Steptoe, et al. 2020. The ethics of realism in virtual and augmented reality. *Frontiers in Virtual Reality* 1 (2020), 1.

[29] Frank Steinicke, Gerd Bruder, Jason Jerald, Harald Frenz, and Markus Lappe. 2010. Estimation of Detection Thresholds for Redirected Walking Techniques. *IEEE Transactions on Visualization and Computer Graphics* 16, 1 (2010), 17–27. https://doi.org/10.1109/TVCG.2009.62

[30] Qi Sun, Anjul Patney, Li-Yi Wei, Omer Shapira, Jingwan Lu, Paul Asente, Suwen Zhu, Morgan Mcguire, David Luebke, and Arie Kaufman. 2018. Towards Virtual Reality Infinite Walking: Dynamic Saccadic Redirection. *ACM Trans. Graph.* 37, 4, Article 67 (July 2018), 13 pages. https://doi.org/10.1145/3197517.3201294

[31] Graham Wilson and Mark McGill. 2018. Violent Video Games in Virtual Reality: Re-Evaluating the Impact and Rating of Interactive Experiences. In *Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play* (Melbourne, VIC, Australia) *(CHI PLAY '18)*. Association for Computing Machinery, New York, NY, USA, 535–548. https://doi.org/10.1145/3242671.3242684

[32] Jacob O Wobbrock and Julie A Kientz. 2016. Research contributions in human-computer interaction. *interactions* 23, 3 (2016), 38–44.