PRIVACY IN THE METAVERSE

MetaGuard

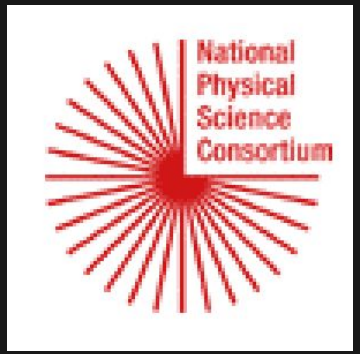
VIVEK NAIR

UC Berkeley
vcn@berkeley.edu

GONZALO MUNILLA GARRIDO

TU Munich
gonzalo.munilla-garrido@tum.de

Acknowledgments



TECH

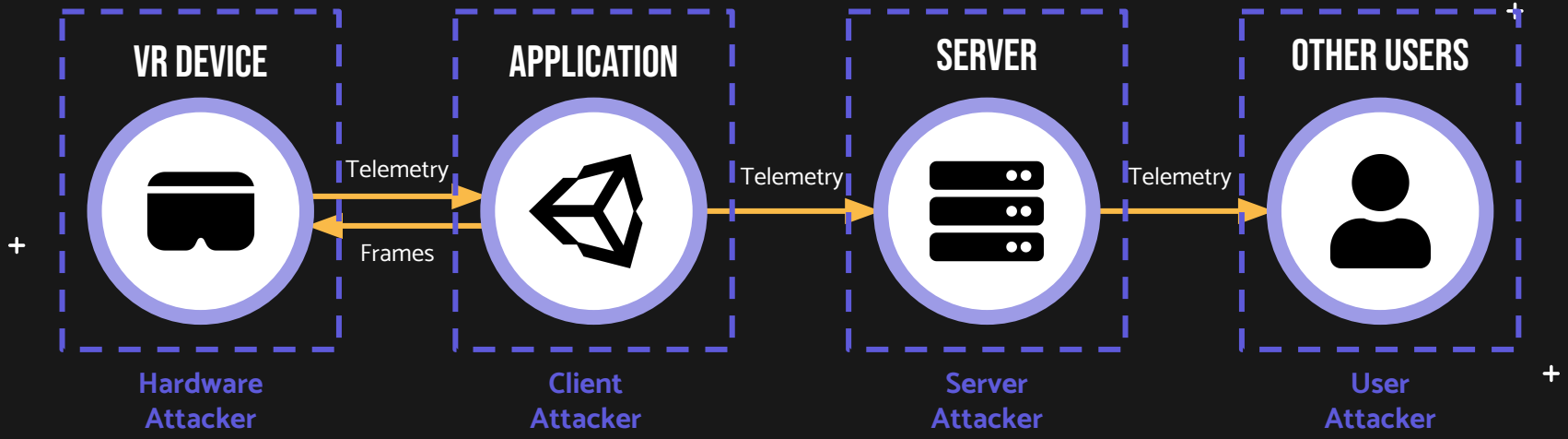
Mark Zuckerberg's 'metaverse' business lost more than $10 billion last year, and the losses keep growing

