XR Privacy

CS 7375: Seminar: Human-Centered Privacy Design and Systems (co-located with PHIL 5110)

Tianshi Li | Assistant Professor

Announcements

- Feedback on the midterm presentation has been released
- Go to the OH if you have questions (Wed 1-2pm, by appointment)
- XR Privacy reading commentaries due this Wednesday 12pm
- For the discussion leads: Do a deep dive in the paper itself (allocating at least 10 minutes)
- No class next Monday; Next Wednesday is a lecture.

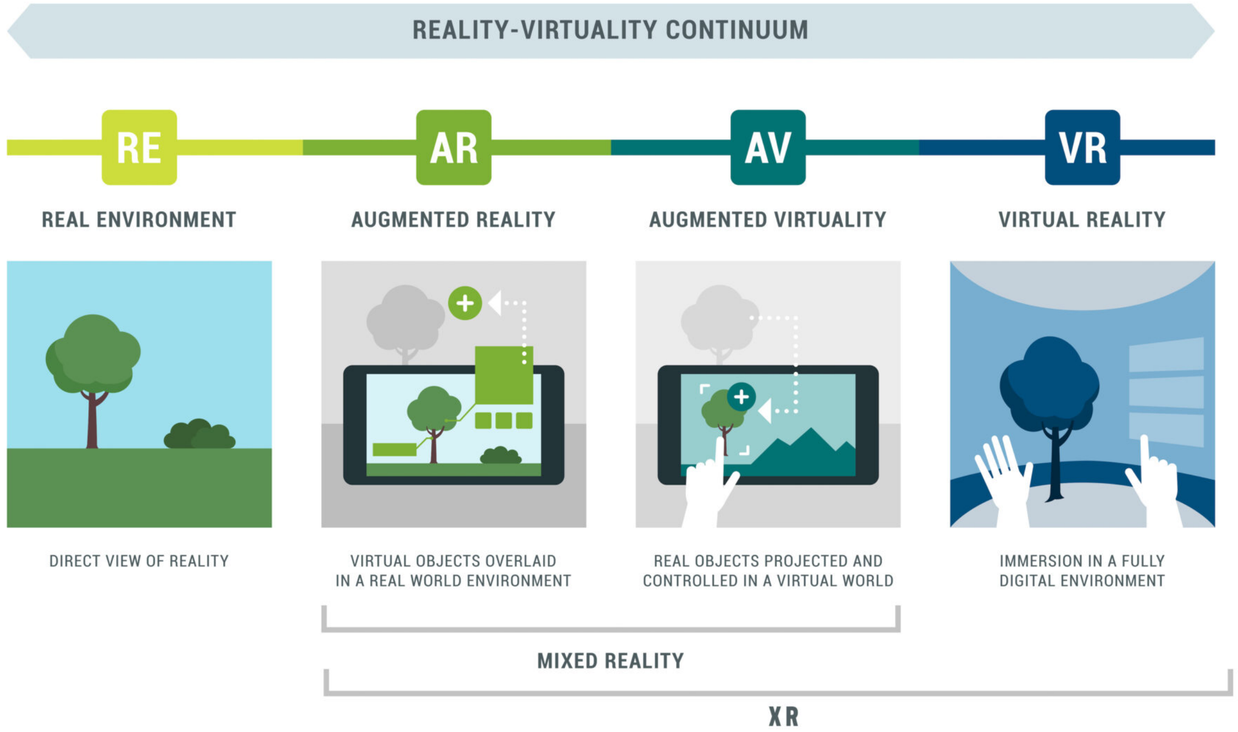
Agenda

- What is VR/AR/MR/XR?
- Input Privacy
- Output Control
- Privacy by Design: Platform-level and App-level

What is VR/AR/MR/XR?

- VR = Virtual Reality
- AR = Augmented Reality
- MR = Mixed reality
- XR = Extended Reality (an umbrella term that covers everything above)

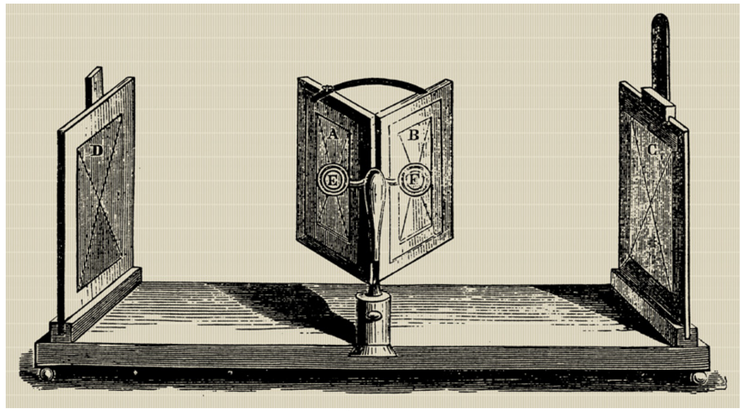
The reality-virtuality continuum



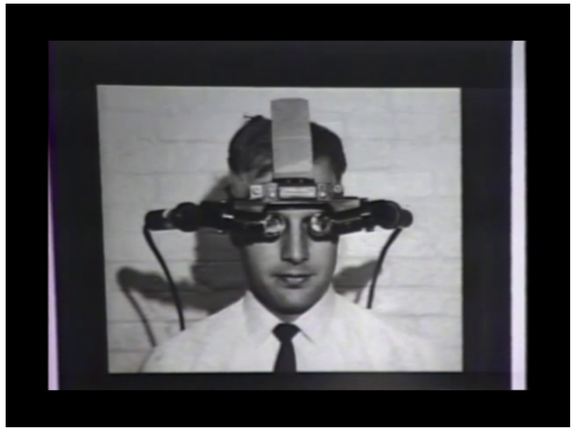
Reality-virtuality continuum (source: https://creatxr.com/the-virtuality-spectrum-understanding-ar-mr-vr-and-xr/)

A Brief History of Virtual Reality

Stereoscopes
Wheatstone, Brewster, ...



