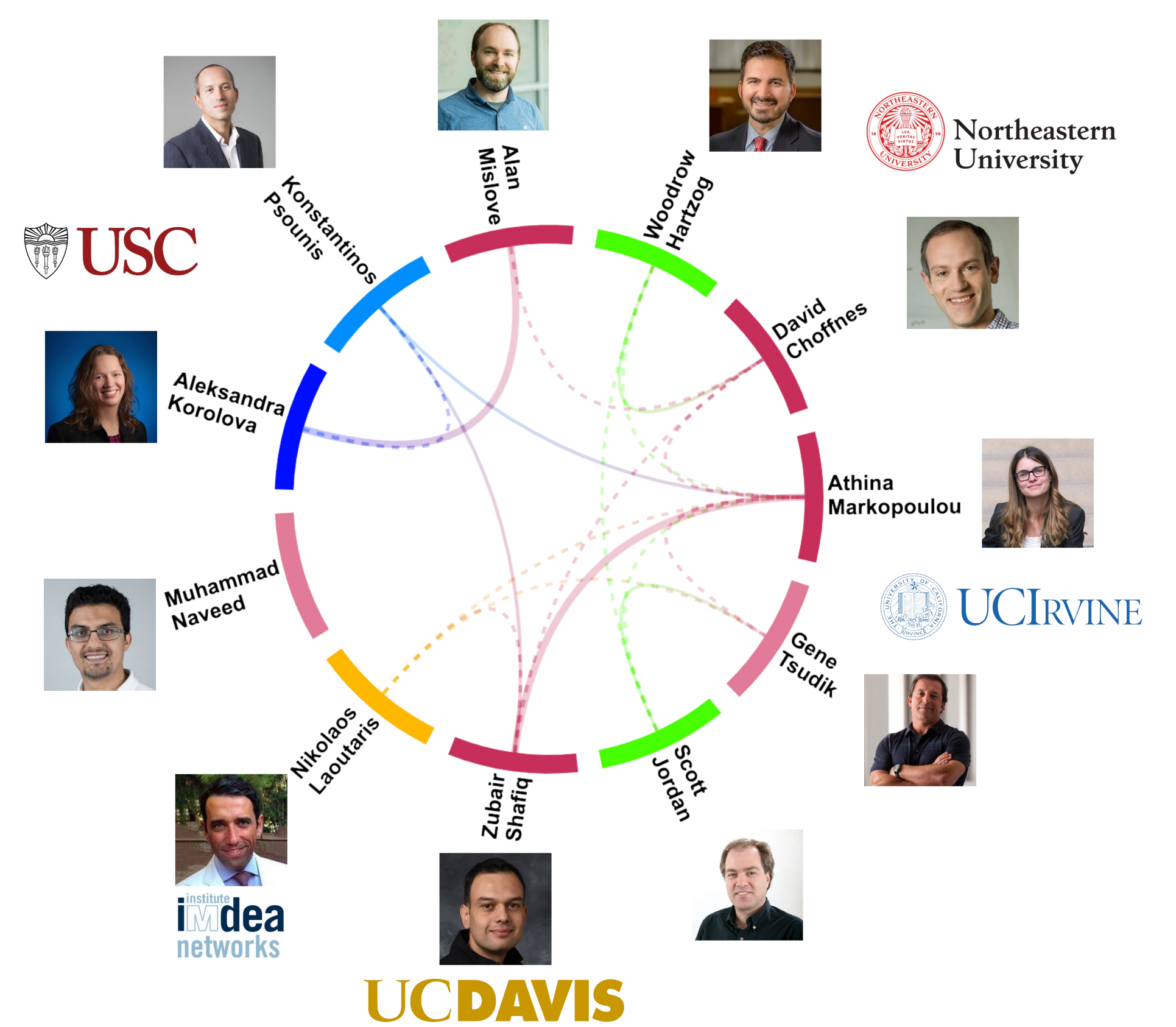