PUBLISHED WED, FEB 2 2022•5:06 PM EST | UPDATED WED, FEB 2 2022•7:26 PM EST

Steve Kovach
@STEVEKOVACH

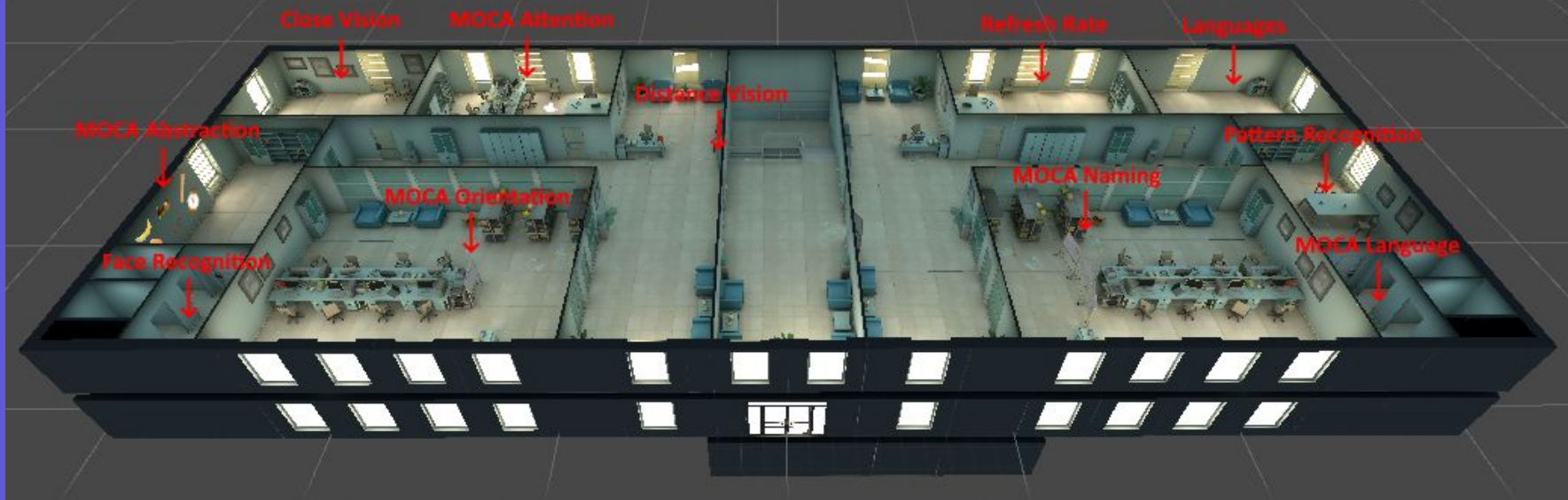
SHARE

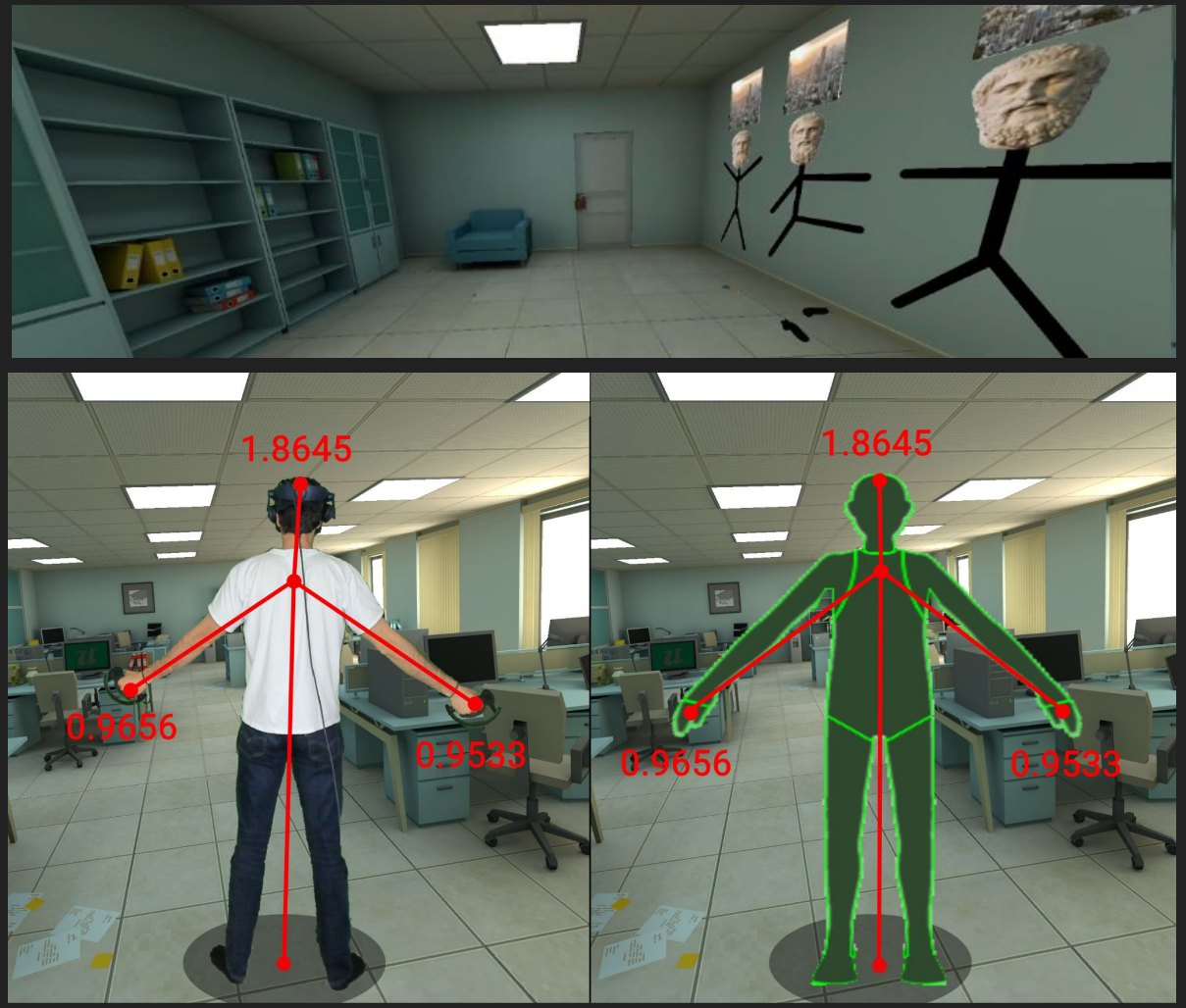
VR INFORMATION FLOW



THE “METADATA” STUDY

Harvesting user data in VR

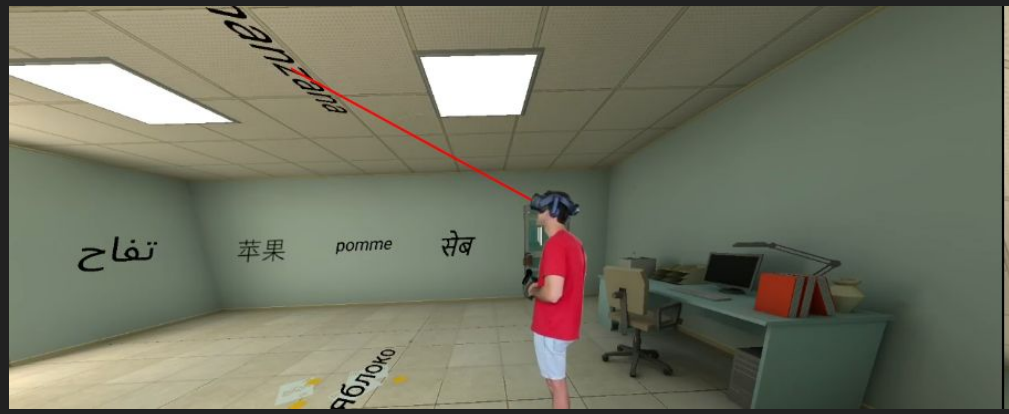



1.8645
0.9656
0.9533
1.8645
0.9656
0.9533


PRESS
PRESS
The world is,
course,
thing
our
ception
it.
The
of
noth
but

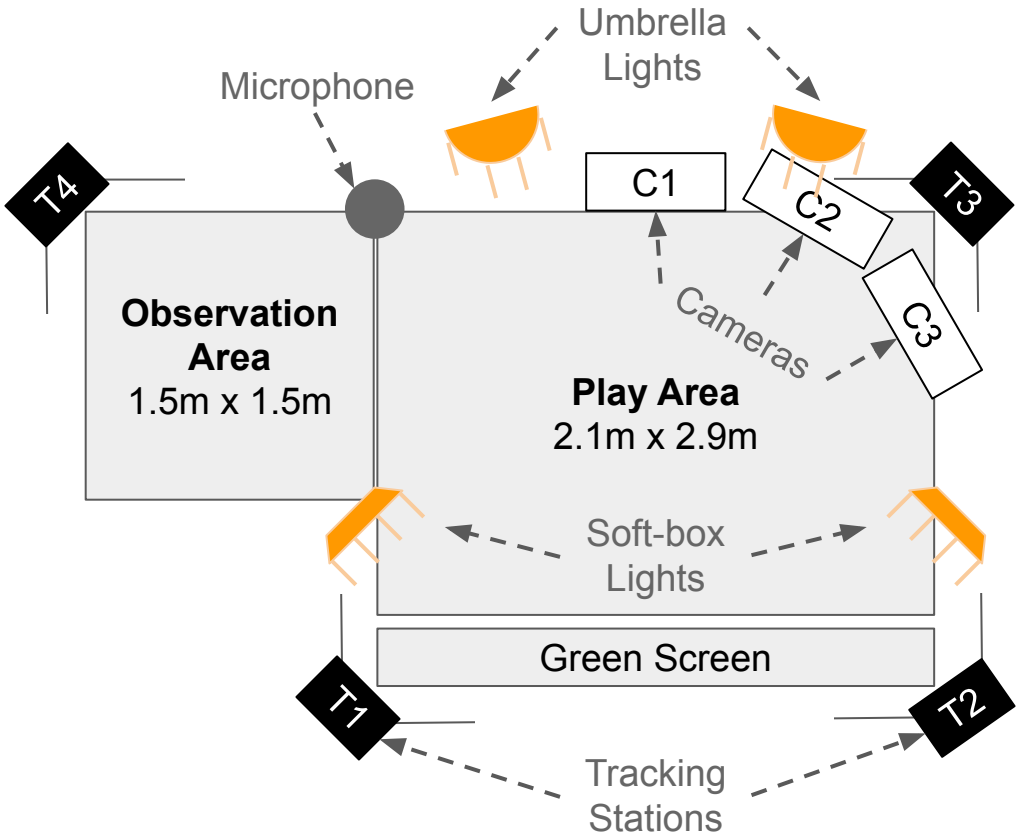

LIFE
ISBETTER
WITHINTHE

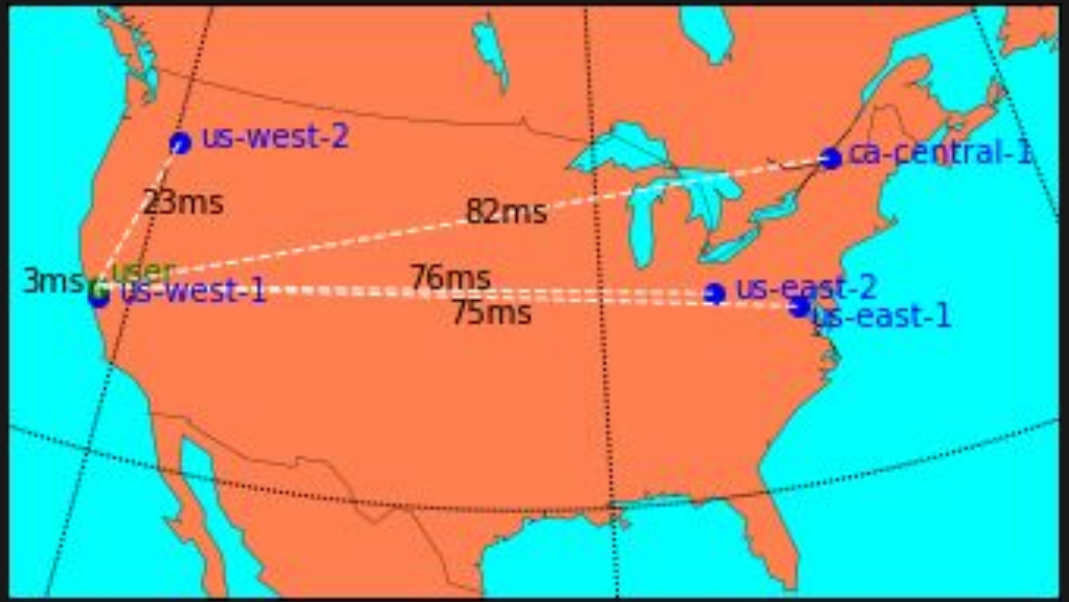

THE
CODEIS
EQUALTO

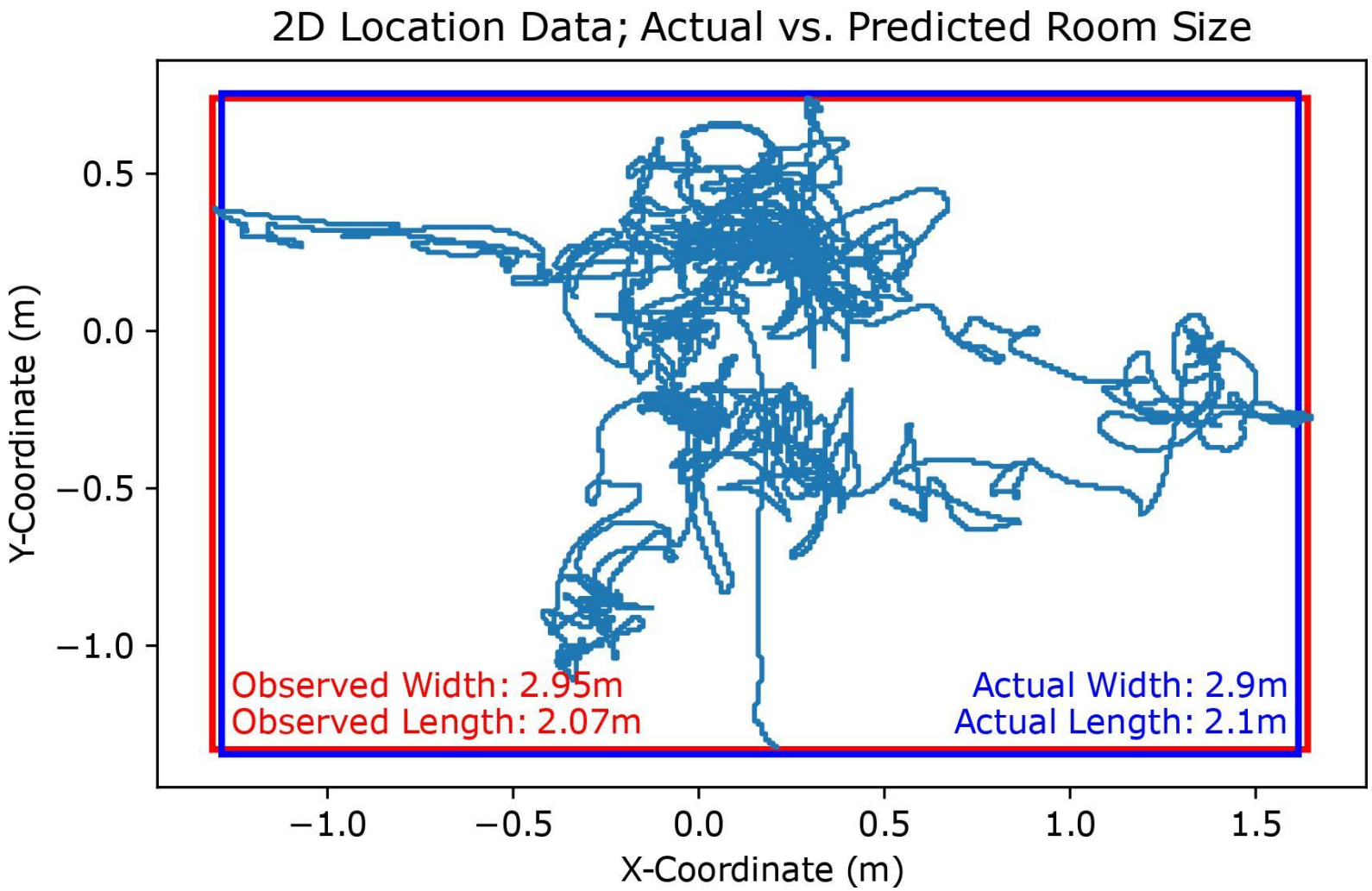

manzana
تفاح
苹果
pomme
सेब
яблоко


manzana

EXPERIMENT SETUP




us-west-2
ca-central-1
23ms
82ms
3ms
user
us-west-1
76ms
us-east-2