VR & AR
Ivan Sutherland



XR explosion
Meta, Sony, Apple, ...

1838 — 1968 — 2012-

Adapted from Slides of Stanford EE 267: Virtual Reality

Mobile AR Example: Pokémon GO

- Pokémon appear anchored to a Trainer's real-world environment
- Built with **Apple's ARKit** and **Google's ARCore** frameworks

Using Mixed Reality Feature

Meta Quest Pro

Has anyone used XR apps?
Has anyone developed XR apps?

What unique privacy challenges can be caused by XR?

What's unique about XR?

Always-on sensing

Apple Vision Pro (supposedly) has 14 cameras!

4x front- and side-facing for SLAM.

2x for pass through.

1x time-of-flight sensor.

4x for eye & face tracking.

2x for torso tracking.

1x for gesture tracking.

What's unique about XR?

Always-on sensing

Apple Vision Pro (supposedly) has 14 cameras!

4x front- and side-facing for SLAM.

2x for pass through.

1x time-of-flight sensor.

4x for eye & face tracking.

2x for torso tracking.

1x for gesture tracking.

What's unique about XR?

Always-on sensing

User

Apple Vision Pro (supposedly) has 14 cameras!

4x front- and side-facing for SLAM.

2x for pass through.

1x time-of-flight sensor.

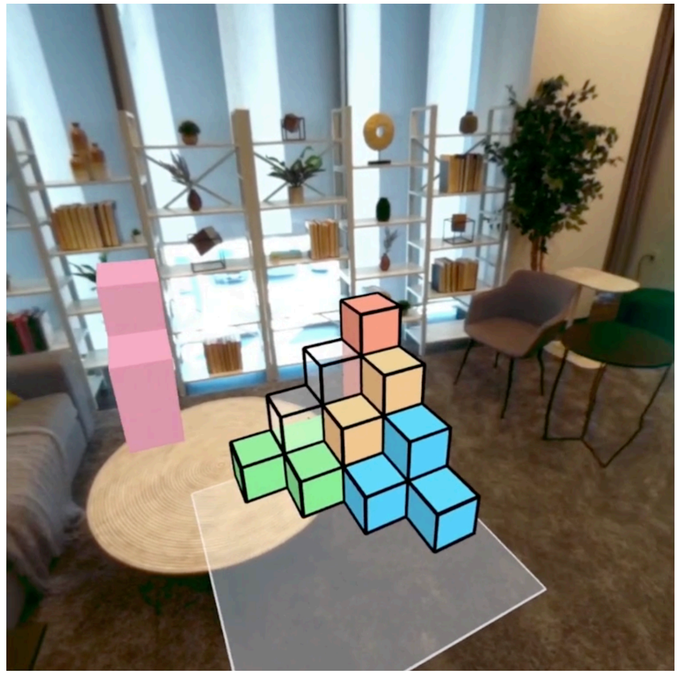
4x for eye & face tracking.

2x for torso tracking.

1x for gesture tracking.

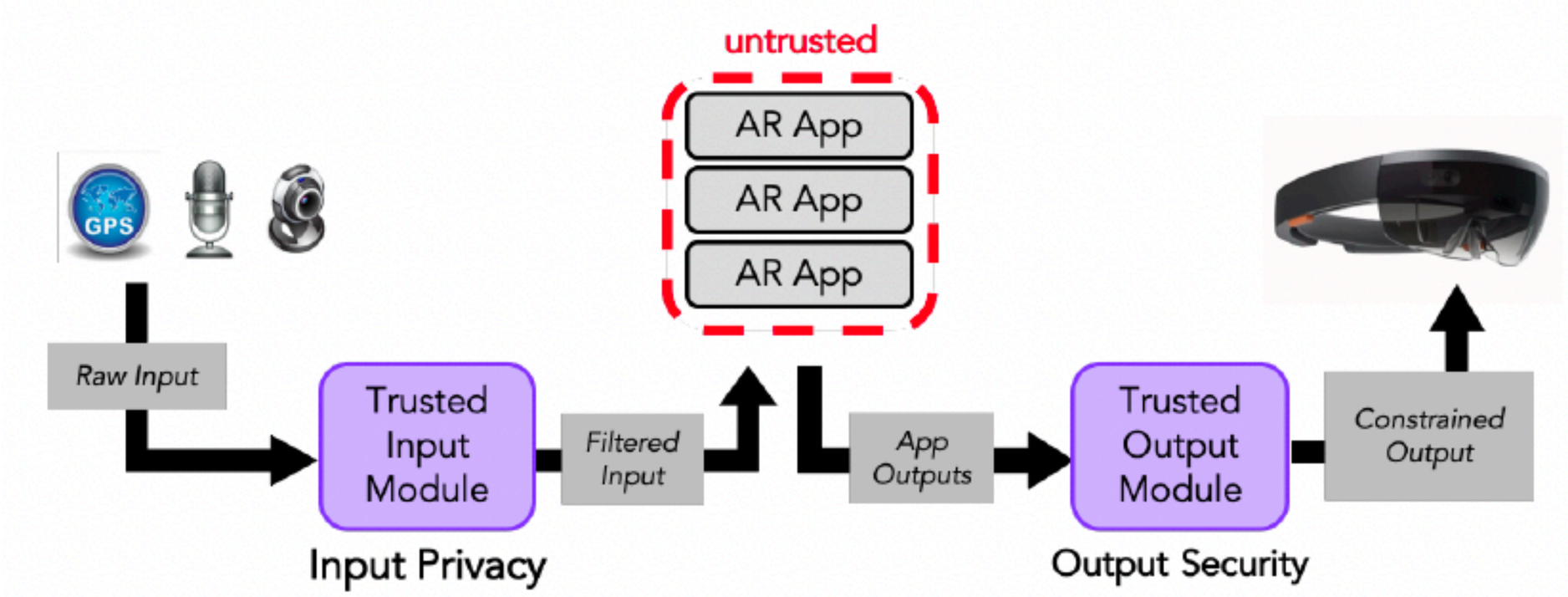
What's unique about XR?

