Rountable 03

Privacy & Data

September 22nd, 2023

Meta • Artificial Intelligence Institute of Seoul National University • XR Hub Korea • Metaverse • Privacy • Transparency • Regulation • Governance • Privacy expectation • Data protection • Contextual expectation • Technology as data protection • Data minimization • Data retention • Anonymity • Conditional privacy • Biometric data • Privacy rights for avatars • Geography • User empowerment • Data autonomy • In-context notifications •

PARTICIPANTS

Moderator

Yong Lim

Director, SNU AI Policy Initiative
Associate Professor, School of Law, Seoul National University

Presenters

Sangchul Park

Assistant Professor, School of Law, Seoul National University

Taja Naidoo

Privacy Public Policy Manager, Policy Solutions at Meta

Experts (A~Z)

Arianne Jimenez

Head of Privacy & Data Policy, Engagement, APAC at Meta

B M Mainul Hossain

Professor, Institute of Information Technology (IIT), University of Dhaka

Byoung-Pil Kim

Professor, Graduate School of Innovation and Technology Management, KAIST

Hiroshi Miyashita

Professor, Chuo University

Irish Salandanan-Almeida

Chief Privacy Officer, Globe Telecom, Inc.

Jo-Fan Yu

Partner, Baker & McKenzie

Suat Hong Koh

Deputy Director (Data Tech), Personal Data Protection Commission, Singapore

Thitirat Thipsamritkul

Lecturer, Faculty of Law, Thammasat University

Meta and the Artificial Intelligence Institute of Seoul National University (AIIS) conducted the third in a series of four roundtable discussions, focused on building the metaverse responsibly. The third roundtable discussion was on "Privacy & Data", with the last scheduled roundtable slated to focus on Safety & Well-being.

Taja Naidoo (Public policy manager, TTC Labs & Policy Solutions at Meta) presented on "Data Transparency & Controls in the Metaverse". Sangchul Park (Assistant Professor, School of Law, SNU) presented on "Privacy in the Context of XR".

The discussion was moderated by Yong Lim (Director, Seoul National University AI Policy Initiative; Associate Professor, School of Law, Seoul National University). 10 experts from 9 countries across the Asia Pacific region shared their views on the following questions:

1. **Does privacy have different meanings?**
2. **How do user expectations of privacy change (or remain the same) in immersive environments, the Metaverse?**
3. **How can we then help people understand how data is collected and used in the Metaverse?** In relation to this, transparency about how data is used in the metaverse is key to building trust, but people can be easily overwhelmed by too much information. How do we best balance transparency and user experiences?
4. **How might we harness the opportunities for empowering people with in-context control presented to us by 3D interaction?** What other vehicles or methods for collaboration between industry, academia and civil society exist or should be created to enhance cooperation in building the Metaverse responsibly, especially with regard to privacy, transparency, consent, and control?
5. **How should people be informed about the use of body based data in XR devices?**
6. **Should we and how might we create private spaces in the Metaverse?**

1 Does privacy have different meanings?

Privacy expectations will mimic those in the real world, in that they will be context-based. However, technological advancements and generational differences can impact privacy sensitivity. The challenge becomes understanding user expectations of privacy and properly informing users how their data may be processed through XR technologies for the purpose of providing certain services.

2 How do users' expectations of privacy change or remain the same in immersive environments, and the Metaverse?

The fundamental privacy expectations that apply to traditional digital services will largely remain the same in the Metaverse, in that users will continue to expect their data to be handled with care and responsibility. However, the collection of novel data types, users' elevated desire for data control and the need for application of privacy laws across jurisdictions will pose new challenges we should creatively and collectively deal with.

3 How can we then help people understand how data is collected and used in the Metaverse?

We need to be creative in our approaches to transparency, privacy education, and clear communication of data controller responsibilities in the Metaverse. A basic understanding of the different entities and players across these layers to determine who controls or processes data at each level is essential for establishing a clear framework for allocating responsibilities and liabilities within the Metaverse ecosystem.

4 How might we harness the opportunities for empowering people with in-context control presented to us by 3D interaction?

The innovative approaches to inform and empower users in the Metaverse will make data privacy controls engaging and effective within immersive experiences. Upfront, in-context and on-demand notifications can be offered to users for enhanced control over their data. We should harness the potential of the Metaverse for enabling various methods of participatory governance. Regulators should ideally offer guidance and provide regulatory sandboxes for collaboration and co-development to shape the evolving landscape of data privacy in the Metaverse.

