Check for updates

NIST Internal Report
NIST IR 8557

Report of the Virtual Workshop on Usable Cybersecurity and Privacy for Immersive Technologies

Michael Fagan
Dylan Gilbert

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8557

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Internal Report
NIST IR 8557

Report of the Virtual Workshop on Usable Cybersecurity and Privacy for Immersive Technologies

Michael Fagan
Dylan Gilbert*
Applied Cybersecurity Division
Information Technology Laboratory

*Former NIST employee; all work for this
publication was done while at NIST.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8557

May 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2025-05-15

How to Cite this NIST Technical Series Publication
Fagan M, Gilbert D (2025) Report of the Virtual Workshop on Usable Cybersecurity and Privacy for Immersive Technologies. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8557. https://doi.org/10.6028/NIST.IR.8557

Author ORCID iDs
Michael Fagan: 0000-0002-1861-2609
Dylan Gilbert: 0009-0003-6061-3757

Contact Information
immersivetech@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information
Additional information about this publication is available at https://csrc.nist.gov/pubs/ir/8557/final, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This document reports on the Virtual Workshop on Usable Cybersecurity and Privacy for Immersive Technologies (the Workshop) hosted by the Symposium in Usable Privacy and Security (SOUPS). The Workshop was held on August 7th, 2024 before the in-person symposium held August 11th and 12th, 2024 in Philadelphia, Pennsylvania. The Workshop consisted of a keynote presentation, two research report presentations, and a panel discussion. This document reports on the Workshop to share the ideas and insights with the broader community.

Keywords

augmented reality; cybersecurity; human factors; immersive technologies; mixed reality; privacy; virtual reality.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Table of Contents

1. Introduction

Advances in computer vision, data processing, and other technologies has laid the foundation for novel virtual reality (VR), augmented reality (AR), and mixed reality (MR) solutions, collectively called immersive technologies. Immersive technologies are hardware and software systems that create interactive digital visual/spatial environments. These technologies hold promise to drive innovation and economic growth in numerous areas such as workforce [1], accessibility[1] [2], and healthcare [3], but they challenge existing assumptions and practices for digital technologies [4][5]. Immersive technologies may create cybersecurity and privacy risks, some perhaps novel and unique that will need to be managed, but they may also have potential for cybersecurity and privacy protections and other risk mitigations [5]. All the while, users are at the center of these technologies, making usability considerations for immersive technologies critical for cybersecurity and privacy. For example, certain communication modalities may have different effectiveness for cybersecurity and privacy information delivered via immersive technologies than on traditional display and input modalities. Not considering usability in this context risks users not using or misusing cybersecurity features, privacy features, or the technologies themselves.

With this background, the National Institute of Standards and Technology (NIST) organized the Virtual Workshop on Usable Cybersecurity and Privacy for Immersive Technologies (the Workshop) hosted by the Symposium in Usable Privacy and Security (SOUPS). The Workshop was held on August 7th, 2024 before the in-person symposium held August 11th and 12th, 2024 in Philadelphia, Pennsylvania. The Workshop attracted over two dozen registrants and consisted of a keynote presentation by Dr. Louis Rosenberg titled “Our Next Reality: the Emerging Dangers of our AI-powered Immersive Future,” two research report presentations, and a panel discussion.

This document reports on the virtual workshop to share the ideas and insights with the broader community. The rest of this report documents the event and outlines observations about immersive technologies’ cybersecurity and privacy considerations from the discussions and presentations:

- Next, background is provided on the origins of this virtual workshop.
- Then, the details of the event are documented.
- Then, insights from the virtual workshop are reported.
- Finally, the report is concluded.

[1] In this report the term “accessibility” is used in the context of limiting or removing barriers for individuals with disabilities to use technology, access information and services, and participate in society generally.