Bridging the physical and digital world



What's unique about XR?

A trusted platform handling information flows; Apps and Users are untrusted



Roesner, Franziska, and Tadayoshi Kohno. "Security and privacy for augmented reality: Our 10-year retrospective." VR4Sec: 1st International Workshop on Security for XR and XR for Security. 2021.

Input Privacy

How information is collected

Always-on sensing

Input from the real-world

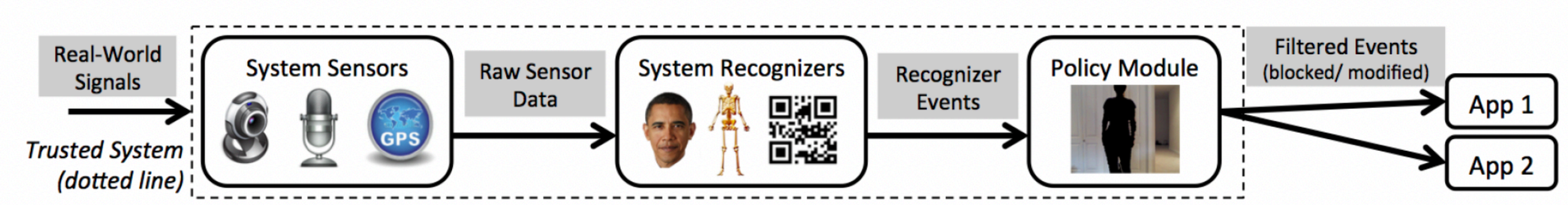
World-Driven Access Control

(Roesner et al. 2014)

- Goal: Help honest users manage applications' permissions
  - Protect users' own privacy by minimizing exposure of sensor information to untrusted apps
  - **Respect bystanders' privacy wishes**
  - Help users achieve these goals with minimal burden

World-Driven Access Control

(Roesner et al. 2014)



Primarily focused on policies communicated explicitly by the environment (e.g., QR code, BLE, Ultrasound), not inferred by the system.

Communicating data recording to the outside world

EyeSight gently pulses with white light to let others around you know that you are capturing photos or video.

Apple Vision Pro

Bystander Signaling

Meta Quest Pro uses outward facing cameras to enable features like Passthrough, which allows you to step outside your view in VR to see your real-time surroundings. We want people nearby to know when these cameras may be capturing them, so we've built external LED lights into the headset that turn on when Passthrough is in use.

Meta Quest Pro

Threats related to novel input modalities

Eye-tracking, facial expressions, head movements, hand movements, etc.

- Meta Quest tracks users' head movements using the headset and the hand movements using the two motion controllers.

https://www.uploadvr.com/oculus-touch-controllers-review/

Threats related to novel input modalities

Eye-tracking, facial expressions, head movements, hand movements, etc.

- Apple Vision Pro allows users to control the device with eye tracking and hand gestures.

https://www.uploadvr.com/apple-vision-pro-gesture-controls/

Threats related to novel input modalities

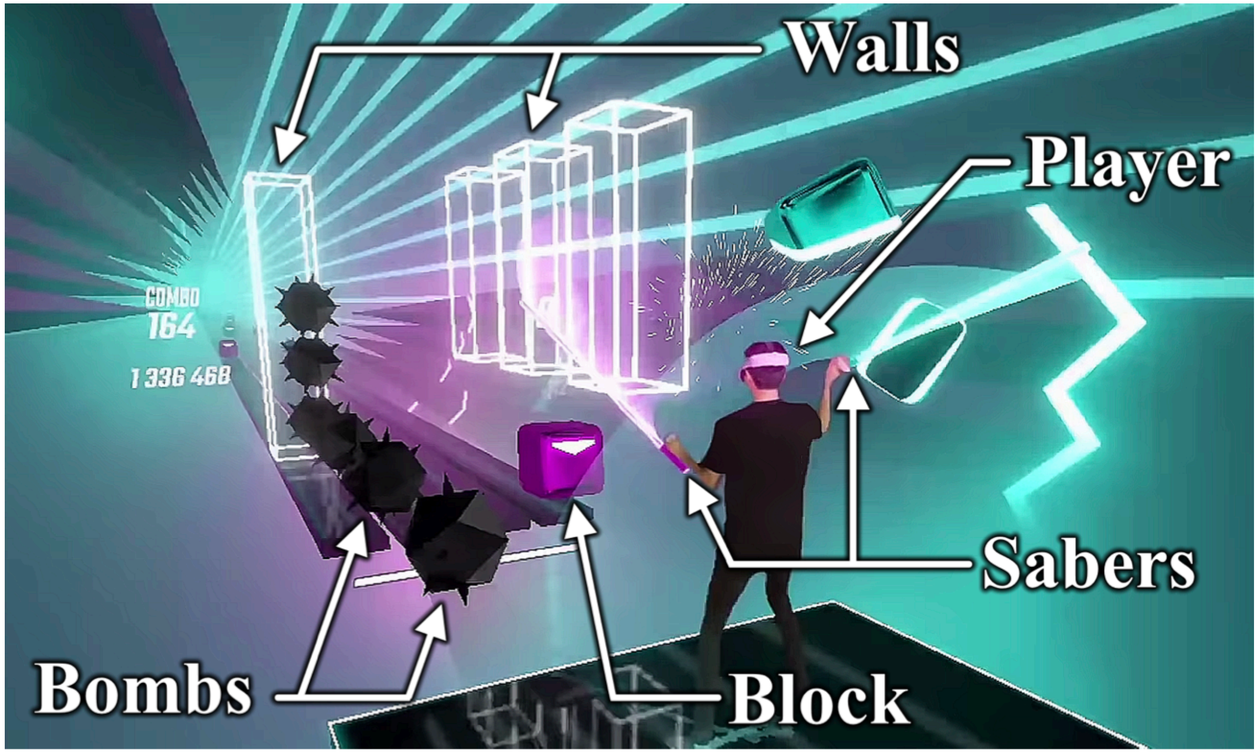
Eye-tracking, facial expressions, head movements, hand movements, etc.