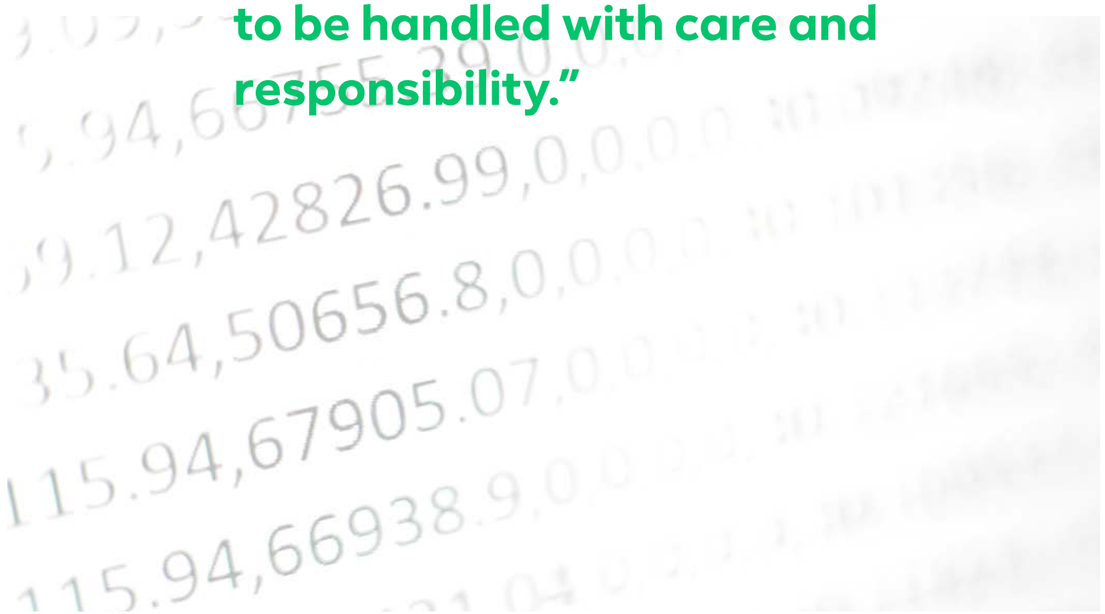
5 How should people be informed about the use of body based data in XR devices?

XR providers and users must comprehend and manage the privacy challenges regarding body-based data while harnessing XR's opportunities to establish a responsible and trustworthy Metaverse. It is important to inform and educate users at multiple points in their journey, with a focus on transparency, accountability and digital literacy. We should also empower users with Privacy-Enhancing Technologies (PETs) and gamified experiences so they can make informed decisions and protect their privacy in the Metaverse.

6 Should we and how might we create private spaces in the Metaverse?

As the importance of private spaces in the Metaverse grows, it is crucial to tailor privacy expectations to the nature of interactions, and to build user trust through transparent communication about data collection and usage. Metaverse operators are entrusted with user data and we share a universal responsibility to balance data protection with the promotion of data usage for the benefit of the individuals and the Metaverse industry.

"The fundamental privacy expectations that apply to traditional digital services will largely remain the same in the Metaverse, in that users will continue to expect their data to be handled with care and responsibility."



How to Cite this Report

XR Policy Dialogue Roundtable 03, "Privacy and Data in the Metaverse", XR Hub Korea, September 22nd, 2023

* This report was prepared by SNU AI Policy Initiative (principal: Seungbum CHOI)

Data Transparency & Controls

Presenter: Taja NAIDOO (Public Policy Manager, Meta), "Data Transparency & Controls in the Metaverse"

I would like to present the findings of a nine-month program in collaboration with SNU (Seoul National University) and IMDA (Infocomm Media Development Authority). The program aimed to explore data transparency in the context of immersive technology, including XR and the Metaverse. Some key insights from the program are:

1. **New Data Types and Uses:** It is crucial to demonstrate the value of sharing data to build trust with users. Various data types, including facial data, vitals, EMG, voice, and movement, all of which are relevant to immersive experiences, raise unique privacy concerns. Users are less concerned about data collection when it's actively and intentionally undertaken, rather than passively.
2. **New Multiparty Experiences:** We need to consider different levels of data sharing in shared immersive experiences. Also, we should provide creators and community facilitators with simple tools to manage data usage in these environments.
3. **Gestural and Facial Controls:** Introducing deliberate friction can help users be more deliberate about data sharing. There is a lot of potential in leveraging place-based norms to provide a control mechanism in data sharing.