75ms
us-east-1


2D Location Data; Actual vs. Predicted Room Size
Y-Coordinate (m)
X-Coordinate (m)
0.5
0.0
−0.5
−1.0
−1.0
−0.5
0.0
0.5
1.0
1.5
Observed Width: 2.95m
Observed Length: 2.07m
Actual Width: 2.9m
Actual Length: 2.1m

Attribute	Type / Source	Precision	Accuracy	Attackers
Height	Primary Telemetry	1 cm	70% within 5 cm 100% within 7 cm	Privileged I-III Non-Privileged*
Longer Arm	Primary Telemetry	boolean	64% for ≥ 1 difference 100% for ≥ 3 cm difference	Privileged I-III Non-Privileged*
Interpupillary Distance	Primary Telemetry	0.1 mm	96% within 0.5 mm (Vive Pro 2) 87% within 0.5 mm (All Devices)	Privileged I-II
Wingspan	Secondary Telemetry	1 cm	86% within 7 cm 100% within 12 cm	Privileged I-III Non-Privileged*
Room Size	Secondary Telemetry	1 m^2	78% within 2 m^2 97% within 3 m^2	Privileged I-III Non-Privileged*
Geolocation	Primary Network	100 km	50% within 400 km 90% within 500 km	Privileged II-III
HMD Refresh Rate	Primary Device	1 Hz	100% within 3 Hz (Privileged Attacker) 81% wtihin 60 Hz (Unprivileged Attacker)	Privileged I-II Privileged III* Non-Privileged*
Controller Tracking Rate	Primary Device	1 Hz	100% within 2.5 Hz	Privileged I-II Privileged III* Non-Privileged*
Device Resolution (MP)	Primary Device	0.1 MP	100% within 0.1 MP	Privileged I-II
Device FOV	Primary Device	10°	100% within 10°	Privileged I-II Privileged III* Non-Privileged*
Computational Power	Primary Device	0.1 GHz 10 Mh/s	CPU: 100% within 0.4 GHz GPU: 100% within 20 Mh/s	Privileged I-II
VR Device	Secondary Device	N/A	100%	Privileged I-III Non-Privileged*
Handedness	Primary Behavior	boolean	97%†	Privileged I-III Non-Privileged
Eyesight	Primary Behavior	boolean	70% (Hyperopia) 81% (Myopia)	Privileged I-III Non-Privileged
Color Blindness	Primary Behavior	boolean	100%	Privileged I-III Non-Privileged
Languages	Primary Behavior	boolean	88%	Privileged I-III Non-Privileged
Physical Fitness	Primary Behavior	boolean	90%	Privileged I-III Non-Privileged
Reaction Time	Primary Behavior	17 ms	88%	Privileged I-II Privileged III* Non-Privileged*
Acuity (MoCA)	Primary Behavior	1 point	81% within 1 point 90% within 2 points 100% diagnostic accuracy	Privileged I-III Non-Privileged

