www.
swiss
cyber
storm
.com

Kavya Pearlman

Founder & CEO, XSRI

A primer on security and safety in eXtended / Augmented Reality environments (XR)

@KavyaPearlman

THE XRSI MISSION

Help Build
Safe and Inclusive
Immersive
Environments.

https://youtu.be/hdcRs7ChXt4

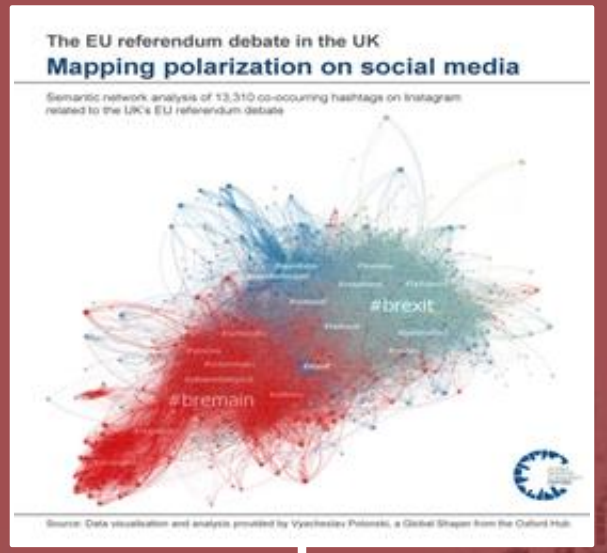
www.swisscyberstorm.com

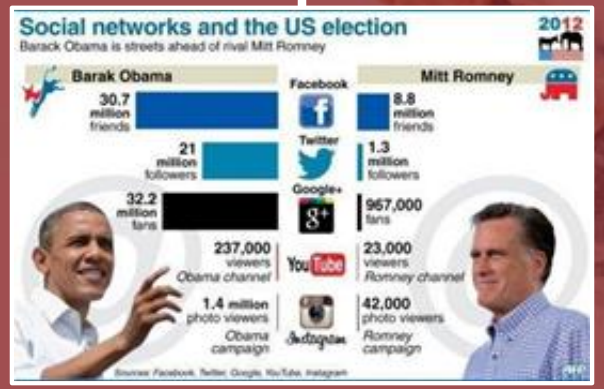
www.xrsi.org
@xrsidotorg

HOW IT STARTED..

I Like...