Taja Naidoo

Privacy Public Policy Manager, Policy Solutions at Meta

I would further introduce two design prototypes that captures the key insights from the program. The first is "Safety Mode Design" focused on monitoring physical status and well-being for festival-goers. The second is "Permissions Map" that allows users to visualize and control data sharing based on location within a shopping center.

To sum up, the complexity and challenges surrounding data transparency and user experiences in the emerging Metaverse emphasizes the importance of user education, default settings, and customization of data sharing based on different immersive experiences. Friction could be strategically introduced to ensure that users have time to make informed decisions about their data sharing. These insights and design prototypes aim to help companies and policymakers navigate the challenges and opportunities presented by the immersive technologies.

Privacy in the Context of XR

Presenter: Sangchul PARK (Assistant Professor, School of Law, SNU) presented on "Privacy in the Context of XR"

I would like to discuss the implications of immersive technologies like the Metaverse on privacy. Immersive technologies can transform various aspects of our daily lives, enhance AI applications, and change how data is collected and used. The EU and the U.S. regulate biometric data, and the major challenge seems to be of balancing privacy with technology's core functions. Adding to this challenge is the need to consider regional variances in privacy perceptions.

As part of a research project in collaboration with Meta and SNU, we are investigating perceptions of the Metaverse across seven countries. Preliminary findings suggest that privacy concerns and consent to personal data usage within the Metaverse vary by region. Preliminary research shows varying privacy perceptions across countries, with Singaporeans being both concerned and willing to consent to data use in the Metaverse.

Sangchul Park

Assistant Professor, School of Law, Seoul National University

Empowerment Tool

Advancements in privacy-enhancing technologies like federated learning and differential privacy has paved the way for transcending the trade-off between privacy and utility in XR experiences. XR environments could offer a unique platform for implementing in-context privacy controls, moving away from the traditional disclosure and consent model.

The actual implementation of such in-context privacy controls should be a subject for an open discussion and we hope that our research would contribute to further discussions on privacy in immersive technologies.

1 Does privacy have different meanings?

Jo-Fan Yu

Partner, Baker & McKenzie

Context-based Expectations of Privacy

In the early stages of the Metaverse, users' privacy expectations are largely based on their real-world experiences. The fact that AR/VR technologies now put users in an extended reality setting doesn't significantly impact user privacy expectations. Instead, it's the context within the Metaverse that play a crucial role in shaping these expectations.

For example, if AR/VR is used for work purposes in a public office setting, users may have lower privacy expectations. However, in more private settings like closed-door meetings or confidential conversations, privacy expectations would be higher.

Varying Sensitivity to Data Privacy

Users are becoming increasingly sensitive to data privacy, especially with the rapid advancement of AI and technology. Users are concerned about the collection, usage, and sharing of data in the Metaverse, and they often struggle to understand how their data is being used.

Global access to information and shared experiences have made regional and country-specific differences in how people interact with 3D spaces and perceive privacy in the Metaverse less significant. Instead, a user's age and exposure to new technologies, like the Metaverse and AI, are more likely to influence their privacy perspectives. Different generations, from older to younger, may have varying expectations of privacy and interactions with emerging technologies. (Jo-Fan YU)

Byoung-Pil Kim

Professor, Graduate School of Innovation and Technology Management, KAIST

AI Chatbot Using Private Conversations

I would like to focus on a significant data privacy case in Korea, known as the "Lee Luda (이루다) Chatbot" case, which has broader implications for data protection, especially in AR and VR settings. In this case, a Korean startup developed an AI chatbot using 10 billion private conversations collected through an app called "Science of Love," which analyzed users' conversations with potential romantic partners to offer dating advice.

The key issue in this case was the use of user conversation data for training an AI chatbot, as the startup's privacy policy included a clause stating that the data could be used for the development of new services. The PIPC (Personal Information Protection Commission), which is Korea's data protection authority, examined the case and determined that the term "new services" was overly broad. They concluded that user privacy expectations needed to be considered, and the use of private conversation data for training another chatbot was not in line with users' expectations unless the data was anonymized.

It is also important to consider the insights of service developers and operators who directly engage with customers to understand user expectations. While it may be challenging to define clear boundaries for user expectations, it is essential for those handling user data to recognize that the law will consider what people reasonably expect regarding privacy in the services they use.