Gender	Inferred Classification	boolean	100%	Privileged I-III Non-Privileged
Age	Inferred Regression	1 yr	100% within 1 yr	Privileged I-III Non-Privileged
Ethnicity	Inferred Classification	categorical	100%	Privileged I-III Non-Privileged
Income	Inferred Regression	$1k	100% within $25k	Privileged I-III Non-Privileged
Disability Status[‡]	Inferred Classification	boolean	100%	Privileged I-III Non-Privileged

Forbes

MONEY • EDITORS' PICK

Worried Your Phone Is Spying On You? Just Wait Until You're In The Metaverse

Dylan Sloan Contributor ⓘ

I am a graduate of Bowdoin College currently living in New York City.

Follow

The Register®

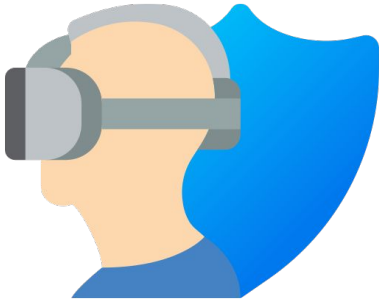
{* PERSONAL TECH *}

Surprise! The metaverse is going to suck for privacy

Forget mobile apps – headsets and smart glasses will be able to harvest so much data

Thomas Claburn in San Francisco

Fri 29 Jul 2022 // 07:24 UTC



02.

DEFENSES

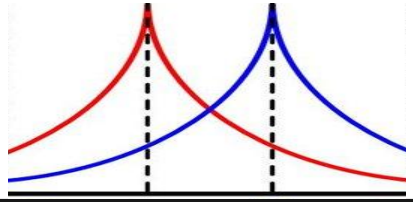
DIFFERENTIAL PRIVACY

ε-DIFFERENTIAL PRIVACY

Definition 1. *(ε-Differential Privacy [25]). A randomized function $\mathcal{M}(\cdot)$ is ε-differentially private if for all input datasets D and D' differing on at most one element, and for all possible outputs $\mathcal{S} \subseteq Range(\mathcal{M})$:*

$$\Pr[\mathcal{M}(D) \in \mathcal{S}] \leq e^{\varepsilon} \times \Pr[\mathcal{M}(D') \in \mathcal{S}].$$