2. Background

The Virtual Workshop on Usable Cybersecurity and Privacy for Immersive Technologies was held to explore cybersecurity and privacy related to immersive technologies (i.e., Virtual Reality, Augmented Reality, and Mixed Reality). The Workshop was aimed to help NIST gain insights related to the following research questions:

1. What are the new technologies, use cases, applications, implementations, solutions, etc. related to AR/VR/MR?
2. What privacy and cybersecurity considerations and implications are there for development and adoption of these technologies?
3. What standards and other resources exist for immersive technology cybersecurity and privacy? Are there gaps that can/should be filled?

Before the Workshop, two public-facing deliverables were published to support the project. A NIST blog post announced the project and helped spur engagements with the community. In addition, a "Topics for Feedback" document was posted on the NIST website for easy sharing with the community. The topics highlighted in the document were:

1. Immersive Technology Ecosystem and Use Cases - "[T]he ecosystem of entities that support immersive technologies. This ecosystem encompasses a range of entities and roles that may have complex, multi-directional relationships. Complexity can increase when entities are supported by a chain of sub-entities (e.g., manufacturers supported by multiple component suppliers)."
2. Immersive Technology Ecosystem and Use Cases - "[C]urrent and potential future uses and misuses of immersive technologies across all applicable sectors and user bases, including any barriers to adoption."
3. Privacy and Cybersecurity Risk Considerations - "Immersive technologies may generate cybersecurity and privacy risks, some of which can be novel or mix in complex ways."
4. Immersive Technology Standards and Risk Management Resources - "Immersive technologies may break existing cybersecurity and privacy assumptions, requiring adaptation or update to tools and techniques documented in standards and guidelines. Additionally, immersive technologies may warrant new standards and guidelines efforts to complement existing resources."

Under each of these topics a series of specific questions were listed to guide feedback. The full "Topics for Feedback" document is included in Appendix B of this report.

3. Event Report

SOUPS hosted the Workshop on the afternoon of August 7th, 2024. NIST posted an external event website to promote the Workshop to immersive technology community members, while the organizers of the SOUPS conference also promoted the Workshop in their outreach. Leading up to the Workshop, the community was given the opportunity to submit research or position papers related to one or more of the following topics:

- Usable cybersecurity and privacy considerations for immersive technologies, with particular interest in novel considerations.
- Potential approaches for usable cybersecurity and privacy (e.g., risk mitigations) for immersive technology solutions and use cases.
- Potential usable cybersecurity and privacy mitigations that may utilize immersive technologies to deliver protections.
- How usable cybersecurity and privacy impact, or are impacted by, other trust factors (i.e., safety, resiliency, reliability) for immersive technology solutions and use cases.
- Insights for standards and standards development for immersive technologies and use cases.

These topics were listed and expanded upon in a Call for Papers. The Call for Papers is provided in Appendix C of this report for reference. Two research papers were received and reviewed by the Workshop's Technical Program Committee. Both papers were accepted to be presented at the workshop:

1. Trusted Inter-Reality Infrastructure: Building Trust within Entities (Digest)
    a. Akira Kanaoka, Toho University and Takuro Yonezawa, Nagoya University
2. Understanding the Interdependence of Trust Factors and Usability in Cybersecurity and Privacy for Immersive Technologies
    a. Bhanujeet Choudhary, David Tulacz, Kavya Pearlman, and Nandita Rao Narla, X Reality Safety Intelligence (XRSI)

Both papers are available as Supplemental Content on this document's CSRC page.

The workshop agenda included an opening keynote presentation from Dr. Louis Rosenberg from the Unanimous AI and the Responsible Metaverse Alliance titled, "Our Next Reality: the Emerging Dangers of our AI-powered Immersive Future." Dr. Rosenberg's talk highlighted potential privacy risks of immersive technologies supported by data-fueled artificial intelligence technologies and discussed the way these risks could be amplified by user interface designs (e.g., so-called "dark patterns") and other manipulative algorithm designs.