This ruling underscored the importance of respecting users' privacy expectations and highlighted that simply specifying data usage in terms of service or privacy policies was insufficient. This interpretation introduces legal uncertainties and raises questions about how to ascertain users' expectations in different contexts.

It is also important to consider the insights of service developers and operators who directly engage with customers to understand user expectations. While it may be challenging to define clear boundaries for user expectations, it is essential for those handling user data to recognize that the law will consider what people reasonably expect regarding privacy in the services they use. (Byoung-Pil KIM)

2 How do users' expectations of privacy change or remain the same in immersive environments, and the Metaverse?

B M Mainul Hossain

Professor, Institute of Information Technology (IIT), University of Dhaka

New Dimensions of Privacy in the Metaverse

In the context of the Metaverse, privacy takes on two essential dimensions: freedom from interference in personal spaces and the confidentiality and control over data sharing. I would like to raise several concerns and considerations:

1. **New Data Types and Uses:** It is crucial to demonstrate the value of sharing data to build trust with users. Various data types, including facial data, vitals, EMG, voice, and movement, all of which are relevant to immersive experiences, raise unique privacy concerns. Users are less concerned about data collection when it's actively and intentionally undertaken, rather than passively.
2. **New Multiparty Experiences:** We need to consider different levels of data sharing in shared immersive experiences. Also, we should provide creators and community facilitators with simple tools to manage data usage in these environments.
3. **Gestural and Facial Controls:** Introducing deliberate friction can help users be more deliberate about data sharing. There is a lot of potential in leveraging place-based norms to provide a control mechanism in data sharing.

These concerns emphasize the evolving nature of privacy in the Metaverse and the need for updated legal frameworks, technical solutions, and policy considerations to safeguard user privacy effectively. (B M Mainul HOSSAIN)

Arianne Jimenez

Head of Privacy & Data Policy, Engagement, APAC at Meta

Need for Creativity in Meeting Privacy Expectations

I would like to highlight several key points on expectations of privacy in the Metaverse and how they compare to traditional digital services, as follows:

1. **Common Privacy Expectations:** The fundamental privacy expectations that apply to traditional digital services, such as purpose limitation, data minimization, data retention, data protection, fairness, and accountability, will largely remain the same in the Metaverse. Users will continue to expect their data to be handled with care and responsibility.
2. **Elevation of Expectations:** Due to the immersive nature of the Metaverse, some privacy expectations may be heightened. Users will expect greater transparency and control over how their data is collected and used. This increased expectation is an opportunity for companies to be creative and innovative in how they communicate and provide control to users, making use of the immersive and interactive nature of XR technologies.
3. **Data Minimization:** Users will have a heightened expectation for data minimization, especially in devices like smart glasses. These devices capture data from the user's surroundings, and there will be a greater need to signal data collection to bystanders and minimize the data collected. Privacy-enhancing techniques like differential privacy or on-device processing may become more important.
4. **Treatment of Novel Data Types:** XR technologies will collect novel data types that traditional digital services do not typically handle. There is a need to define and categorize these new data types and determine the appropriate level of care and privacy protection for them. Users may have different or heightened expectations for the privacy of these data types.

while many privacy expectations remain consistent between traditional digital services and the Metaverse, the immersive nature of the Metaverse will lead to increased expectations of transparency and control, greater focus on data minimization, and the need to address novel data types. Companies have an opportunity to be creative in meeting these heightened expectations.

In summary, while many privacy expectations remain consistent between traditional digital services and the Metaverse, the immersive nature of the Metaverse will lead to increased expectations of transparency and control, greater focus on data minimization, and the need to address novel data types. Companies have an opportunity to be creative in meeting these heightened expectations. (Arianne JIMENEZ)

3 How can we then help people understand how data is collected and used in the Metaverse, and transparency about how data is used in the Metaverse's key to building trust?

Irish Salandanan-Almeida

Chief Privacy Officer, Globe Telecom, Inc.