- Apple Vision Pro allows users to create an animated avatar in real time that matches their mouth and hand movements for natural-looking conversations.

https://www.zdnet.com/article/meet-your-digital-persona-apples-vision-pro-users-to-get-real-time-animated-avatars/

Identifiability

Motion-based reidentification



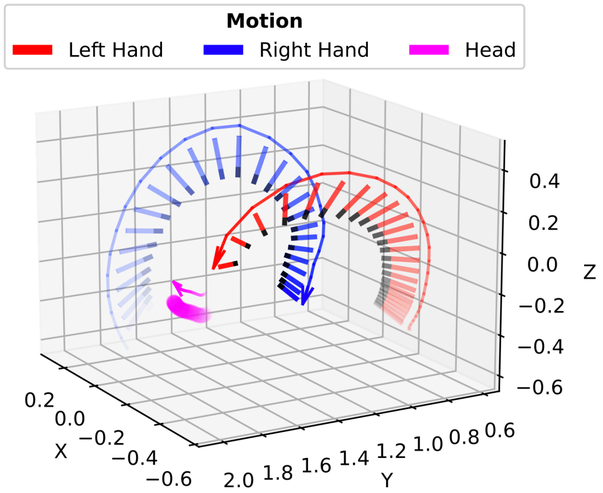


Figure 4: Head and hand motion from one second of telemetry.

https://beatleader.xyz/

Nair, Vivek, et al. "Unique identification of 50,000+ virtual reality users from head & hand motion data." 32nd USENIX Security Symposium (USENIX Security 23). 2023.

Identifiability

Motion-based reidentification

- After training a classification model on **5 minutes of data per person**, a user can be uniquely identified amongst the entire pool of **50,000+** with **94.33% accuracy from 100 seconds of motion**, and with **73.20%** accuracy from just **10 seconds of motion**.

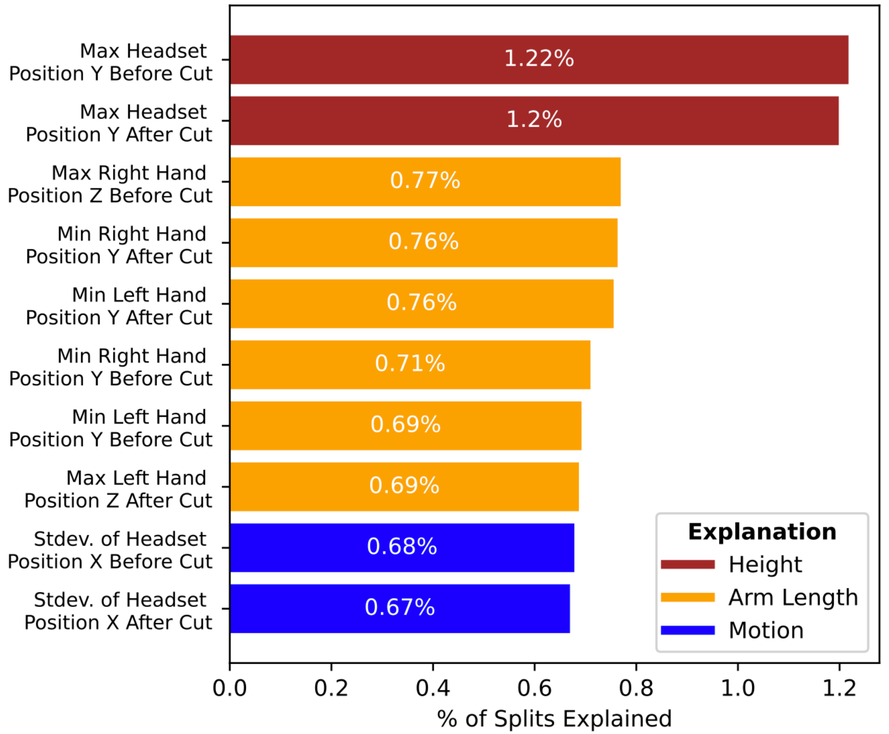


Figure 14: Explanation for 10 most important features.

Nair, Vivek, et al. "Unique identification of 50,000+ virtual reality users from head & hand motion data." 32nd USENIX Security Symposium (USENIX Security 23). 2023.

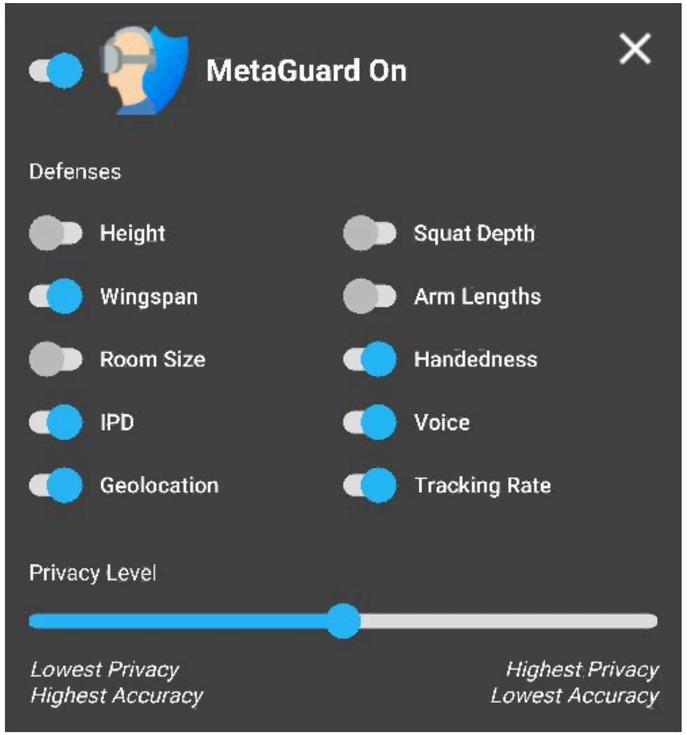
Infer private attributes from motion data