The keynote was followed by a presentation from an author of each research paper where the authors had an opportunity to gather feedback on and promote their work. The last component of the Workshop was a panel discussion moderated by Dylan Gilbert from NIST and featuring the following panelists:

1. Elizabeth Hyman, President and CEO, XR Association
2. Christopher Lafayette, Emergent Technologist, Gatherverse
3. Jameson Spivack, Senior Policy Analyst for Immersive Technologies, Future of Privacy Forum

The panel provided a lively discussion of current and upcoming trends pertinent to usable cybersecurity and privacy for immersive technologies and gave the audience an opportunity to engage with experts in the immersive technology community.

4. Insights

The Workshop yielded numerous insights organized below around the project's core research areas of immersive technology trends, cybersecurity, privacy, and standards. Additional insights relevant to the immersive tech ecosystem and standards and risk management which did not fit cleanly under the project's core research questions are included as well. Please note that these insights are not formal recommendations from the authors or NIST or represent the consensus of the participants. They are provided to report the various points of view heard at the Workshop.

4.1. Insights Related to Immersive Technology Trends: New Frontiers, but Potential Pitfalls

The community shared many unique aspects of immersive technologies. For example, the types and number of sensors used to power immersive technologies are unique, and research is ongoing into ways to integrate emerging technologies (e.g., incorporating quantum sensors to improve Lidar for 3D modelling). Beneficial current and future use cases were shared as well. In this context, the term *use* case was used quite broadly by the audience and was used to refer to applications of immersive technologies or spaces where there are potential immersive technology applications. Dangerous, impossible, or expensive use cases were identified as being well-suited for immersive technologies. In addition, use cases for immersive technology application are emerging across myriad sectors, including professional training (e.g., surgeons operating on digital cadavers), personalized therapeutic experiences, architecture and construction, and immersive entertainment experiences.

But some points of caution were noted. Participants raised potential safety and behavioral concerns, including some that are novel (e.g., time dilation, immersive cyberbullying and harassment, and VR "hangovers" (i.e., disassociation/derealization)). Discussions highlighted that the scope, scale, and persistence of data processing as well as the scope and scale of inferences and potential for behavioral manipulation associated with immersive technologies (especially when powered by artificial intelligence (AI)) sets it apart from other technologies. Throughout the workshop, consistent connections to AI were drawn by participants, highlighting that AI has a close relationship to immersive technologies. It was argued by some that multi-modal AI is immersive technology. AI agents communicating through audio interface is a likely future use case.

4.2. Insights Related to Cybersecurity and Privacy: Immense Scale and Personal Impact

Many individual considerations for cybersecurity and privacy were discussed. One consistent point of discussion was the scope and scale of data needed to make immersive technologies function. Specifically, the community highlighted that the context in which data processing takes place and privacy and cybersecurity risks arise (i.e., immersive worlds powered by granular biometric, spatial, and behavioral/emotional data) is unique to immersive technologies. Privacy and cybersecurity impacts may be amplified by immersive technologies due to the nature and scale of data processing. Novel types of data processing activities include biometrics for uses other than identity management, real-time spatial mapping, and the combination of user behavioral and physical data. Also, virtual environments require significant amounts of data and similarly significant technological protections for data (e.g., encryption, local or on-device processing). This can present costs and trade-offs (e.g., privacy and security vs. safety).

Another common point was the personal nature of immersive technologies. Immersive technologies can have more precise tailoring of experiences based on emotional states or inferences from behavioral and biometric data. Highly personalized environments can facilitate benefits to privacy and cybersecurity (e.g., "gamifying" privacy and cybersecurity to make it more interesting, understandable, and manageable; use of intelligent, edge-based virtual agents to help users improve their privacy and security outcomes). These tailored experiences can, however, also increase risks of individuals being manipulated in ways which could adversely impact their privacy and the security of their data. Though behavioral norms are important, they are challenging to establish for experiences that may not be currently possible or are in a nascent state (i.e., many experiences and behaviors for immersive technologies are currently speculative). Individuals noted that there is a lack of clarity around consumer expectations of privacy and cybersecurity in immersive environments due to their relative novelty and a current lack of normative and ethical frameworks.