How Privacy-related UI in the Metaverse Could be Different

I would like to address the topic of data transparency and control in the Metaverse and present several key points:

1. **Incorporating Privacy Notices in the User Interface:** To achieve meaningful transparency in the Metaverse, I would suggest we creatively incorporate privacy notices directly into the user interface. Unlike traditional digital platforms, the Metaverse offers fewer opportunities for users to click on hyperlinks or consent to data processing. As such, just-in-time and in-context privacy notices could be used in the Metaverse.
2. **Just-in-Time and In-Context Notices:** Just-in-time notices would alert users when relevant to their actions without disrupting their experience, while in-context notifications would inform users only when relevant to their current activities in the Metaverse.
3. **Privacy Education within the Platform:** Also recommended is integrating data privacy awareness and education within the Metaverse platform. This could include quick walkthroughs or tutorials on how to navigate the virtual world, keep information secure, and report issues like cyberbullying or harassment.
4. **Complexity and Simplicity of Privacy:** Privacy in the Metaverse is both complex and simple. It can be complex because the identity of the data controller may not always be apparent, and it can change depending on the specific virtual space. Communicating the identity of the data controller to users is a challenge. However, the expectation of privacy in the Metaverse is similar to the real world, where the property owner is responsible for the safety of tenants. In the Metaverse, it's the developer or platform owner's responsibility to secure user data, while users also have a responsibility to understand data practices and protect their own data.

Privacy in the Metaverse is both complex and simple. It can be complex because the identity of the data controller may not always be apparent, and it can change depending on the specific virtual space. Communicating the identity of the data controller to users is a challenge.

In summary, I would emphasize the need for creative approaches to transparency, privacy education, and clear communication of data controller responsibilities in the Metaverse. It should also be highlighted that user expectations of privacy in the Metaverse resemble those in the real world. (Irish SALANDANAN-ALMEIDA)

Metaverse Ecosystem as a Pyramid

Arianne Jimenez

Head of Privacy & Data Policy, Engagement, APAC at Meta

I would like to introduce a framework for thinking about the Metaverse and how to allocate responsibilities and liabilities. The framework is structured as a pyramid with different layers, each representing a different aspect of the Metaverse ecosystem:

1. **Metaverse Environment:** At the bottom of the pyramid is the Metaverse environment itself, the foundational layer.
2. **Hardware Device Developers:** The next layer consists of the developers of hardware devices used to access the Metaverse, such as AR/VR headsets.
3. **App Stores and Platforms:** Above the hardware layer, there are app stores or platforms, similar to current app stores like the Apple App Store or Google Play Store, which host applications for the Metaverse.
4. **Distinct Experiences:** This layer represents the distinct applications, games, and environments that users interact with within the Metaverse.
5. **Communities:** At the top of the pyramid, there are communities formed within the Metaverse, including social interactions and user-generated content.

We need a deeper understanding of the different entities and players across these layers to determine who controls or processes data at each level. This understanding is essential for establishing a clear framework for allocating responsibilities and liabilities within the Metaverse ecosystem.

We need a deeper understanding of the different entities and players across these layers to determine who controls or processes data at each level. This understanding is essential for establishing a clear framework for allocating responsibilities and liabilities within the Metaverse ecosystem.

The proposed framework provides an example of a structured way to analyze and allocate responsibilities and liabilities in the Metaverse based on the specific layer of involvement within the ecosystem. (Arianne JIMENEZ)

4 How might we harness the opportunities for empowering people with in-context control presented to us by 3D interaction? What other vehicles or methods for collaboration between industry, academia and civil society exist or should be created to enhance cooperation in building the Metaverse

responsibly, especially with regard to privacy, transparency, consent, and control?

Sangchul Park

Assistant Professor, School of Law, Seoul National University

Achieving Dynamic Control in the Metaverse

It is important to facilitate in-context control for users in the Metaverse. Various tools such as compasses, intelligent private agents, dashboards, and gestural and spatial controls that can be used to provide relevant explanations to users at the right time. This approach aims to avoid overwhelming users with lengthy privacy policies and allows for personalized, context-aware decision-making.

We need to enhance the adaptability and scalability of privacy laws to achieve dynamic control in the Metaverse. The key component in achieving this is to understand people's real perceptions and expectations and to initiate legislative reform in this regard.

Nurturing Participatory Governance & Assigning Liability to Least Cost Avoiders

Regarding the second question, I would agree with Irish's point about the combination of education, literacy, and active citizen participation being vital for fostering trust in the Metaverse.

There is major potential in the Metaverse for enhancing human autonomy and capturing people's wisdom for participatory governance.

There is major potential in the Metaverse for enhancing human autonomy and capturing people's wisdom for participatory governance.

There is major potential in the Metaverse for enhancing human autonomy and capturing people's wisdom for participatory governance. Interestingly, the support for participatory governance in the Metaverse varies by region. A survey found differences in perspectives between Asian and Western respondents regarding governance in the Metaverse, with strong support among Western respondents for resolving real-world issues through voting among participants.