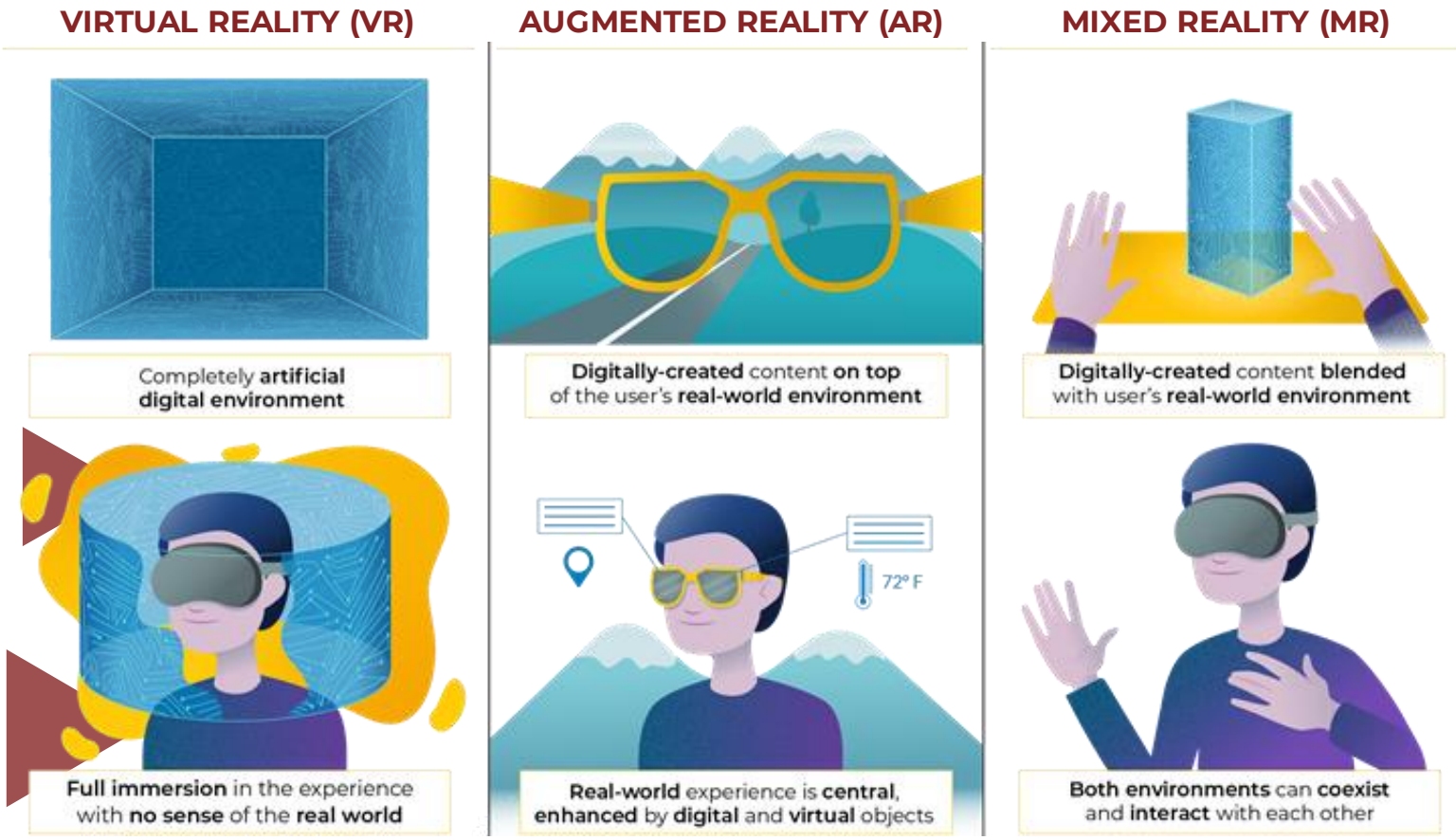
Technology impacts society and politics





XR

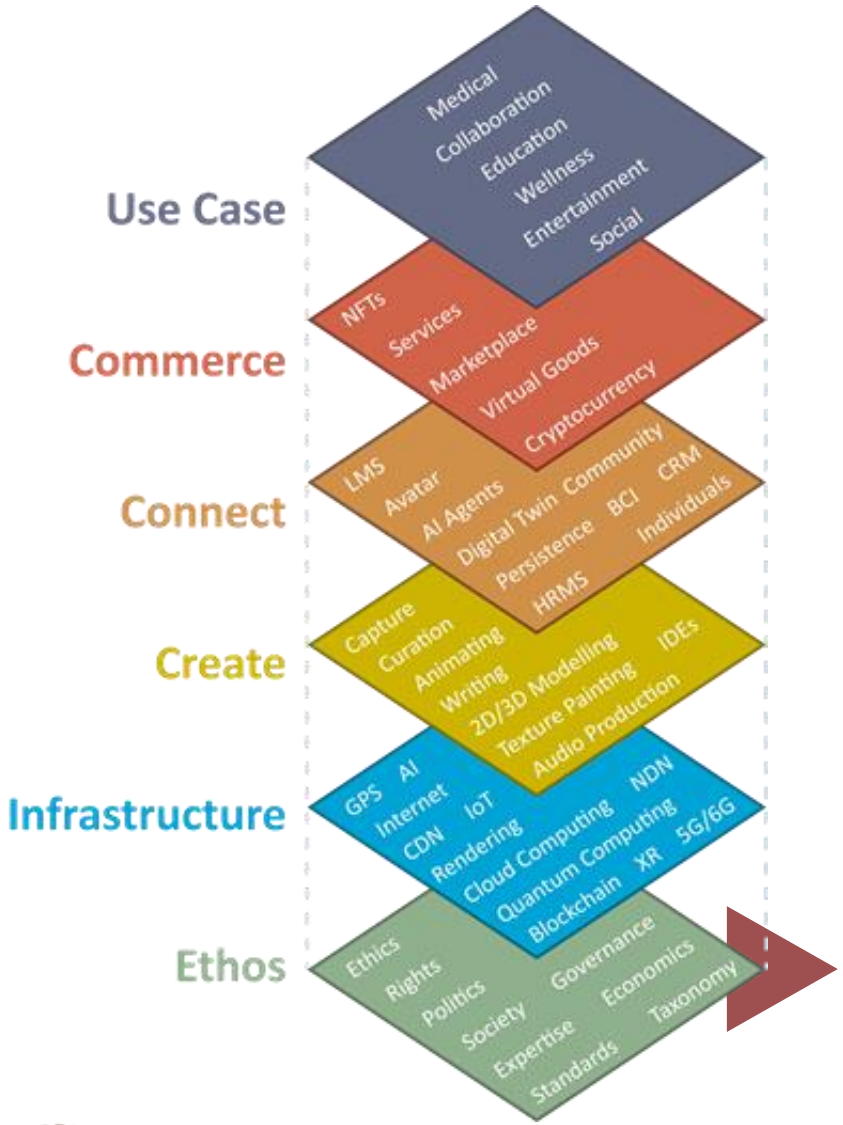
Augmented vs Virtual vs Mixed Reality



www.swisscyberstorm.com

@xrsidotorg

Anatomy of the Metaverse



Considerations at every level

Diversity & Inclusion	Accessibility & Digital Divide	Identity Protection
Privacy & Anonymity	Safety & Security	Ethics & Standards

The metaverse will allow humans to Create, Connect, do Commerce and even get medical assessment, diagnosis, treatment, and therapy by using various converging technologies. This creates significant challenges and raises questions that need to be addressed.

The Collingridge Dilemma

"The social consequences of a technology cannot be predicted early in the life of the technology. When change is easy, the need for it cannot be foreseen; when the need for change is apparent, change has become expensive, difficult and time-consuming."

-David Collingridge

A DOUBLE-BLIND PROBLEM FOR THE XR DOMAIN

- An information problem: impacts cannot be easily predicted until the technology is extensively developed and widely used.
- A power problem: control or change is difficult when the technology has become fully entrenched. (Tech Liberation, 2021)

Cambridge Analytica

5000 data points per user

Alexander Nix

former Cambridge Analytica CEO and director of Strategic Communication Laboratories

at Iowa caucus, 2016

LOCATION AND NAVIGATION

AR COLLABORATION AND GAMING

TELEPORTATION

CONTEXTUALIZED AI

CONSIDERATION

Safety | Privacy
Unintended Effects
Societal Impact
User Harm
Equitable Tech
Data Transparency
Data Ownership

A whole new level of data mining

In latest-generation HMDs, body movements are tracked **90 times per second**.

The systems record
18 types of movements
across the head and hands.

20 minutes
in a VR simulation
=
2,000,000
unique recordings of body language

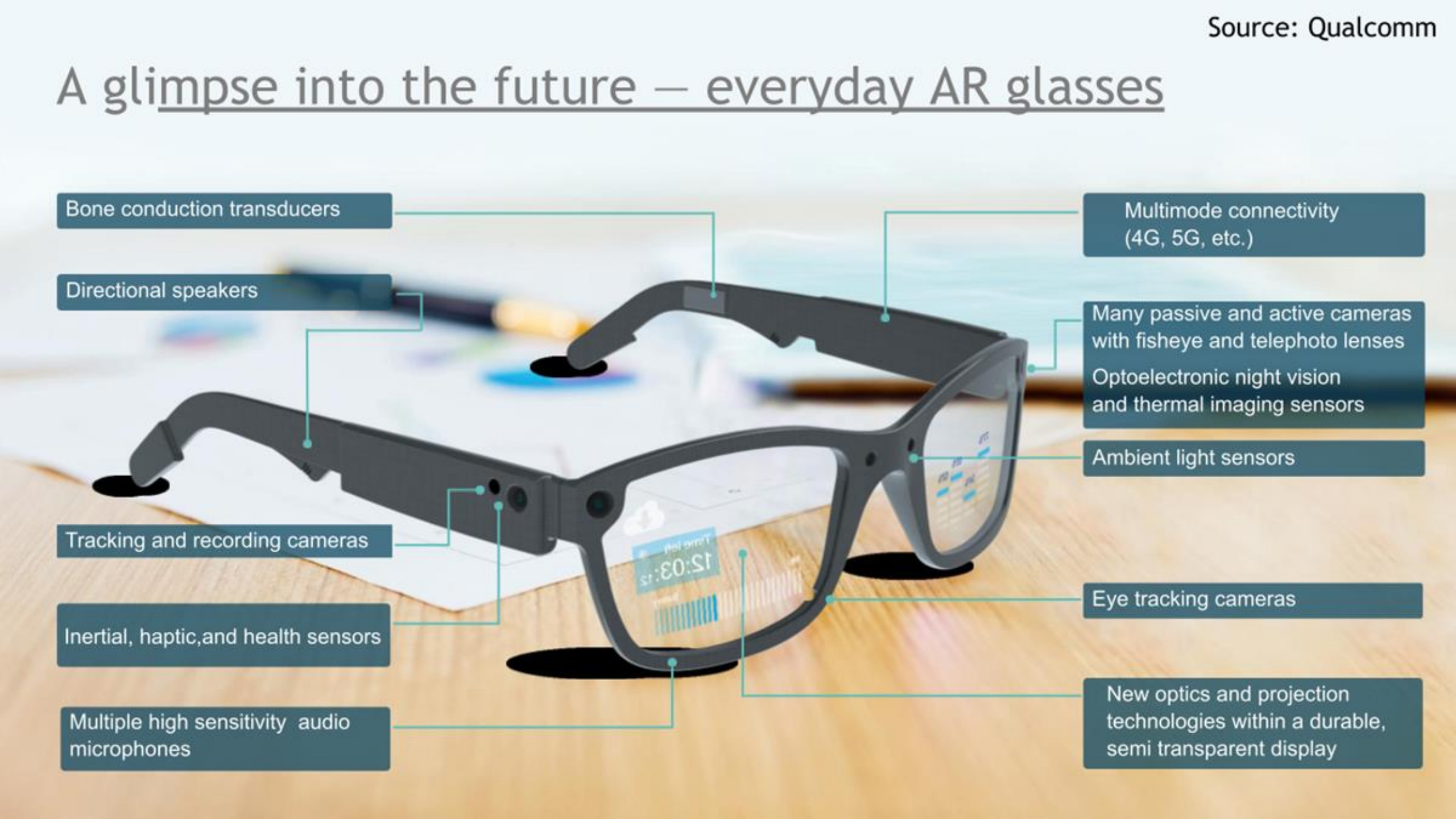
https://vhil.stanford.edu/mm/2018/08/bailenson-jamap-protecting-nonverbal.pdf