The increasing integration of AI into immersive technologies underscores the importance of managing privacy and cybersecurity risks throughout the data and system development life cycle, but developers may lack incentive or requirements to do so.

Specific to privacy, the following key considerations for immersive technologies were highlighted through discussions. Participants noted that there could be tensions between data minimization requirements and the amount and variety of data needed to power immersive technologies. Also, principles such as consent, user control, and autonomy may be difficult to uphold for involuntary and unconscious or subconscious behaviors or physical acts.

4.3. Insights Related to Standards: Pre-Standardization Research Needed

The community recommended several areas related to immersive technologies that could benefit from additional standardization efforts. Usability is a hurdle for hardware and software standards (e.g., ways to manage multiple accounts within the same device). Identity standards for immersive tech could be helpful to address this. Standards for trustworthy AI (e.g., watermarking and other content authentication) would be welcomed.

In discussions, a number of specific areas for pre-standardization research that NIST could support were brought to the fore, such as taxonomies (i.e., terms/definitions) that are tied to specific use cases. Participants noted that a shared taxonomy of data types and accompanying risks could also be useful. Additional topics related to standards that were noted were measurement of accuracy/efficacy of immersive tech and associated impacts and the development of a typology of risk.

4.4. Additional Insights: Challenging the Landscape with Unique Use Cases and Considerations

Some insights did not fit cleanly into the areas above. It was highlighted that sectors have specific considerations. The education sector is a rapidly growing part of the immersive technologies ecosystem, but gaps in teacher and learner knowledge and understanding about the technologies (e.g., their educational value, how they can be used, and potential risks) is a barrier to adoption. There is noted growth in healthcare applications as well. For example, large hospitals are training physicians on immersive technologies for pain mitigation, stroke rehab, and stress treatment. Wearable sensors are capturing biological signals related to attention and behavior. This can help with psychiatry and psychology and to assist with treating physical impairments such as vision, hearing, or speech.

Human-focused considerations were also discussed. Legal and regulatory requirements related to accessibility may not translate well to immersive technologies, potentially creating barriers to federal government procurement. Ownership or control over the technologies was noted to have implications for impact on individuals. For example, the subscription model has different effects (potentially more adverse for individuals) than ownership models.

It was also noted that some aspects of the immersive technology ecosystem may be centralized (i.e., the same organizations making hardware, software, and applications). This has the possibility to create benefits to privacy and cybersecurity but may raise concerns around market diversity, competition, and potential limitations and drawbacks for consumers.

While immersive technologies raise some unique cybersecurity and privacy considerations, existing NIST risk management guidelines, tools, and resources can support risk-based and ethical decision-making in the development and use of immersive systems, products, and services. A current lack of ethical and normative frameworks specifically for immersive technologies may introduce challenges to understanding individuals’ expectations of privacy and the security of their data in immersive environments, but development of such frameworks falls outside of NIST’s purview. Incentives are a key driver in cybersecurity and privacy best practices. This underscores the importance of lowering technical barriers to adoption of technologies that may be useful for managing risks in immersive environments (e.g., privacy-enhancing technologies), while also acknowledging non-technical considerations that may disincentivize effective risk management, such as legal uncertainty, knowledge gaps, market consolidation, etc.

5. Conclusion

Immersive technologies pose great benefits for the nation and may be critical to several sectors in the future such as education, industrial maintenance, and entertainment. That said, many aspects of the technology space and standards are nascent, hindering specific discussion of cybersecurity and privacy. Though there are questions that need consideration related to cybersecurity and privacy of immersive technologies, as noted in the Section 4, existing NIST risk management guidelines, tools, and resources can support risk-based and ethical decision-making in the development and use of immersive systems, products, and services. Thus, participants in immersive technology ecosystems (e.g., product manufacturers and providers, supporting service providers, institutional and individual users) can leverage the existing NIST cybersecurity and privacy portfolio, either directly or through tailoring and profiling. Through this mechanism, as NIST has done before, practical application of cybersecurity and privacy risk management can be supported in the near term with new projects and research directions potentially identified through continued community engagement.