BOUNDED LAPLACE MECHANISM



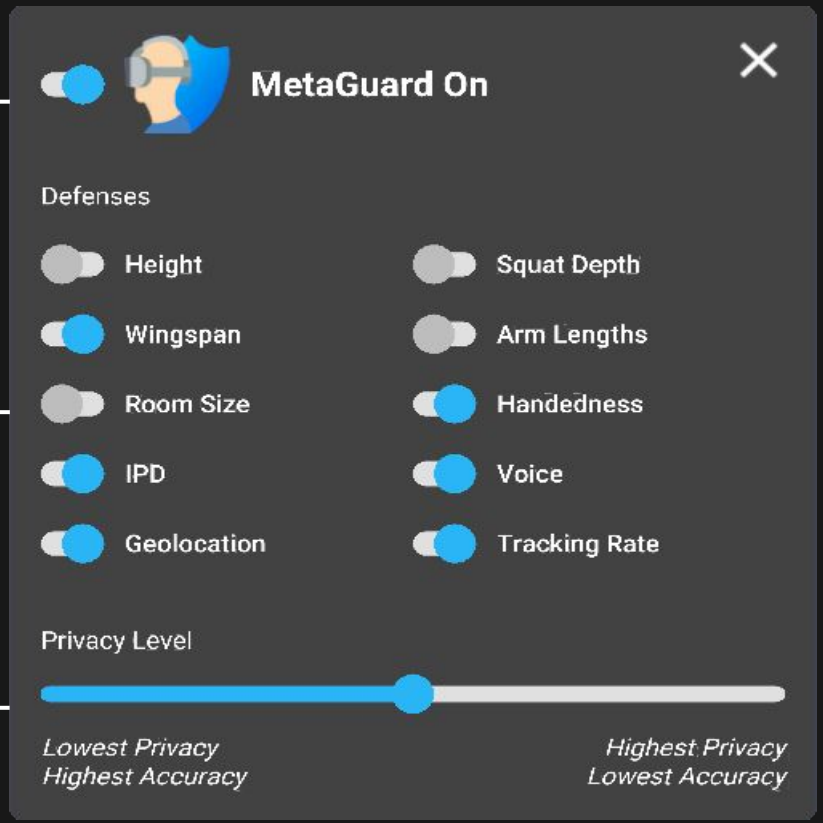
RANDOMIZED RESPONSE


Anonymous
MetaGuard Co

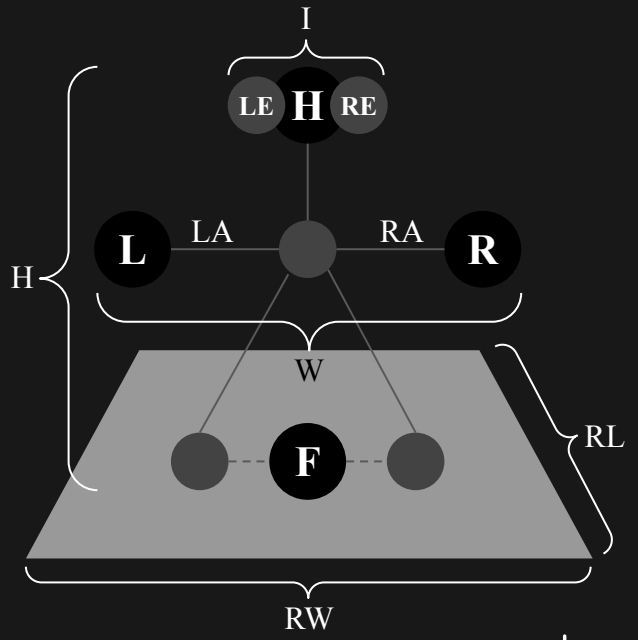
MASTER TOGGLE

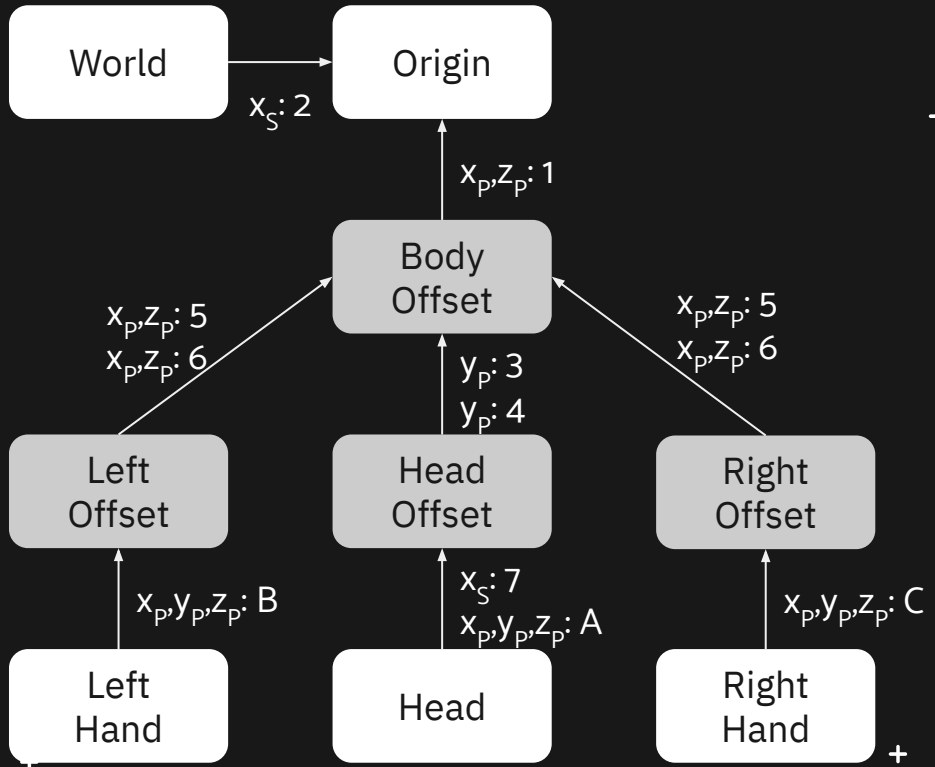
FEATURE TOGGLES

PRIVACY SLIDER



INSTANTANEOUS GROUND TRUTH





Key

x_P: Coordinate position

x_S: Coordinate scale

Transformations (Defenses)

1. Room Size Transform
2. Binary Transform
3. Height Transform
4. Fitness Transform
5. Wingspan Transform
6. Arm Transform
7. IPD Transform

Tracking (Telemetry)