www.swisscyberstorm.com

www.xrsi.org
@xrsidotorg

Source: Qualcomm

A glimpse into the future — everyday AR glasses



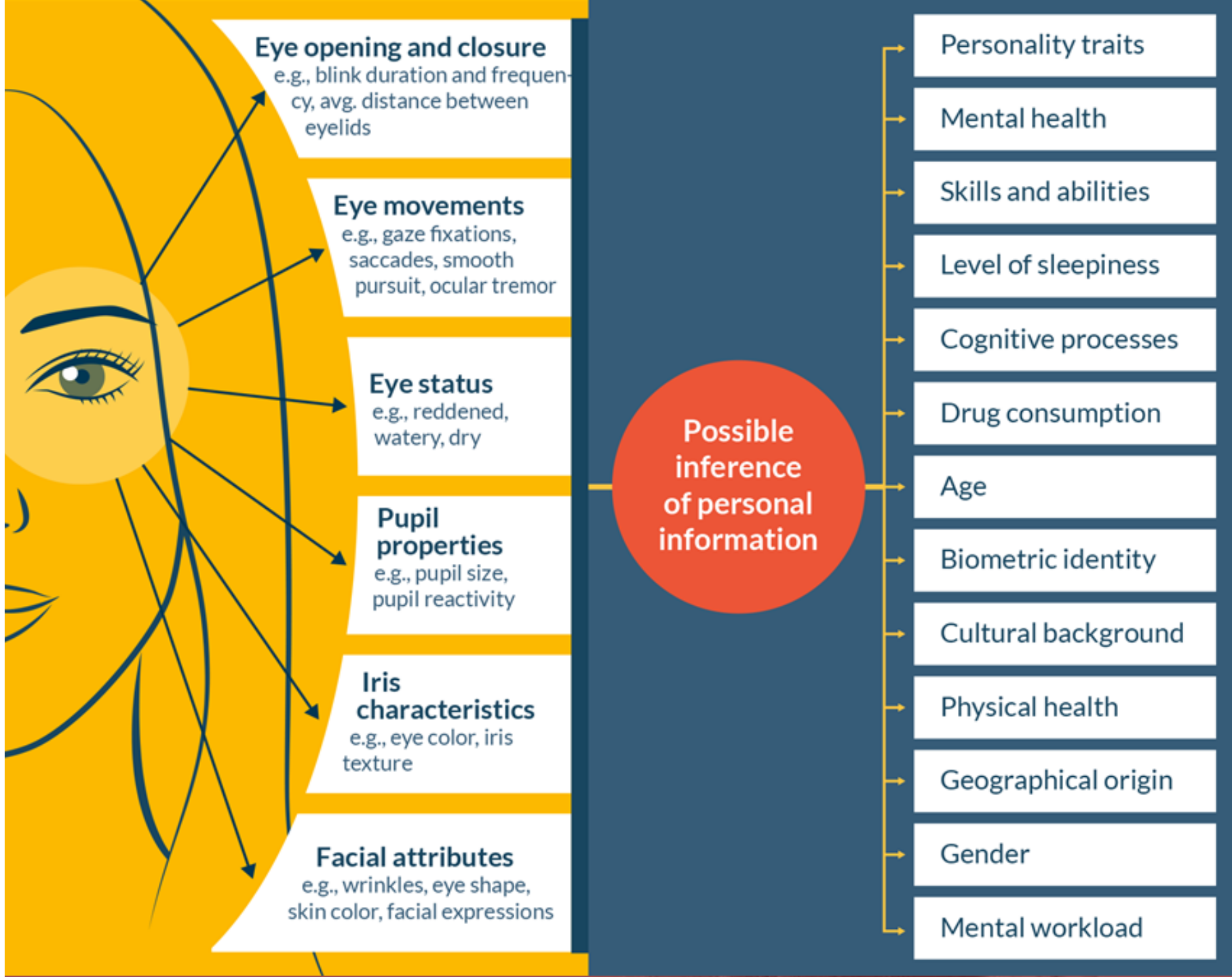
How is it going?