References

[1] XR Association (2025) Education in XR. (XR Association, Washington, D.C.). Available at https://xra.org/wp-content/uploads/2023/05/XRA_Slicks_Education_V1.pdf-1.pdf

[2] XR Association (2025) Inclusive XR. (XR Association, Washington, D.C.). Available at https://xra.org/wp-content/uploads/2023/05/XRA_Slicks_Accessibility_V3.pdf-1.pdf

[3] XR Association (2025) XR Technology and Healthcare. (XR Association, Washington, D.C.). Available at https://xra.org/wp-content/uploads/2023/05/XRA_Slicks_Healthcare_V2.pdf-1.pdf

[4] Santos, N. M., & Peslak, A. (2022). Immersive technologies: Benefits, timeframes, and obstacles. Issues in Information Systems, 23(2). https://iacis.org/iis/2022/2_iis_2022_170-184.pdf

[5] Giaretta, A. (2024). Security and privacy in virtual reality: a literature survey. Virtual Reality, 29(1), 10. https://link.springer.com/content/pdf/10.1007/s10055-024-01079-9.pdf

Appendix A. List of Symbols, Abbreviations, and Acronyms

AI
Artificial Intelligence

AR
Augmented Reality

MR
Mixed Reality

SOUPS
Symposium on Usable Privacy and Security

VR
Virtual Reality

XRSI
X Reality Safety Intelligence

Appendix B. Topics for Feedback Distributed Before the Workshop

Immersive Technologies Cybersecurity and Privacy Topics for Feedback

I. Background

Advances in computer vision, data processing, and other technologies have enabled novel Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR) solutions, collectively called immersive technologies. In general, immersive technologies are hardware and software systems that create interactive digital visual and spatial environments that users can inhabit. These immersive environments can vary in the extent to which they incorporate virtual components. For example, AR layers digital objects over the user's "real-world" environment, while VR can transport users to an entirely virtual alternate environment. These technologies hold promise to drive innovation and economic growth in numerous areas such as workforce, accessibility, and healthcare. Their creation and use can, however, generate cybersecurity and privacy risks, some of which may be novel.

These new technologies have interdisciplinary and integrative implications as well. They mix knowledge and approaches from myriad fields, such as neuroscience, psychology, behavioral studies, and statistics. Further, their integration with other emergent technologies like Artificial Intelligence (AI) and Internet of Things (IoT) adds complexity to the unique context in which cybersecurity and privacy risks can arise and will need to be managed.