A large-scale survey of VR users (N=1,006)

	Per Sequence				Per User			
Attribute	**Total #**	**Test #**	**Accuracy**	**Significance**	**Total #**	**Test #**	**Accuracy**	**Significance**
StandaloneGrip	31,100	6,000	85.9%	p <0.001	311	60	91.7%	p <0.001
Height	19,100	6,000	76.5%	p <0.001	191	60	86.7%	p <0.001
Controller	33,200	6,000	81.2%	p <0.001	332	60	85.0%	p <0.001
Weight	9,800	6,000	73.6%	p <0.001	98	60	85.0%	p <0.001
FootSize	9,100	6,000	73.2%	p <0.001	91	60	85.0%	p <0.001
Country	33,300	6,000	60.3%	p <0.001	333	60	81.7%	p <0.001
RhythmGames	10,900	6,000	63.5%	p <0.001	109	60	80.0%	p <0.001
Age	62,300	6,000	64.9%	p <0.001	623	60	78.3%	p <0.001
TotalPlayTime	34,400	6,000	67.7%	p <0.001	344	60	78.3%	p <0.001
Headset	65,000	6,000	66.9%	p <0.001	650	60	76.7%	p <0.001
LeftArm	10,300	6,000	65.2%	p <0.001	103	60	76.7%	p <0.001
RightArm	10,200	6,000	64.9%	p <0.001	102	60	75.0%	p <0.001
Athletics	8,700	6,000	59.1%	p <0.001	87	60	75.0%	p <0.001
MaritalStatus	81,400	6,000	60.2%	p <0.001	814	60	73.3%	p <0.001
EmploymentStatus	64,200	6,000	65.1%	p <0.001	642	60	71.7%	p <0.001
AnyRhythmGames	83,000	6,000	54.8%	p <0.001	830	60	70.0%	p <0.001
Ethnicity	73,900	6,000	59.7%	p <0.001	739	60	70.0%	p <0.001
SteamComputerFormFactor	51,300	6,000	58.5%	p <0.001	513	60	70.0%	p <0.001
Footwear	36,700	6,000	60.5%	p <0.001	367	60	70.0%	p <0.001
AnyVRRhythmGames	83,000	8,000	56.8%	p <0.001	830	80	68.8%	p <0.001
Income	76,700	8,000	55.0%	p <0.001	767	80	68.8%	p <0.001
Wingspan	16,000	8,000	59.9%	p <0.001	160	80	68.8%	p <0.001

Nair, Vivek, et al. "Inferring private personal attributes of virtual reality users from head and hand motion data." arXiv preprint arXiv:2305.19198 (2023).

Using DP to mitigate



Nair, Vivek C., Gonzalo Munilla-Garrido, and Dawn Song. "Going incognito in the metaverse: Achieving theoretically optimal privacy-usability tradeoffs in VR." UIST 2023.

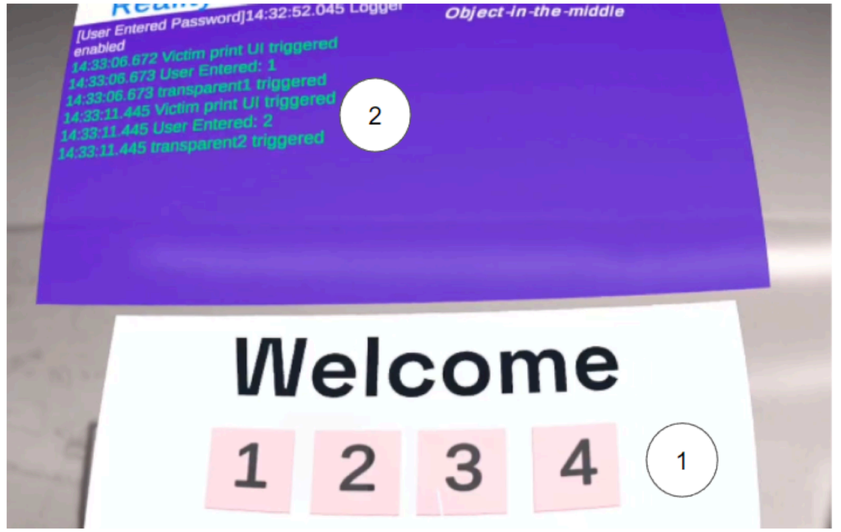
Adversarial objects Steal Input from the Virtual Space

1 The interface for authentication.

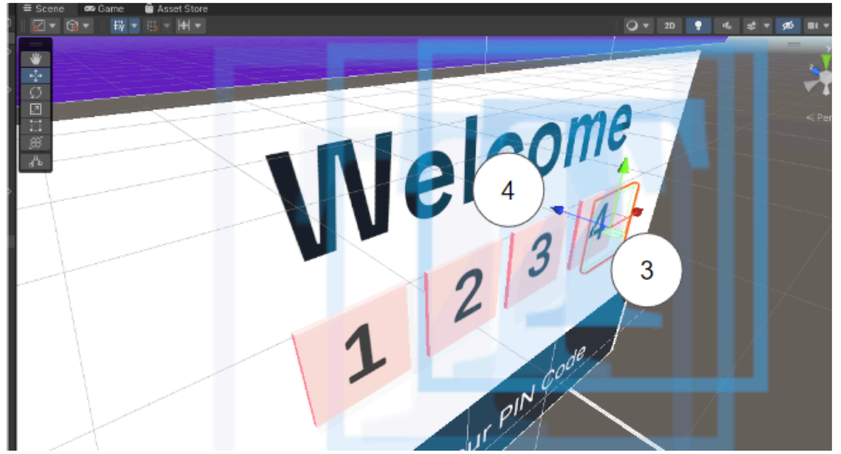
2 The logger for the execution result.