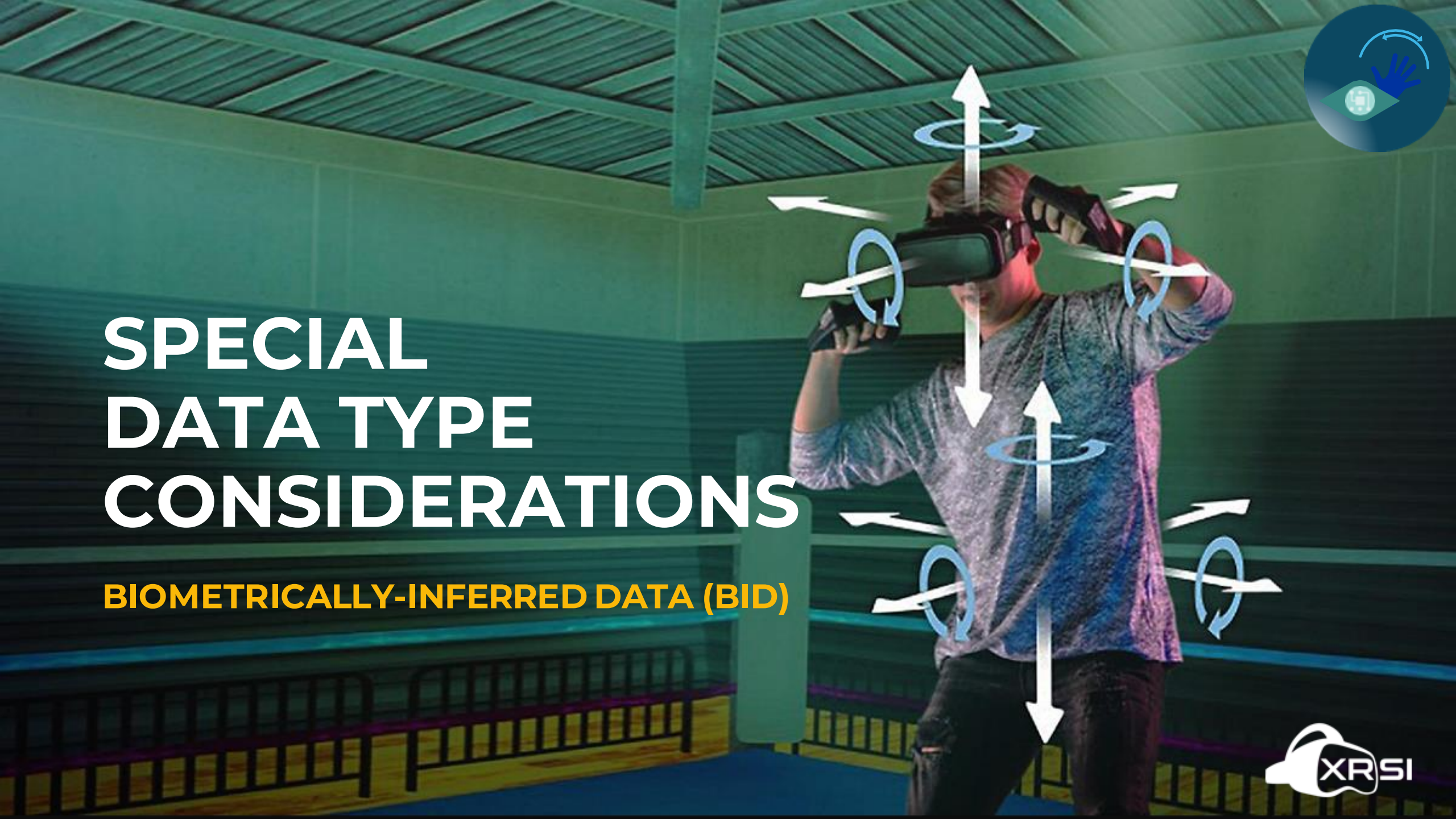
WHAT DOES THE FUTURE LOOK LIKE?

Source: Qualcomm

SPECIAL DATA TYPE CONSIDERATIONS

BIOMETRICALLY INFERRED DATA (BID)

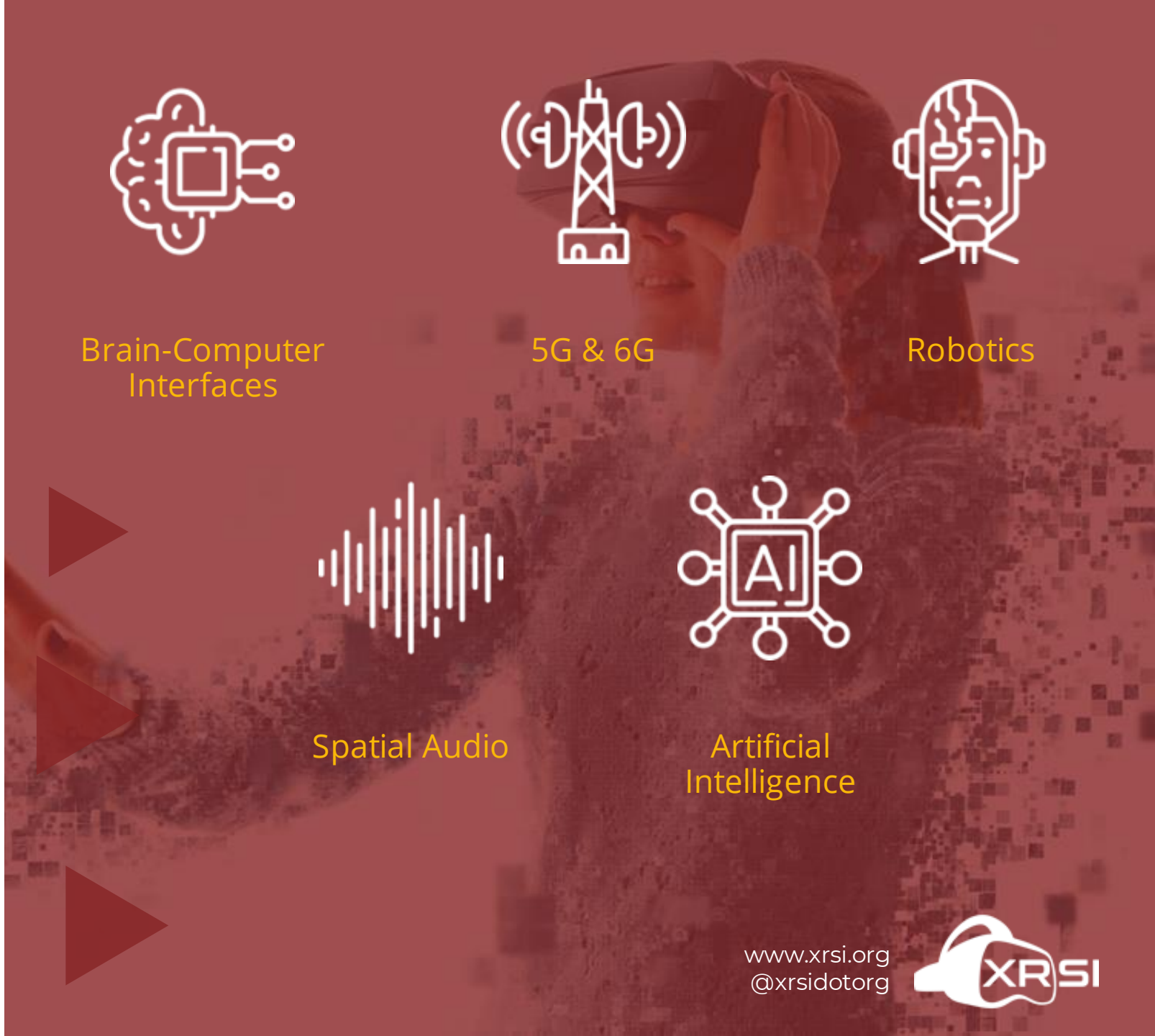




SPECIAL DATA TYPE CONSIDERATIONS

BIOMETRICALLY-INFERRED DATA (BID)