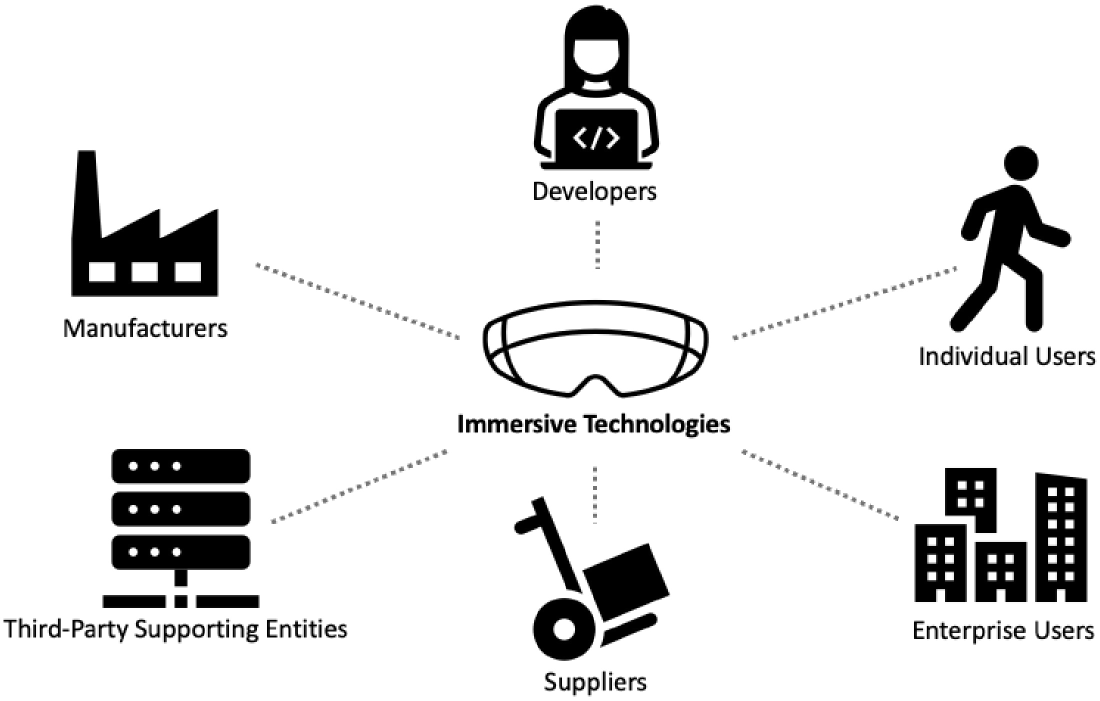
With these motivations, NIST aims to learn more about potential cybersecurity and privacy considerations associated with immersive technologies. We seek comment or feedback on a variety of topics (described below) to help inform future research and development of guidelines, tools, and other resources to support effective privacy and cybersecurity risk management for immersive technologies.

NIST will gather feedback on these topics at a variety of roundtables, meetings, workshops, and other engagements, but we also welcome direct feedback via our email: immersivetech@nist.gov. Updated information on this workstream is available at https://www.nist.gov/securing-emerging-technologies.

II. Topics for Feedback

Respondents can address one or more of the following topics and need not respond to all topics.

A. Immersive Technology Ecosystem and Use Cases



NIST seeks comment on the ecosystem of entities that support immersive technologies. This ecosystem encompasses a range of entities and roles that may have complex, multi-directional relationships. Complexity can increase when entities are supported by a chain of sub-entities (e.g., manufacturers supported by multiple component suppliers). In particular, NIST seeks stakeholder feedback on the following topics:

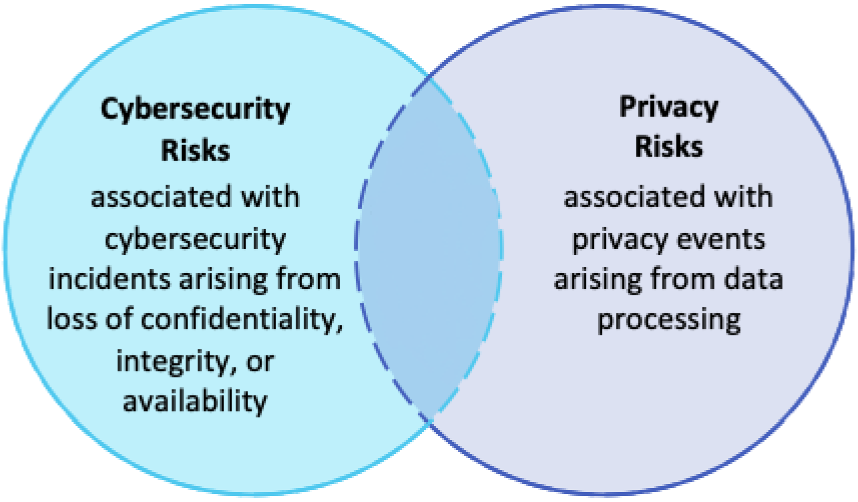
1. Types of entities and roles (e.g., manufacturer, developer, customer, user, and business partners) that characterize the immersive technologies ecosystem
2. Ways in which the immersive technologies ecosystem is unique from other data processing ecosystems