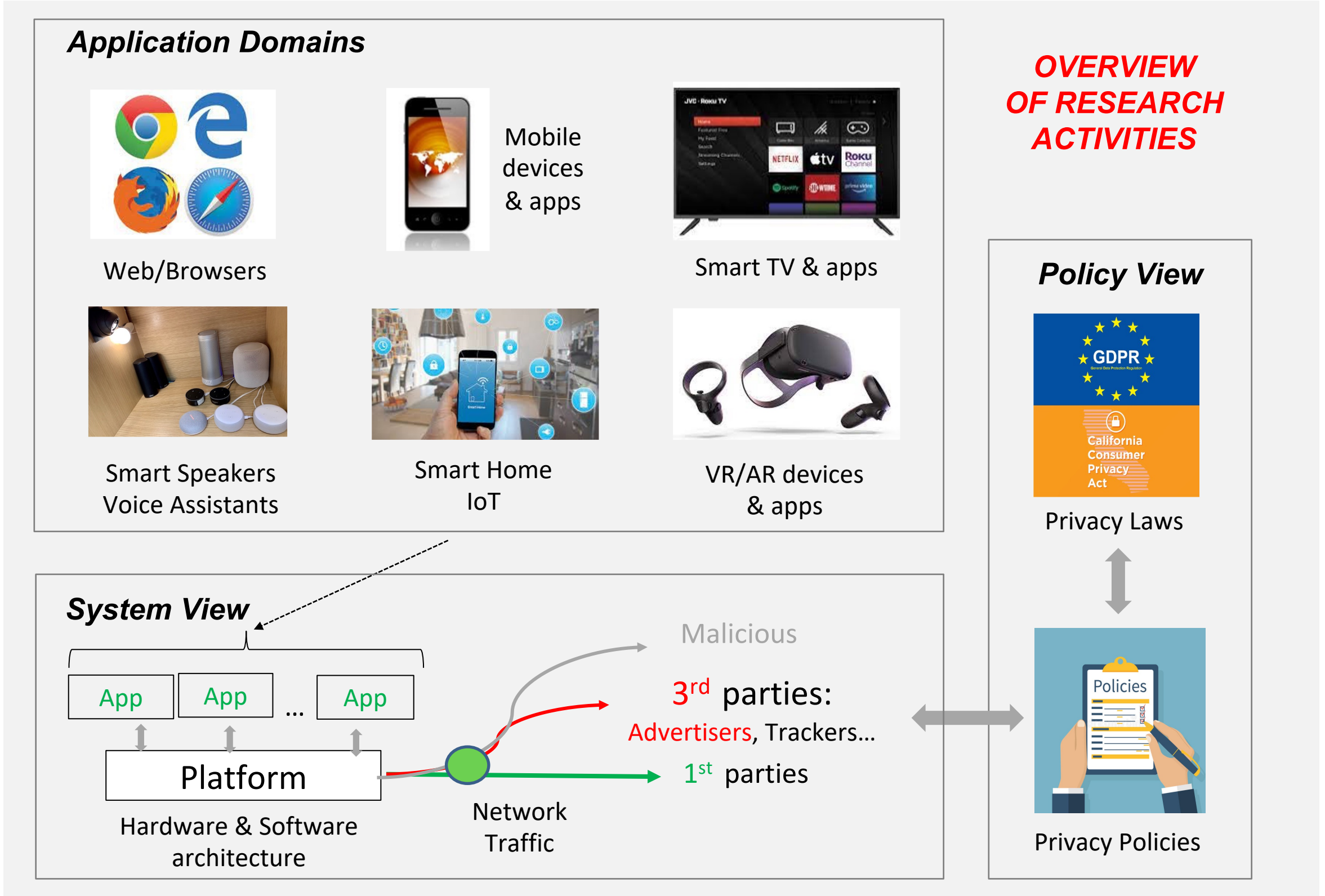