Intersection of XR Technologies and research opportunities



www.swisscyberstorm.com

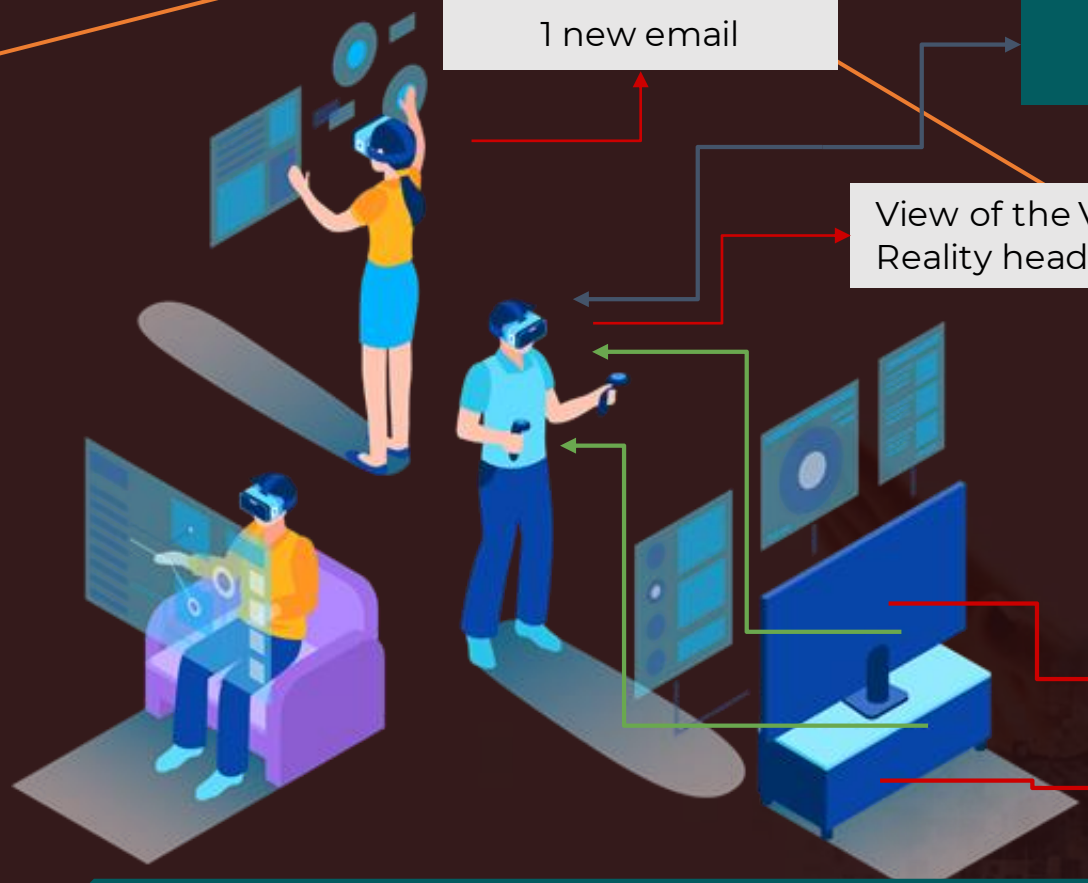
www.xrsi.org
@xrsidotorg

VIRTUAL REALITY ATTACKS

VR Attack Surface

VR Attack Surface

Source: Casey, P., Baggili, I., & Yarramreddy, A. (2019). Immersive Virtual Reality Attacks and the Human Joystick. IEEE Transactions on Dependable and Secure Computing.



1 unread message

1 new email

User Data

View of the Virtual Reality headset

Social Networks

Web Services

Applications

Social Network Data

Web Service Data

Remote Application Data

Samsung display

IKEA furniture

Output data flow

Input data flow

In-network data flow

Virtual Reality Environment ⟷ Supporting Data Services

Novel attacks in VR

TRACKER ATTACK
Look where you are exactly

CHAPERONE ATTACK
Remove your safety boundaries

HUMAN JOYSTICK ATTACK
Move you wherever we want

OVERLAY ATTACK
Block your vision

Source: Casey, P., Baggili, I., & Yarramreddy, A. (2019). Immersive Virtual Reality Attacks and the Human Joystick. IEEE Transactions on Dependable and Secure Computing.