3 The **invisible object** the attacker places over the pin pad object.

4 The blue arrow suggests the direction of the synthetic input to trigger the pin pad object.



(a) User's view of the victim app.



(b) Demonstration of the object-in-the-middle attack.

Cheng, Kaiming, et al. "When the User Is Inside the User Interface: An Empirical Study of UI Security Properties in Augmented Reality." USENIX Security Symposium. 2024.

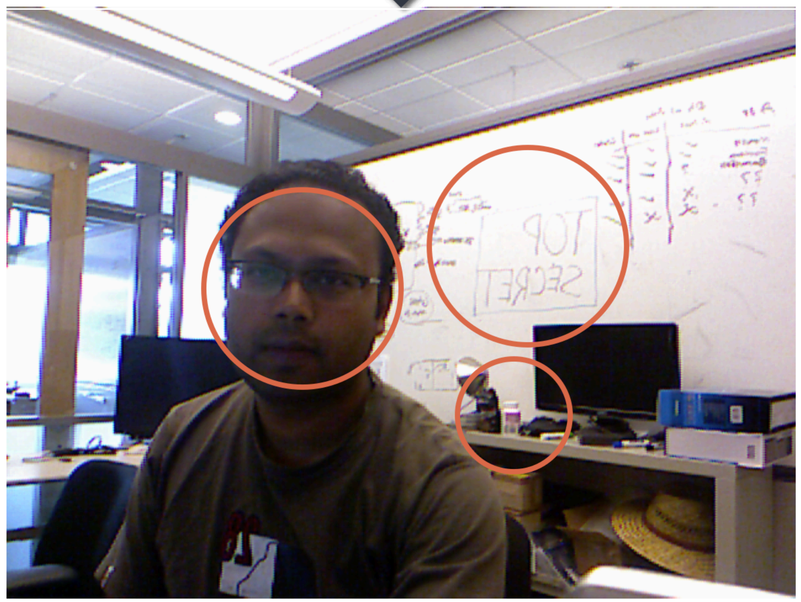
Output Privacy

How information is shared

https://rec-room.fandom.com/wiki/Whiteboard

Protect sensitive information from untrusted apps

all apps see this



tons of sensitive information!

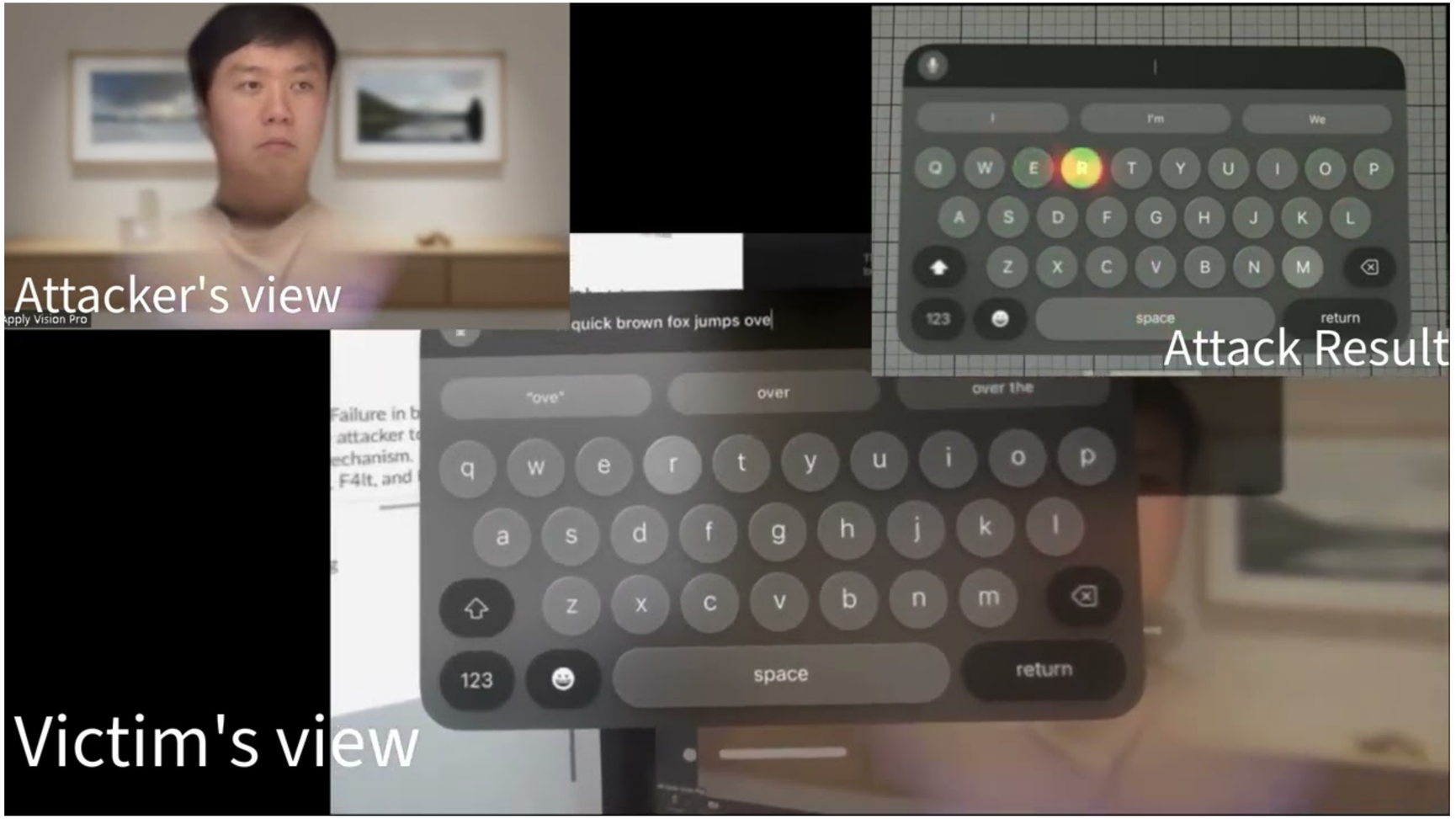
Jana, Suman, et al. "Enabling {Fine-Grained} permissions for augmented reality applications with recognizers." 22nd USENIX Security Symposium (USENIX Security 13). 2013.