I also appreciate the pyramid analogy presented by Arianne, which helps in understanding the allocation of roles and responsibilities across the Metaverse value chain. We should identify those who could avoid misuse of data and other bad acts with minimum cost and assign liability on the least cost avoiders. (Sangchul PARK)

Suat Hong Koh

Deputy Director (Data Tech), Personal Data Protection Commission, Singapore

Regulators will Provide Regulatory Sandbox & Guidance

I would like to discuss the opportunities for collaboration between regulators, industry, and academia in addressing emerging issues and concerns related to the Metaverse. There are various ways in which such collaborations can be facilitated:

1. **Design Jams:** Collaborative events where regulators and industry partners explore new technologies and data uses will be important. The outcomes of these events can provide insights and guidance for addressing new challenges in the Metaverse.
2. **Co-development through Data Regulatory Sandbox:** Regulators like the PDPC (Personal Data Protection Commission) work with industry partners to test new innovations within a data regulatory

sandbox. This approach allows the industry to develop products with data protection considerations from the outset.

3. **Open Innovation Platform:** The PDPC leverages open innovation platforms to call for new and innovative solutions from problem solvers worldwide. These platforms can be used to address specific challenges arising in the Metaverse and seek solutions from a global community of innovators.
4. **Providing Specific Guidance:** Also important is offering specific guidance to industries looking to develop new products and services in the Metaverse. Such guidance can help address contextual issues and ensure compliance with data protection regulations.

Overall, the PDPC is committed to the collaboration and co-development to shape the evolving landscape of data privacy in the Metaverse, and will play a role in providing guidance and support to the industry. (Suat Hong KOH)

Taja Naidoo

Privacy Public Policy Manager, Policy Solutions at Meta

Innovative Approaches to Inform and Empower Users

We need to both inform and empower users in the context of data transparency and control in the Metaverse. The challenge lies in aligning people's expressed preferences regarding privacy with their actual behavior in terms of privacy settings and engagement with privacy controls. To address this, we need to creatively inform and empower users within immersive experiences in the Metaverse.
I would like to raise some key points:

1. **Informing and Empowering:** I would stress the significance of not only informing users about data practices but also providing them with the tools and agency to control their data in the Metaverse.
2. **Unique Challenges of the Metaverse:** In the Metaverse, traditional approaches to informing and empowering users might not work due to the absence of hyperlinks and conventional privacy policies. Companies and users will need to be more creative in the methods they use.

The challenge lies in aligning people's expressed preferences regarding privacy with their actual behavior in terms of privacy settings and engagement with privacy controls. To address this, we need to creatively inform and empower users within immersive experiences in the Metaverse.

3. **The Upfront, In-Context, On-Demand Model:** The model of informing users upfront, providing in-context notifications, and offering on-demand controls still holds value in the Metaverse context. Immersive experiences can follow a linear progression that includes moments for proactive notifications, whether blocking or non-blocking.
4. **Creative Design:** Creativity in design is crucial, especially for on-demand notifications and controls. Examples like an in-hand settings dial or a "sound bubble" to enable private conversations were highlighted as innovative ways to empower users.

Overall, the innovative approaches to inform and empower users in the Metaverse will make data privacy controls engaging and effective within immersive experiences. (Taja NAIDOO)

Byoung-Pil Kim

Professor, Graduate School of Innovation and Technology Management, KAIST

Different Privacy Expectations for Virtual Personas

I would like to pose a potential distinction between two approaches regarding privacy expectations in the Metaverse.

1. **Continuation of Physical World Expectations:** If the goal is for individuals to exist in the Metaverse as extensions of their physical selves, then their privacy expectations should align with what they expect in the real world. In this scenario, privacy in the Metaverse should mirror privacy in the physical world.
2. **Creation of New Virtual Identities:** Conversely, if the intention is to create entirely new virtual personas that are disconnected from one's physical identity, then the privacy expectations for these virtual characters may differ significantly. The current legal frameworks often do not provide the same level of protection to virtual characters as they do to real individuals.

We may need new legal frameworks that recognize and protect the privacy and rights of digital personas in the Metaverse, especially if these virtual entities have unique personalities and identities. (Byoung-Pil KIM)

5 How should people be informed about the use of body based data in XR devices?

Hiroshi Miyashita

Professor, Chuo University

A New Set of Challenges for Privacy in the XR Environment

In the XR (Extended Reality) environment, there are several key privacy challenges regarding body-based data and emerging technologies. XR technology can identify users with high accuracy based on head and hand motion data, even when their faces are masked with AI characters. Additionally, body data analytics are used in various applications, such as monitoring driver alertness and detecting emotions or suspicious individuals in public places.