Tracker Attack

Turn on front facing camera

Stream video feed

back to attacker

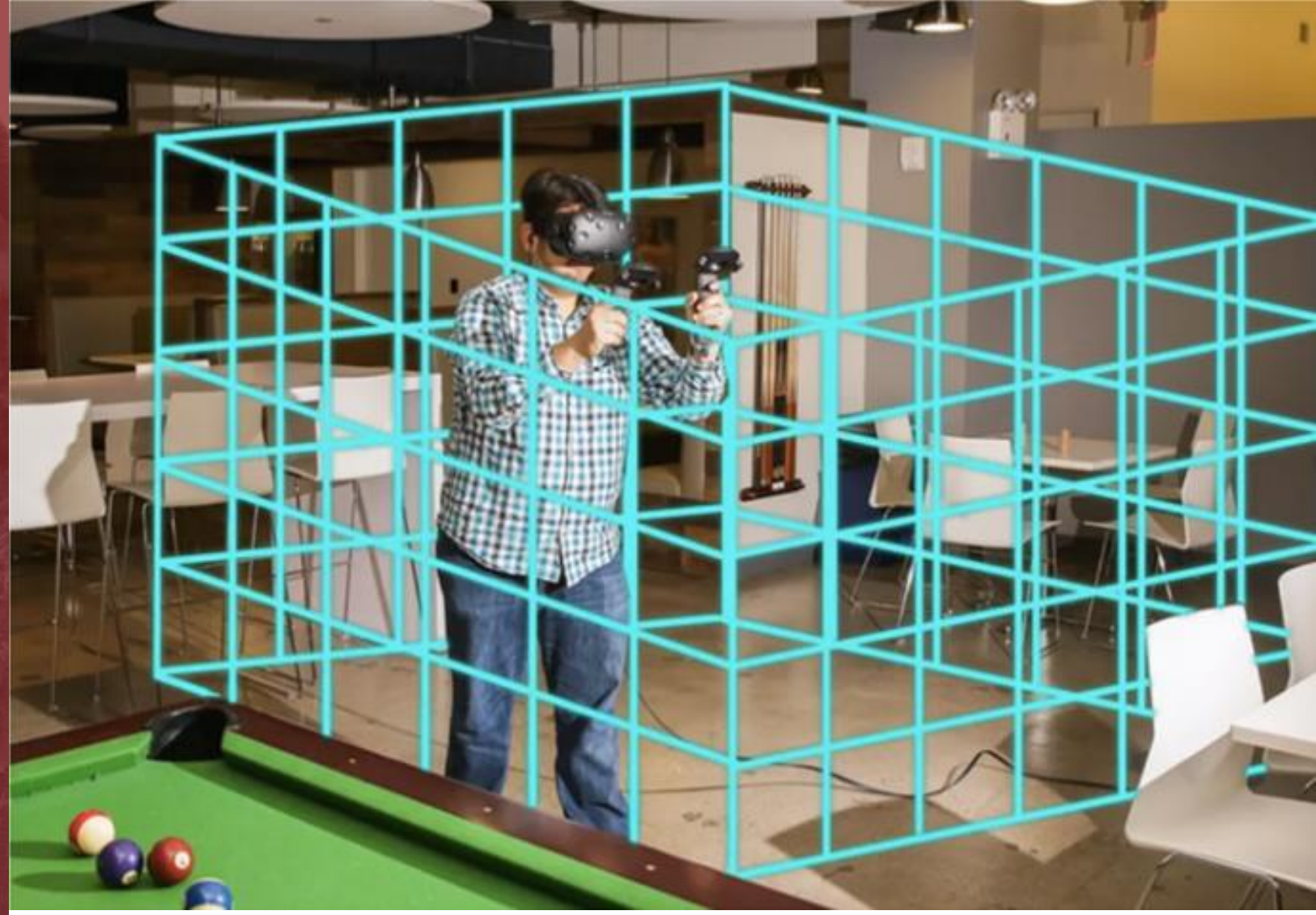
Look inside victim's room

Even if the cam

is disabled by the user

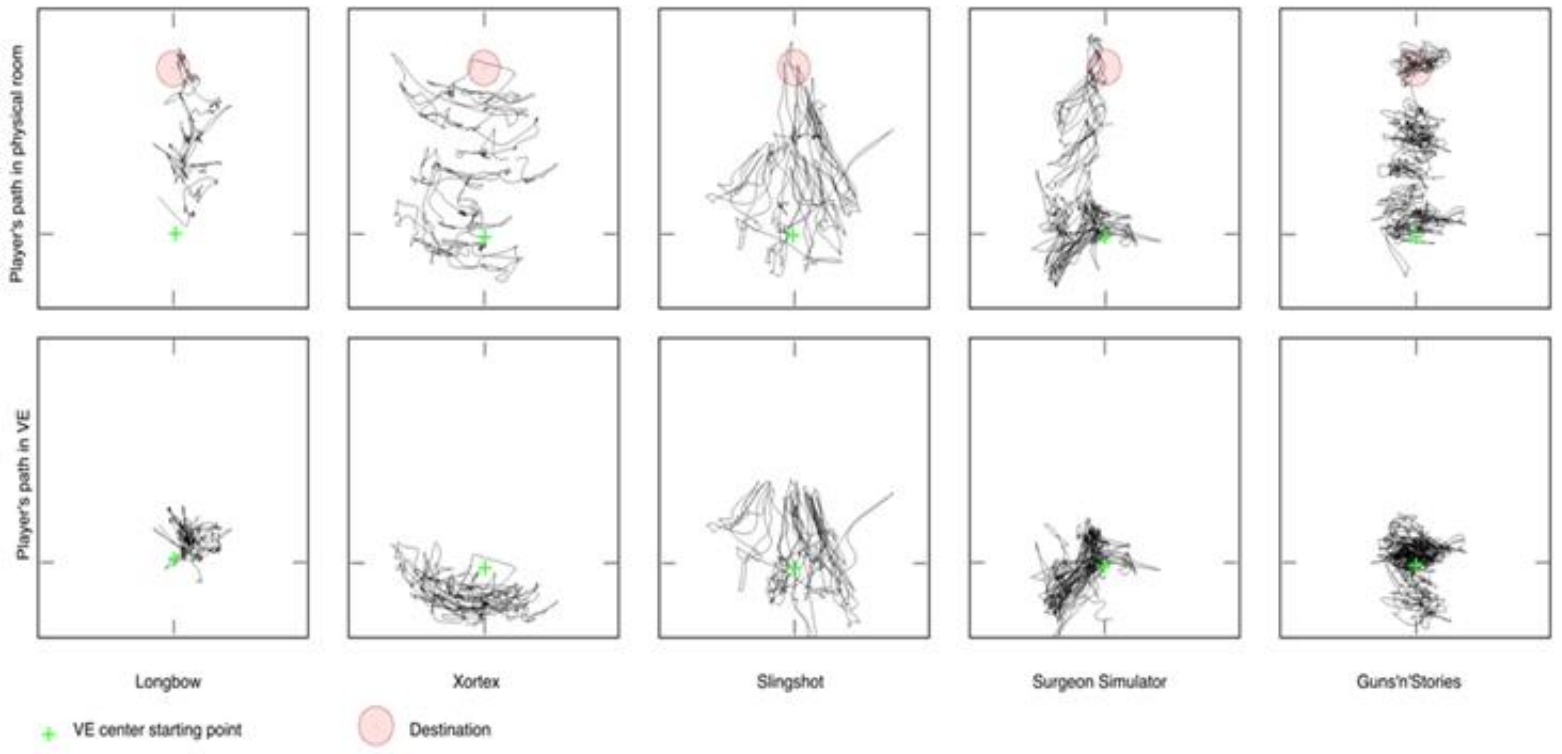
Source: Casey, P., Baggili, I., & Yarramreddy, A. (2019). Immersive Virtual Reality Attacks and the Human Joystick. IEEE Transactions on Dependable and Secure Computing.

Chaperone Attack



Source: Casey, P., Baggili, I., & Yarramreddy, A. (2019). Immersive Virtual Reality Attacks and the Human Joystick. IEEE Transactions on Dependable and Secure Computing.