NIST also seeks comments on current and potential future uses and misuses of immersive technologies across all applicable sectors and user bases, including any barriers to adoption. In particular, NIST seeks stakeholder feedback on the following topics:

3. Current and potential future use cases for immersive technologies, including benefits to innovation and to the public interest
4. The role(s) of emergent technologies (e.g., AI, IoT, blockchain, etc.) in current or potential future immersive technology use cases
5. The role(s) that emerging, but nascent, technologies (e.g., quantum computing, brain-computer interfaces) could play in potential future immersive technology use cases

6. Ways in which immersive technologies could be misused, including potential harms such misuse could create for individuals or groups
7. Barriers (e.g., technical limitations, costs, usability, etc.) that hinder the development or deployment of current and future immersive technologies

B. Privacy and Cybersecurity Risk Considerations


Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
Privacy Risks
associated with privacy events arising from data processing

Cybersecurity and privacy risks are distinct but can overlap, as illustrated in the Venn diagram above.[2] For example, data confidentiality may be both a cybersecurity and privacy consideration for a system. But system availability considerations may not involve privacy, while secondary use of information derived from user engagement may not involve system cybersecurity. Immersive technologies may generate cybersecurity and privacy risks, some of which can be novel or mix in complex ways. NIST seeks comment on this topic, including the following:

1. Examples of cybersecurity or privacy risks associated with immersive technologies
2. Cybersecurity or privacy risks that are unique or novel to immersive technologies
    a. If such risks exist, factors that make them unique or novel (e.g., the type(s) or characteristics of data processed, the context in which the data is processed, etc.)
3. Ways in which immersive technologies can improve cybersecurity or privacy outcomes
4. New technological, organizational, or societal approaches to cybersecurity and privacy that are available or needed for immersive technologies
5. Ways in which the use of machine learning and other AI techniques or systems impact cybersecurity and privacy risks for immersive technologies
6. Ways in which delivery of other trust factors or engineering objectives (i.e., privacy, safety, resiliency, reliability) rely on, or are hindered by, cybersecurity in the context of immersive technologies

[2] For more information on the relationship between cybersecurity and privacy risk, see, e.g., *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0* (2020), at p. 2. Available at https://doi.org/10.6028/NIST.CSWP.01162020.

   a. Ways, if any, that cybersecurity enables immersive technologies to be privacy-, and safety-preserving, resilient, and reliable for users
   b. Ways, if any, that cybersecurity when applied to immersive technologies may be detrimental to privacy, safety, resiliency, or reliability
7. How traditional privacy principles (e.g., data minimization) are applied in the context of immersive technologies
   a. Ways in which these technologies support privacy principles or pose challenges to upholding privacy principles
8. How security and privacy engineering objectives are applied in the context of immersive technologies
9. Risk mitigations for privacy and cybersecurity for immersive technologies
   a. The role(s) of privacy enhancing technologies (e.g., differential privacy, secure multi-party computation, privacy-preserving federated learning, etc.) in managing risks associated with immersive technologies
10. The extent to which immersive technologies impact the cybersecurity and privacy workforce, including examples of potential benefits and problems
11. The regulatory landscape and the relationship (whether positive or deficient) to managing privacy and cybersecurity risk

C. Immersive Technology Standards and Risk Management Resources

Standards and guidelines play a critical role in cybersecurity and privacy. Immersive technologies may break existing cybersecurity and privacy assumptions, requiring adaptation or update to tools and techniques documented in standards and guidelines. Additionally, immersive technologies may warrant new standards and guidelines efforts to complement existing resources. To inform NIST’s understanding of these considerations, NIST seeks comment on the following:

1. The current state of standards and standards development for immersive technologies
2. NIST’s role in supporting development of standards for immersive technologies
3. NIST’s role in supporting effective risk management for immersive technologies through guidelines, resources, and tools

D. Other Topics and Considerations

NIST welcomes stakeholder feedback on any other topics and considerations related to immersive technologies.