We need to inform users about the privacy risks associated with body-based data. Transparency and accountability are seen as essential for building trust in the XR environment, as many of these risks are hidden from users.

We should consider the following in addressing these new privacy risks:

1. **Transparency:** We need to inform users about the privacy risks associated with body-based data. Transparency and accountability are seen as essential for building trust in the XR environment, as many of these risks are hidden from users.
2. **Privacy Education:** We should focus on educating those most vulnerable to privacy risks. In particular, the younger generation's

lack of awareness regarding privacy risks related to body-based data poses a major threat. Privacy education to ensure that users, especially the digitally connected younger generation, understand these risks is important.

3. **Neuroprivacy:** Another set of risk lies in the emergence of neuro-technology and brain privacy in XR. There are companies conducting research on measuring concentration and emotional states through brain and eye-tracking data. European regulators, such as the UK and Spain, have already published policy papers on neuroprivacy.

Regulators in Europe are addressing these issues, and XR providers and users must comprehend and manage these privacy challenges while harnessing XR's opportunities to establish a responsible and trustworthy Metaverse. (Hiroshi MIYASHITA)

Taja Naidoo

Privacy Public Policy Manager, Policy Solutions at Meta

Combination of Technology & Education to Enhance Privacy

A comprehensive approach to privacy education in XR involves considering the entire user journey, using gamification for engagement, and providing clear and understandable information about data usage and privacy rights. It also requires transparency and accountability measures, both user-facing and within the XR ecosystem.

1. **Broad Classification of Body-Based Data:** The term "biometric" has multiple definitions, and it's important to consider a broad classification of data generated from the human body when discussing privacy in XR. Different jurisdictions may categorize such data differently.
2. **Informing People:** To inform users effectively, it is essential to consider the entire user journey, starting from researching a device to onboarding and experiencing XR. This includes using educational campaigns, iconography, and other methods to help users understand the implications of data usage.

The overarching idea is to inform and educate users at multiple points in their journey, with a focus on transparency, accountability, and digital literacy, to empower them to make informed decisions and protect their privacy in the Metaverse. (Taja NAIDOO)

3. **Gamifying Data Education:** Especially for younger users, gamification can be a useful approach to educate them about data. Gamified experiences can increase engagement and help users grasp information more effectively.
4. **Privacy-Enhancing Technologies (PETs):** PETs like differential privacy and multiparty computation can enhance privacy within the XR ecosystem. While these technologies have their place, they may not be suitable for educating end-users due to their technical complexity.
5. **Transparency and Accountability:** Transparency and accountability in XR go beyond user-facing information. There are processes, technical mitigations, and data protections happening behind the scenes that users may not be aware of. Educating users about these aspects may require broader educational efforts, possibly even within schools and universities.

The overarching idea is to inform and educate users at multiple points in their journey, with a focus on transparency, accountability, and digital literacy, to empower them to make informed decisions and protect their privacy in the Metaverse. (Taja NAIDOO)

6 Should we and how might we create private spaces in the Metaverse?

Social Interactions in a Variety of Virtual Settings

Arianne Jimenez

Head of Privacy & Data Policy, Engagement, APAC at Meta

User experiences in the Metaverse are expected to resemble physical reality more closely than the two-dimensional internet. Imagine individuals creating their own virtual spaces in the Metaverse, similar to a virtual living room, where they can interact with a select group of friends in a private setting. These virtual spaces will be designed by users, reflecting their preferences and privacy expectations.

In such spaces, the expectation of privacy would be similar to private physical conversations in a living room. We can also imagine virtual spaces of different sizes in the Metaverse, from small intimate rooms to larger social halls, auditoriums, and stadiums. The privacy expectations would differ in each of these spaces, leading to the development of unique rules to govern them.

In such spaces, the expectation of privacy would be similar to private physical conversations in a living room. We can also imagine virtual spaces of different sizes in the Metaverse, from small intimate rooms to larger social halls, auditoriums, and stadiums. The privacy expectations would differ in each of these spaces, leading to the development of unique rules to govern them.

While the concept of virtual spaces in the Metaverse is intriguing, the specific rules and technologies to support these spaces are still evolving, requiring more time for exploration and development to establish suitable rules and technology for supporting these spaces. (Arianne JIMENEZ)

Understanding the Varied Expectations for Privacy & Building Trust through Transparency

Irish Salandanan-Almeida

Chief Privacy Officer, Globe Telecom, Inc.