Shoulder-surfing: Non-users as the intruder

George, Ceenu, et al. "Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality." NDSS, 2017.

Reconstruct text entered via gaze-controlled typing

Leakage to other XR users



Wang, Hanqiu, et al. "GAZEploit: Remote Keystroke Inference Attack by Gaze Estimation from Avatar Views in VR/MR Devices." (CCS'24)

Reconstruct text entered via gaze-controlled typing

Apple's fix

Presence

Available for: Apple Vision Pro

Impact: Inputs to the virtual keyboard may be inferred from Persona

Description: The issue was addressed by suspending Persona when the virtual keyboard is active.

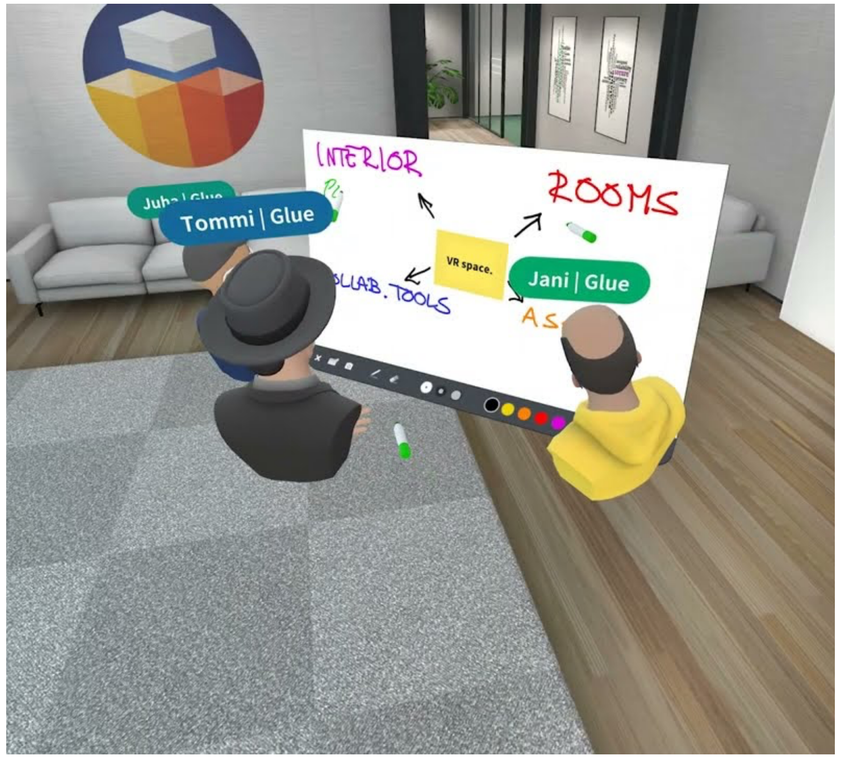
CVE-2024-40865: Hanqiu Wang of University of Florida, Zihao Zhan of Texas Tech University, Haoqi Shan of Certik, Siqi Dai of University of Florida, Max Panoff of University of Florida, and Shuo Wang of University of Florida

Entry added September 5, 2024

Tradeoff between privacy and functionality?

3D Content-sharing for multi-user AR

- Control access to (virtual) personal objects
- Managing (physical) personal space in AR
- Negotiating access to other users’ content
- Navigating partially shared AR environments



Privacy by design

Using Apple Vision Pro as a case study

Apple Vision Pro Privacy Overview

Learn how Apple Vision Pro and visionOS protect your data

February 2024

Privacy features brought to Apple Vision Pro

1. Advanced Data Protection
2. App Tracking Transparency
3. Data Access prompts
4. Data Protection classes
5. Hide My Email
6. iMessage encryption
7. iCloud Private Relay
8. Location Services
9. Privacy indicators
10. Private Network Address
11. Safari Private Browsing

And many more!

Privacy by design

We've been building privacy features and protections into our products for years. Safari Private Browsing, App Tracking Transparency, Privacy Nutrition Labels, and Advanced Data Protection are part of the privacy foundation of many of our products including Apple Vision Pro. As a result, Apple Vision Pro shares the same strong privacy and security foundation in all our platforms.

In some cases, we expanded these features on visionOS to meet the unique needs of Apple Vision Pro. For example, we added three new data types that apps can add to their Privacy Nutrition Label on the App Store: information about head movement, hand movement, and your surroundings.

We integrated hardware and software on Apple Vision Pro to protect your information in light of the unique privacy challenges posed by spatial computing. Apple Vision Pro features, from using it with your eyes and hands to showing digital content in your physical space, also have privacy built in. There are four privacy principles that inform everything we do at Apple, including all the new features on Apple Vision Pro. These four principles are: data minimization, on-device processing, transparency and control, and security.

https://www.apple.com/privacy/docs/Apple_Vision_Pro_Privacy_Overview.pdf

PbD principles emphasized in Vision Pro

- Data minimization
- On-device processing
- Transparency and control
- Security

Data minimization
Apple Vision Pro and visionOS minimize how much information developers, including Apple, can collect by only using the data necessary to support seamless spatial experiences. visionOS includes powerful on-device technologies to support realistic lighting and audio, so developers do not need to access information about your surroundings.