Protecting Personal Data Flow on the Internet



SaTC Frontiers: Collaborative: 1956393¹, 1955227², 2103439³, 1956435⁴
 Institutions: UC Irvine¹, Northeastern Univ.², UC Davis³, USC⁴
 Lead PIs: A. Markopoulou¹, D. Choffnes², Z. Shafiq³, K. Psounis⁴
<https://properdata.eng.uci.edu/>, contact: properdata@uci.edu



Highlight: HARPO: Learning to Subvert Online Behavioral Advertising.

J. Zhang, K. Psounis, M. Haroon, Z. Shafiq, in NDSS 2022

Challenges

- Privacy-invasive tracking techniques are used for user profiling & ad targeting.
- Defense approaches: privacy-by-design, defensive (blocking) or offensive.

Solution

- Obfuscate user's browsing history.
- Principled RL-based obfuscation approach.
- Developed surrogate ML models to train RL agent, with limited or no black-box access to real-world tracking models.

Impact

- Demonstrated HARPO's performance (2x privacy less overhead vs. baselines; stealth, personalization) in real-world experiments.
- Browser extension released to public.

Approaches	Privacy Metrics			
	L_1	L_2	L_3	L_4
Control	0.00%	0.00	0.00%	1.00
AdNauseam	12.85%	1.53	2.70%	1.21
TrackThis	32.67%	2.81	-1.50%	0.89
Rand-intent	33.10%	3.18	8.40%	1.69
Bias-intent	31.27%	Up to 3x	10.30%	Up to 16x 2.07
Harpo	43.24%	5.22	43.30%	6.28

Highlight: A Comparative Study of Dark Patterns Across Web Modalities

J. Gunawan, A. Pradeep, D. Choffnes, W. Hartzog, C. Wilson, in CSCW 2021.

Challenges

- Dark patterns can be deployed on any interface type to manipulate users.
- Little is known about how these patterns impact users on different interfaces.

Approach

- Manual interaction analysis and annotation.
- Comparative methodology identifies cross-modality inconsistencies within the same web service.

Scientific Impact

- Revealed cross-modality problems or blind spots, that may be overlooked by designers in the interface development process.
- Improved understanding of dark patterns, particularly in security/privacy contexts, like when first joining a service, trying to configure settings, or leaving a service. Our findings highlight which interaction flows might have more dark pattern prevalence.

Broader Impact

- Grad student (J. Gunawan) presented in FTC Workshop on "Bringing Dark Patterns to Light" (Oct '21).
- Users of web technologies do not always have equivalent access to all modalities of a service, often divided by socioeconomic lines. Our findings highlight inequalities built into designs.
- Methodologies can be used in future research, and to improve interface design and internal audits.
- Dataset and analysis code were made publicly available.
- Provide advice in response to inquiries from web services included in the study.

Highlight: Privacy-from-Birth: Protecting Sensed Data from Malicious Sensors with VERSA

I. D. O. Nunes, S. Hwang, S. Jakkamsetti, G. Tsudik, in IEEE S&P 2022

Challenges

- IoT S&P must start from the "birth" of data.
- Can we prevent malware from reading from GPIO or hijacking sensed data, before it is encrypted and sent to controller?

Solution & Scientific Impact

- Verified Remote Sensing Authorization (VERSA) is the first architecture to guarantee privacy-from-birth.
- Architecture Components: (1) VERSA Verified Hardware (2) VERSA software implemented using HACL*, a formally verified crypto library.

Highlight: OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR

R. Trimananda, H. Le, H. Cui, J. T. Ho, A. Shuba, A. Markopoulou, in USENIX Security 2022

Challenges

Audit AR/VR apps w.r.t.

- Their tracking practices.
- Consistency with their privacy policies.

Approach

- On-device network traffic monitoring.
- Apply NLP to Privacy Policy analysis; customize for VR.

Scientific Impact

- First study of VR Advertising & Tracking Ecosystem: early stage, mostly first parties.
- Tools and Datasets made available.

Broader Impact

- Disclosure to Meta and VR app developers included in the study.
- Discussions with FTC on VR privacy.

Highlight on Broadening Participation in Computing

Research Exploration Workshop on Privacy and IoT, May 2021

- Participants: 60 URM undergrad students, from our institutions and community colleges.
- Organizers: ProperData Faculty & Grad Students, Office of Access and Inclusion, Google ExploreCSR.
- Activities: intro to privacy research, hands-on training in raspberry pi, talks, panels, career development, intro to grad school.
- <https://sites.uci.edu/explorecsrworkshop/>

Highlights on Broader Societal Impact

Auditing Algorithmic Bias

Work on Auditing Political Ad Delivery Algorithms, by Co-PIs Mislove & Korolova

- Presentations to: FTC, Federal Reserve Board of Governors, US Committee on Financial services, Office of Technology Research and Investigation Seminar.
- Testimony to Investigations & Oversight Sub. of the U.S. House Committee on Space, Science, and Technology.

Organizing events: open workshop on Contact Tracing (Oct. 2020); closed workshop (jointly with SPLICE) on IoT Privacy Policy (April 2022).

Interactions with FTC: Several conversations with FTC on smartTV Privacy, VR privacy, dark patterns.

NU grad student Johanna Gunawan presented in FTC Workshop on "Bringing Dark Patterns to Light", April 2021.

UCI grad student J. Varmarken presented work on SmartTV tracking at FTC's PrivacyCon 2021.