Appendix C. Virtual Workshop's Call for Papers

Call for Papers: Virtual Workshop on Usable Cybersecurity and Privacy for Immersive Technologies

Advances in computer vision, data processing, and other technologies has laid the foundation for novel virtual reality (VR), augmented reality (AR), and mixed reality (MR) solutions, collectively called immersive technologies. Immersive technologies are hardware and software systems that create interactive digital visual/spatial environments. These technologies hold promise to drive innovation and economic growth in numerous areas such as workforce, accessibility, and healthcare, but they challenge existing assumptions and practices for digital technologies. For example, large amounts of data may be collected from or about people to create digital worlds or augment the real world, and users can interact with immersive technologies in different ways than other technologies. Cybersecurity and privacy related to immersive technologies must be considered carefully. Immersive technologies may create cybersecurity and privacy risks, some perhaps novel and unique that will need to be managed, but they may also have potential for cybersecurity and privacy protections and other risk mitigations. All the while, users are at the center of these technologies, making usability considerations for immersive technologies critical for cybersecurity and privacy. For example, certain communication modalities may be more (e.g., audio/visual) or less (e.g., menus, text) effective for cybersecurity and privacy information delivered via immersive technologies. Not considering usability in this context risks users not using or misusing cybersecurity features, privacy features, or the technologies themselves. This virtual workshop will explore these technologies and the cybersecurity and privacy considerations they introduce. We invite submissions on the following topics:

- Usable cybersecurity and privacy considerations for immersive technologies, with particular interest in novel considerations.
- Potential approaches for usable cybersecurity and privacy (e.g., risk mitigations) for immersive technology solutions and use cases.
- Potential usable cybersecurity and privacy mitigations that may utilize immersive technologies to deliver protections.
- How usable cybersecurity and privacy impact, or are impacted by, other trust factors (i.e., safety, resiliency, reliability) for immersive technology solutions and use cases.
- Insights for standards and standards development for immersive technologies and use cases.

Submissions will be judged based on their applicability to one or more of the topics above, the novelty of the work, quality of the submission, and relevance of the contribution to the field. We solicit papers describing new research contributions in this area as well as case studies, work in progress, preliminary results, novel ideas, and position papers.

Papers should be at most six pages (excluding references) using the SOUPS template format (MS Word or LaTeX). Submissions should be emailed to immersivetech@nist.gov.

A word about paper length. Papers should be succinct, but thorough in presenting the work. Typical papers will be 5-6 pages long (plus references), but papers can be shorter (e.g. 2-3 pages) if, for example, they present a novel idea with limited preliminary results or a position likely to drive a lively discussion. Shorter, more focused papers are encouraged and will be reviewed like any other paper. If you only need 2 or 4 pages (plus references) to clearly explain your work or idea, please submit a paper of that length. Reviewers will be instructed to assess the value of the talk to the workshop audience irrespective of the paper length; however, we stress again that the presentation should be sufficiently thorough for reviewers to make this evaluation.

Workshop papers will be made available to attendees prior to the workshop. However, they will not appear in the official SOUPS proceedings. Paper presentations will be approximately 10-12 minutes in length followed by 5 minutes of questions and answers. Presentations must be made remotely as this will be a virtual workshop.

The deadline for submissions is May 23 23:59 AoE (Anywhere on Earth).

Notification of acceptance will be sent to authors by June 6.

The deadline for camera-ready versions of accepted submissions is June 20 23:59 AoE (Anywhere on Earth).

The workshop will be held virtually on August 7 from 13:00 to 17:00 EST.

You can find out more at our event page or by emailing immersivetech@nist.gov.