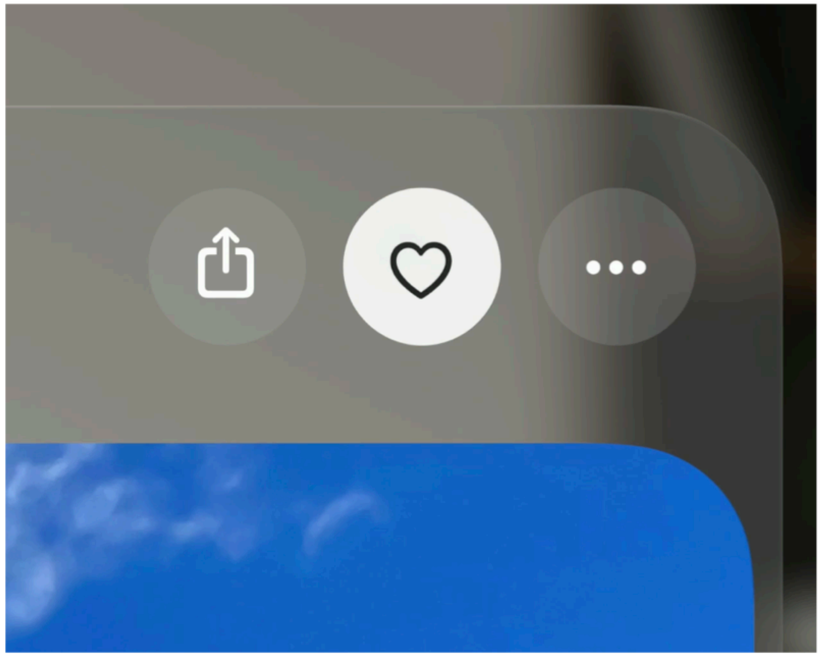
On-device processing
visionOS processes data on-device where possible instead of sharing it with Apple or other developers. To protect where you look, the hover effects that are shown when you look at content are rendered on-device by visionOS and are not shared with the app you are using. visionOS also maps your surroundings on-device in order to realistically render virtual objects in your physical space. Additionally, your Persona is generated entirely on-device with photos you take of yourself using your Apple Vision Pro.

Transparency and control
visionOS helps you understand how your data is being used, and gives you control over when it’s shared. In addition to offering the existing data privacy permissions from our other platforms, visionOS includes control over sharing hand movement and surroundings data with apps. Additionally, the Guest User feature gives you control over what content friends and family members are able to see when they use your Apple Vision Pro.

Security
Security is the foundation of privacy. Optic ID data is encrypted and never leaves your device. Optic ID uses the Secure Enclave, a special subcomponent of the M2 chip, to store and protect your sensitive biometric data.

Data minimization

- The system handles camera and sensor inputs without passing the information to apps directly



When you look at button, visionOS highlights that button without revealing to the app what you are looking at.

Challenge: Privacy-functionality tradeoffs

Apple Vision Pro is crippled by privacy in 2 major ways

I'm all in on the vision of "spacial computing" as distinct from "VR" but imo apple has missed the mark in limiting the kinds of apps we can build on visionOS. I understand why they might want limitations early on to test the waters and ease adoption, but i really think if these aren't corrected relatively soon it will be passed over as a dead ecosystem once the novelty wears off.

The killer feature for mixed reality is bidirectional interaction with the environment, but visionOS lacks programmatic access to both eye tracking and dynamic environments.

I think eye tracking is self explanatory but by dynamic environment i mean things like dynamically loading AR anchors instead of needing to hardcode them in the assets, or texture extraction/manipulation like you would need for a snapchat style filters app, handwriting recognition, etc.

almost every transformative application i can think of for headsets is barred behind these two features.

i know everyone is saying that ofc the first iteration has room for improvement but i'm really worried because these aren't technical limitations, they're intentional tradeoffs core to apple's philosophy of privacy. so unless they have a major change of heart, or users warm up to the reality, we'll never see these features.

Im optimistic that apple has seen this far and is just being really cautious with controlling the rollout but idk as a developer its still frustrating to wonder.

what do you think?

https://www.reddit.com/r/VisionPro/comments/19c0t7s/apple_vision_pro_is_crippled_by_privacy_in_2/

Transparency and control

- In the few cases where the app actually needs access to **hand position or information about the user's surroundings**, the system requires the app to **obtain authorization from the user** first.

Challenge: Reliance on self-regulation

Developer and user

Important

It's your responsibility to protect any data your app collects, and to use it in responsible and privacy-preserving ways. Don't ask for data that you don't need, be transparent about how you use the data you acquire, and respect the choices of the person whose data it is.

Challenge: Lack of fine-grained control support

Manage the information you share with people and apps

- *Control app tracking:* All apps are required to ask your permission before tracking you or your Apple Vision Pro across websites and apps owned by other companies for advertising or to share your information with a data broker. You can change permission later, and you can stop all apps from requesting permission.
- *Control what you share with apps:* You can review and adjust the data you share with apps, the location information you share, the sensor information you share, and how Apple delivers advertising to you in the App Store, Apple News, and Stocks.
- *Review the privacy practices of apps:* Get more info about an app in the App Store for a developer-reported summary of the app's privacy practices, including what data is collected. For the apps that you download, review the App Privacy Report, which shows you how apps are using the permissions you granted them.

https://support.apple.com/guide/apple-vision-pro/use-built-in-privacy-and-security-protections-tan9ae59af9/visionos

Announcements

- Feedback on the midterm presentation has been released
- Go to the OH if you have questions (Wed 1-2pm, by appointment)
- XR Privacy reading commentaries due this Wednesday 12pm
- For the discussion leads: Do a deep dive in the paper itself (allocating at least 10 minutes)
- No class next Monday; Next Wednesday is a lecture.