I would echo Arianne's perspective on the interactions in the Metaverse mirroring those in the real world, suggesting the need for private spaces in the virtual realm. It would be important to maintain confidentiality and data privacy in virtual interactions with friends or colleagues, similar to real-life expectations.

The nature of the interaction or transaction would be key in determining users' expectations of privacy. Privacy expectations may vary, with less emphasis on privacy in entertainment or gaming scenarios and heightened expectations in financial or medical contexts.

Private spaces are seen as essential for transactions involving sensitive information.

Furthermore, developers and platform owners should avoid overcollecting data for undisclosed purposes or hiding information in lengthy terms and conditions. Building trust among users is essential to encourage their participation in the Metaverse, addressing concerns about data privacy and digital security.

In summary, as the importance of private spaces in the Metaverse grows, it is crucial to tailor privacy expectations to the nature of interactions, and to build user trust through transparent communication about data collection and usage. (Irish SALANDANAN-ALMEIDA)

Thitirat Thipsamritkul

Lecturer, Faculty of Law, Thammasat University

Metaverse Operators Entrusted with User Privacy

I would like to make quick point in response to Professor Kim's suggestion about reducing links to real identities in the Metaverse. Although internet users have always wished to separate their digital identities from real-world identities, assuming a complete disconnect between their online and offline identities might cause false expectations of security, leading to privacy risks.

My second point is related to Arianne's comments on creating private spaces in the Metaverse. I would make an analogy between user-designed virtual spaces and individual hotel rooms, suggesting that users may not have full control over the entire Metaverse but rather design private spaces within it. Building trust between those who own and manage these virtual spaces, the operator of the Metaverse, and the users would be crucial, as exemplified by the hotel industry's long history of establishing norms to create trust and ensure privacy of its customers. (Thitirat THIPSAMRITKUL)

Suat Hong Koh

Deputy Director (Data Tech), Personal Data Protection Commission, Singapore

Balancing Data Protection with the Need for Data Usage

Representing a regulatory perspective, I would emphasize the importance of balancing data protection with the promotion of data usage for the benefit of the individuals and the Metaverse industry. As more use cases develop in the Metaverse, views on data protection and privacy will become clearer.

Representing a regulatory perspective, I would emphasize the importance of balancing data protection with the promotion of data usage for the benefit of the individuals and the Metaverse industry. As more use cases develop in the Metaverse, views on data protection and privacy will become clearer.

In the context of defining and creating private spaces in the Metaverse, we should be mindful that criminals, as well as law-abiding citizens, are also using the end-to-end encryption in messaging apps like WhatsApp to their benefit. This heightens the need to collectively define what private spaces in the Metaverse should look like, considering both privacy and data protection and the prevention of harm, particularly in terms of law enforcement's ability to safeguard individuals, especially children. (Suat Hong KOH)

A Universal Responsibility

XR offers a diverse range of opportunities, including entertainment, education, and medical applications. While we acknowledge that people's expectations can vary based on different factors such as the purpose, generation, and visions they have, we need to strive for a universal consensus in building trust in XR. Privacy considerations may be local, but the responsibility for addressing them should be universal. (Hiroshi MIYASHITA)terms of law enforcement's ability to safeguard individuals, especially children. (Suat Hong KOH)

Taja Naidoo

Privacy Public Policy Manager, Policy Solutions at Meta

Invitation to Collaborate Further

I appreciate the insightful comments by Ms. Suat Hong Koh regarding encryption technology. I would note that privacy is a foundational right that enables the realization and enforcement of other rights. The ongoing negotiations and discussions about privacy with current technologies can provide valuable insights for addressing privacy concerns in the Metaverse. I would also invite the participants to explore the report available on ttclabs.net, which contains tools and frameworks developed during design jams and would like to solicit feedback and collaboration from the group. (Taja NAIDOO)

CLOSING REMARKS

Important issues in balancing data protection with utility in the Metaverse have been discussed. Novel data types and immersive environments provide both challenges and opportunities in building the trust that users' data will be processed in a transparent manner and in a way that will enrich their experience in the Metaverse. The final roundtable will discuss additional issues related to the safety and well-being in the Metaverse. Our aim is to facilitate these discussions so that they may inform stakeholders and bring about meaningful change in policymaking within the Metaverse (Yong LIM).