A. Head Tracking

B. Left Hand Tracking

C. Right Hand Tracking

COORDINATE TRANSFORMATIONS

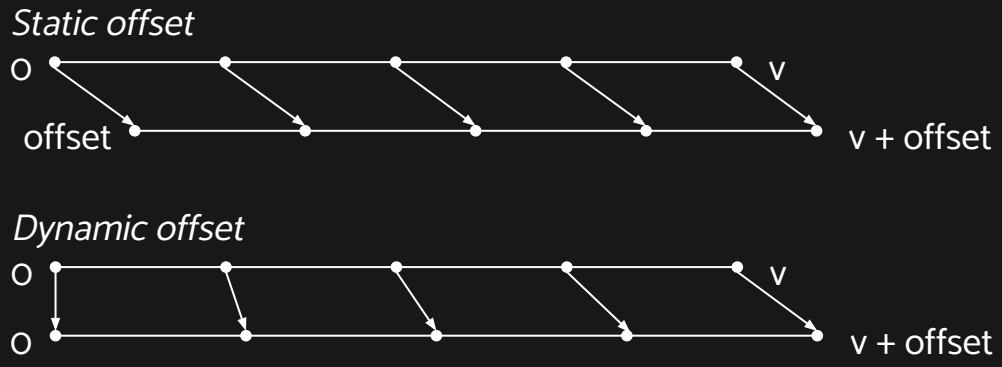


Table 3A: Primary and Secondary Attributes

Attribute	Metric	No Privacy	Low Privacy	Medium Privacy	High Privacy
Height	Within 5cm	70%	53.07% ±2.41%	45.00% ±2.35%	32.63% ±2.3%
	Within 7cm	100%	68.6% ±2.18%	58.17% ±2.09%	44.47% ±2.43%
	R^2	0.79	0.37 ±0.040	0.22 ±0.035	0.06 ±0.020
Physical Fitness	Categorical	90%	86.11% ±2.65%	79.11% ±2.60%	61.56% ±4.15%
IPD (Vive Pro 2)	Within 0.5mm	96%	18.53% ±1.76%	13.40% ±1.33%	11.10% ±1.24%
	R^2	0.991	0.399 ±0.041	0.165 ±0.031	0.068 ±0.019
IPD (All Devices)	Within 0.5mm	87%	19.47% ±1.81%	14.17% ±1.35%	12.17% ±1.26%
	R^2	0.857	0.318 ±0.038	0.134 ±0.027	0.068 ±0.017
Wingspan	Within 7cm	87%	53.93% ±3.61%	42.13% ±3.32%	40.80% ±2.80%
	Within 12cm	100%	78.80% ±2.76%	66.00% ±3.31%	65.46% ±3.14%
	R^2	0.669	0.134 ±0.042	0.047 ±0.019	0.036 ±0.021
Room Size	Within $2m^2$	78%	22.11% ±2.85%	16.33% ±2.74%	12.66% ±2.98%
	Within $3m^2$	97%	33.52% ±3.80%	23.44% ±3.08%	19.53% ±2.92%
	R^2	0.974	0.406 ±0.153	0.495 ±0.171	0.360 ±0.136
Longer Arm	$\geq$ 1cm Difference	63%	58.63% ±5.79%	52.35% ±6.83%	54.90% ±5.12%
	$\geq$ 3cm Difference	100%	77.78% ±13.46%	62.22% ±15.09%	53.33% ±15.64%
Handedness	Categorical	97%	85%	50%	15%
Geolocation	Within 400km	50%	0%	0%	0%
	Within 500km	90%	6.66%	0%	0%
Reaction Time	Categorical	87.50%	79.20%	62.50%	54.20%
HMD Refresh Rate	Within 3 Hz	100%	0%	0%	0%
Tracking Refresh Rate	Within 2.5 Hz	100%	0%	0%	0%
VR Device	Categorical	100%	10%	0%	0%

Table 3B: Inferred Attributes

Attribute	Metric	No Privacy	Low Privacy	Medium Privacy	High Privacy
Voice	Gender	97%	72.5% ±15%	65% ±15%	61.25% ±13.75%
	Ethnicity	63%	52.5% ±7.5%	40% ±5%	32.5% ±0.5%
Gender	Categorical	100%	76.5% ±1.29%	70.47% ±1.85%	57.19% ±2.20%
Age	Within 1yr	100%	41.75% ±1.65%	36.09% ±1.87%	24.28% ±1.87%
Ethnicity	Categorical	100%	51.25% ±2.70%	40.75% ±2.36%	31.37% ±2.40%
Income	Within $10k	100%	26.15% ±1.41%	28.00% ±1.87%	26.06% ±2.11%
Identity	Identity	100%	5.44% ±0.68%	4.59% ±0.76%	4.0% ±0.67%

TABLE 3: Main Results (accuracy and R^2 values with 99% confidence intervals)

THANKS!

MetaData
https://arxiv.org/abs/2207.13176

MetaGuard
https://github.com/MetaGuard
https://arxiv.org/abs/2208.05604