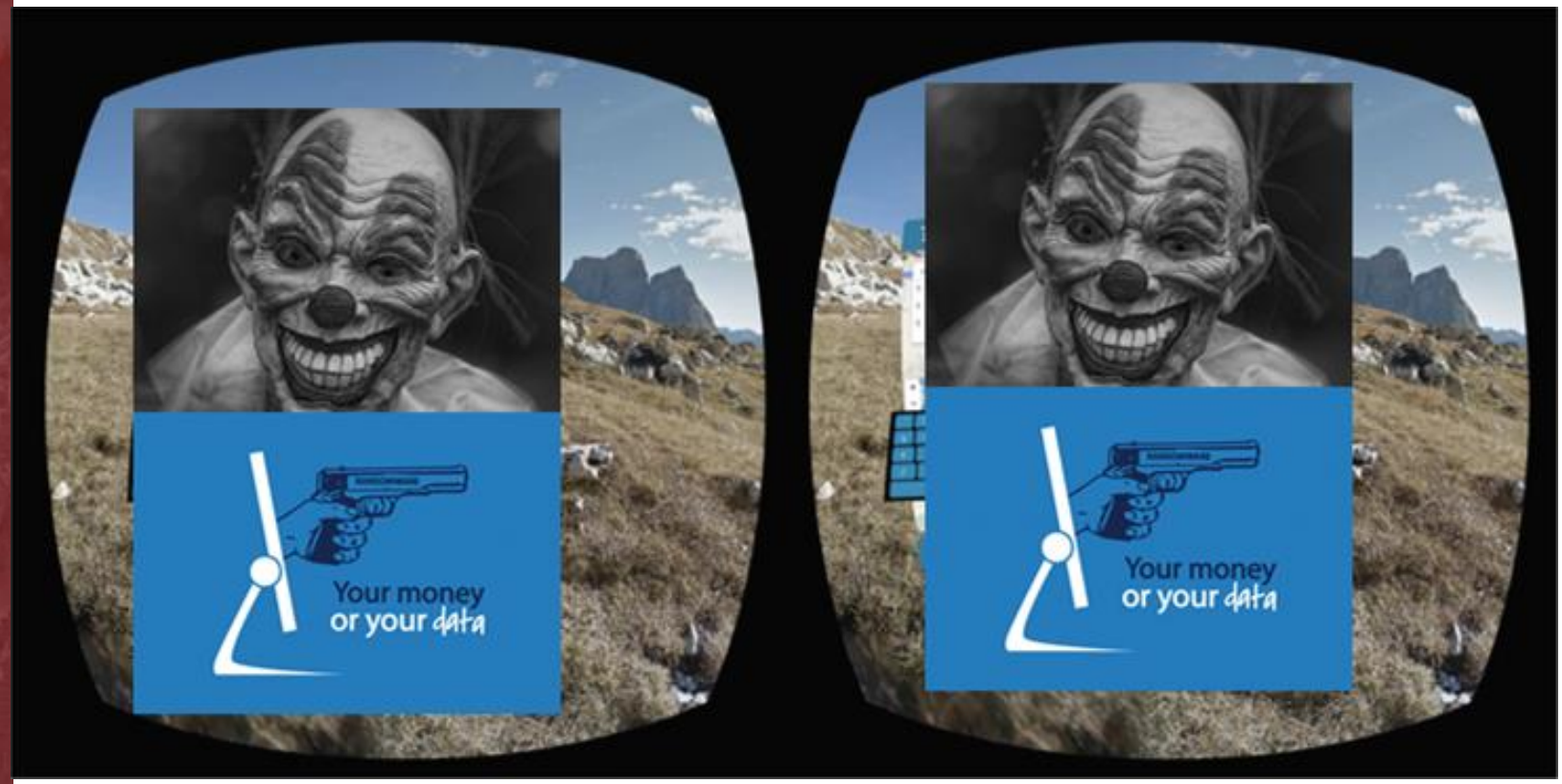
Human Joystick Attack



Source: Casey, P., Baggili, I., & Yarramreddy, A. (2019). Immersive Virtual Reality Attacks and the Human Joystick. IEEE Transactions on Dependable and Secure Computing.

Overlay Attack

a new type of **Ransomware**?



Source: Casey, P., Baggili, I., & Yarramreddy, A. (2019). Immersive Virtual Reality Attacks and the Human Joystick. IEEE Transactions on Dependable and Secure Computing.

Risk Mitigation Categories

Data Protection

Ensure I/O including data aggregated by system for use by third-party applications is properly stored and protected

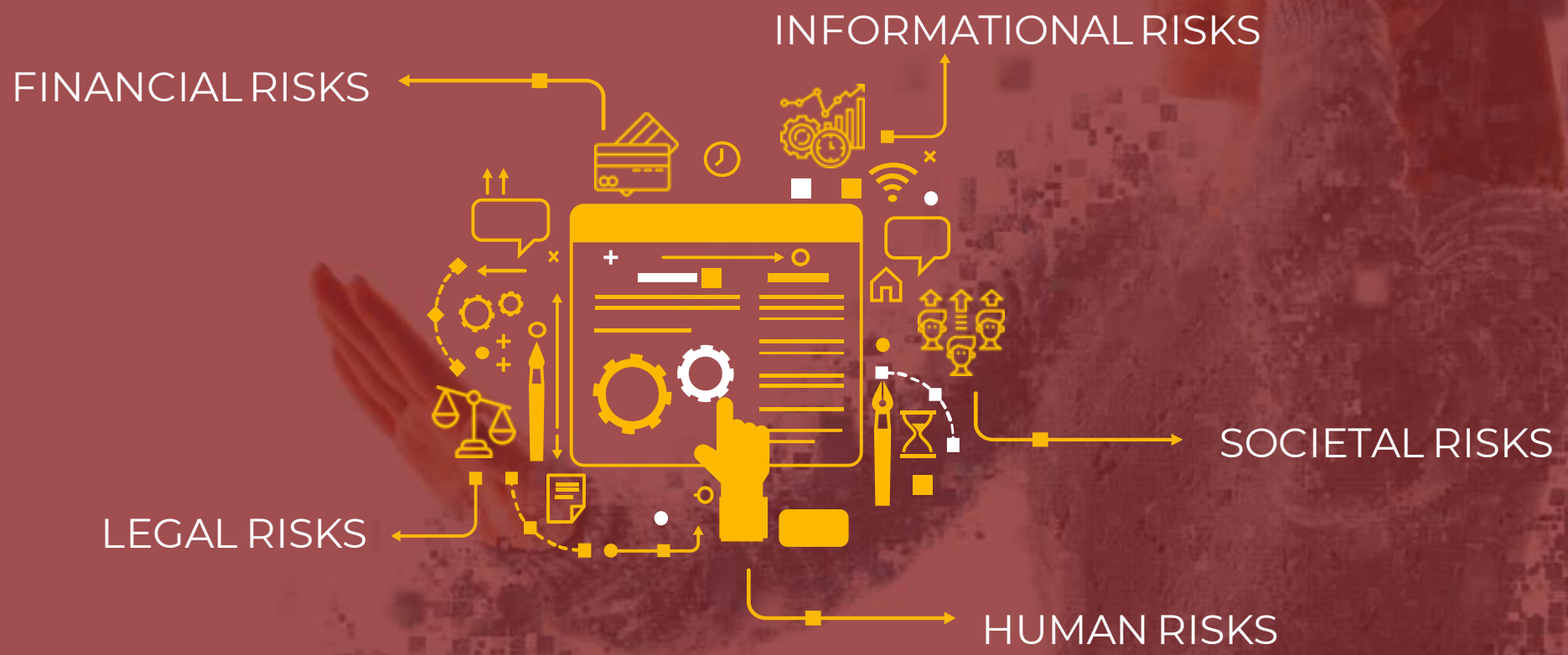
User Interaction Protection

Users can share virtual environments, their interactions and information within the VE should be protected

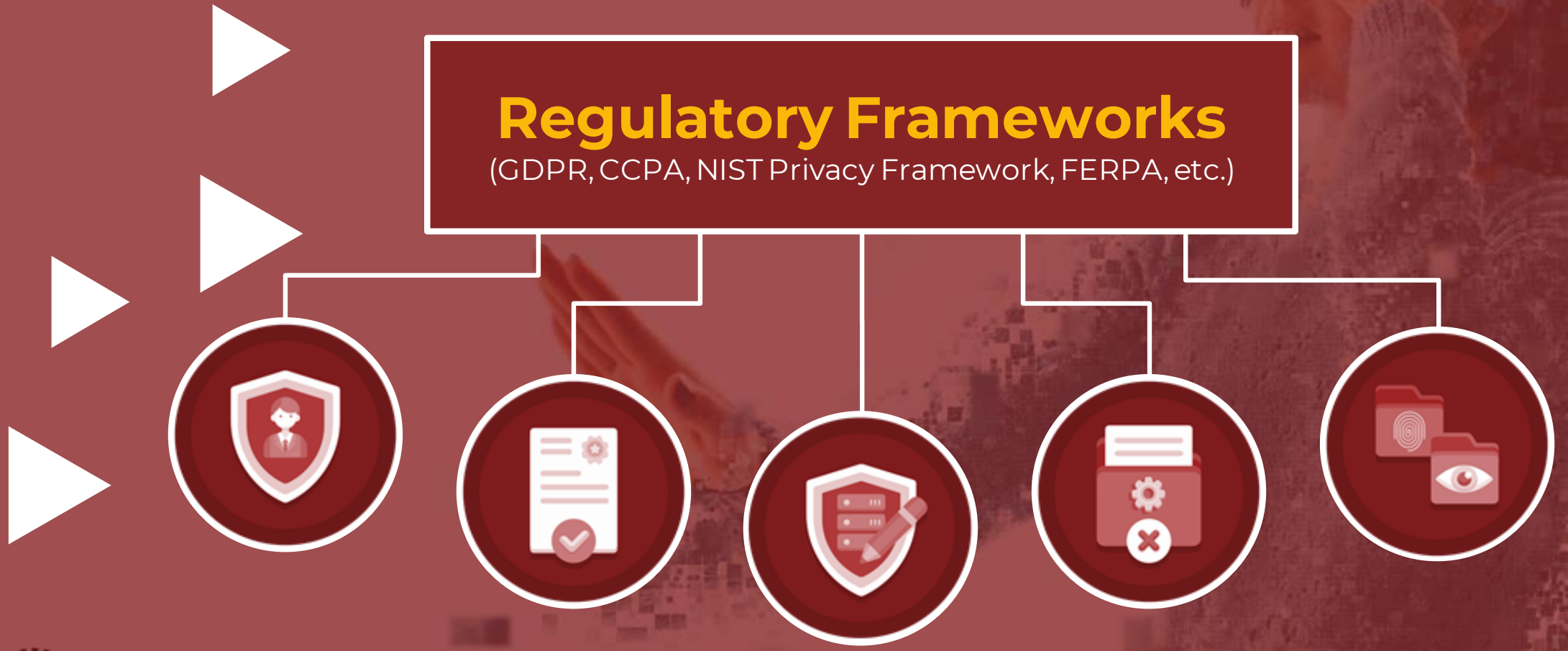
Device Protection

Protecting the physical devices and their data.

Consideration of Novel Risks

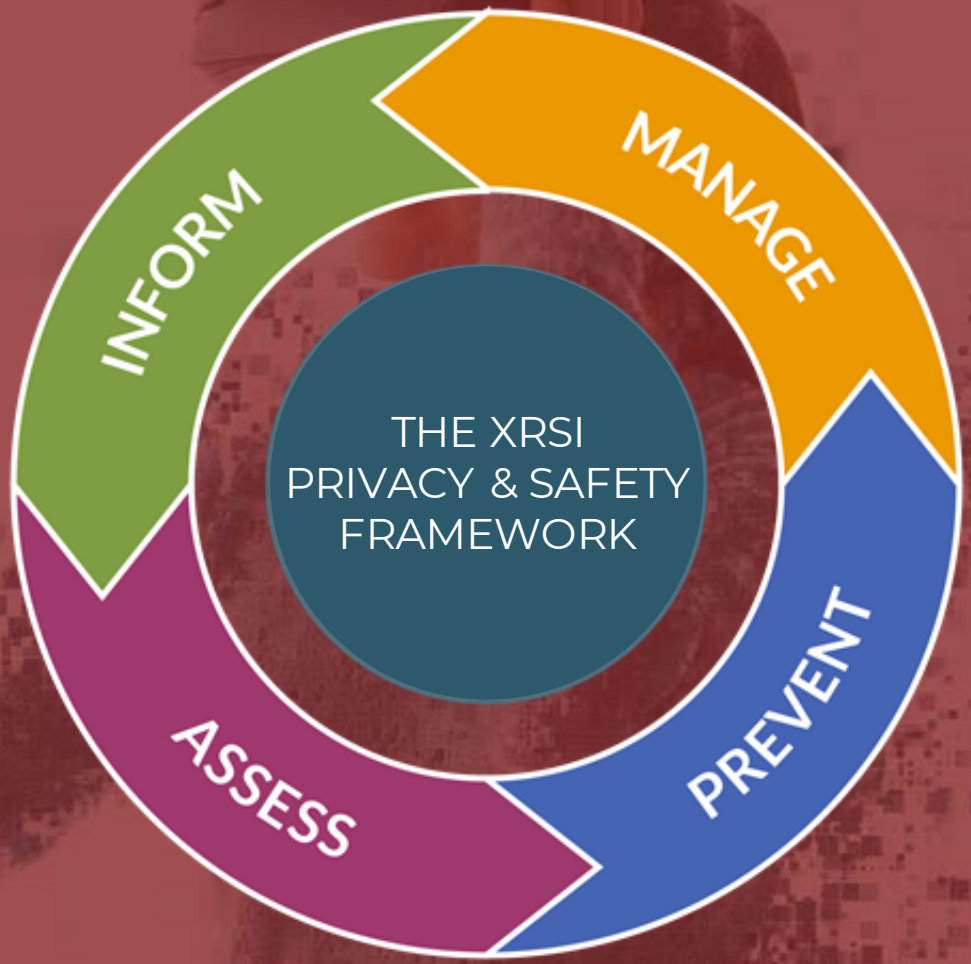


Are regulations the answer?



The XRSI Privacy & Safety Framework

Version 2.0 Development Ongoing



www.swisscyberstorm.com

www.xrsi.org
@xrsidotorg

XRSI Policy and Advisory Task Force and **Medical XR Council** are helping global regulatory bodies draft **responsible** policies and laws

1. CAMRA ACT in the United States
1. KIDS and PRIVCY ACT in the United States
1. AR/VR Positioning Statement for eSafety Commissioner of Australia
1. Cybersecurity Research and positioning statement for British Health Services via NHSx and HEE-NHS, UK
1. Advising Facebook Reality Labs and many other big tech orgs on self-regulating Frameworks and Policies

Swiss Cyber Storm 2021
www.swisscyberstorm.com
October 12, 2021

THANK YOU!

THINK. COLLABORATE. DONATE.

Kavya Pearlman

CyberGuardian – CEO and Founder - XR Safety Initiative

www.xrsi.org | medical.xrsi.org

kavya@xrsi.org | info@xrsi.org

@KavyaPearlman | @XRSIdotOrg | @XRSafetyMedical

kavyapearlman | xrsidotorg