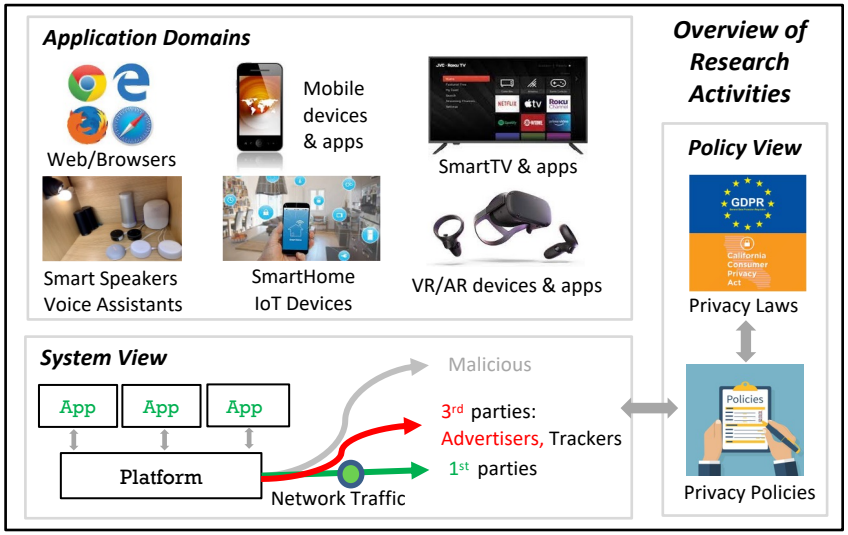
ProperData

Protecting Personal Data Flow on the Internet

SaTC Frontiers: Collaborative: *1956393* [1], *1955227* [2], *2103439* [3], *1956435* [4]
Institutions: UC Irvine [1], Northeastern Univ. [2], UC Davis [3], USC [4]
Lead PIs: A. Markopoulou [1], D. Choffnes [2], Z. Shafiq [3], K. Psounis [4]
https://properdata.eng.uci.edu/, contact: properdata@uci.edu

Overview of Research Activities



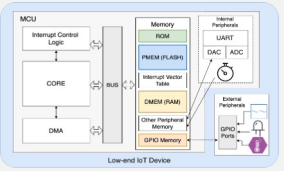
Broadening Participation in Computing

- **Research Exploration Workshops on Privacy & IoT**, May 2021
- Participants: 60 URM undergrad students, from our institutions and community colleges.
- Organized by: ProperData faculty and graduate students, Google ExploreCSR.
- Activities: hands-on experience with raspberry Pi, intro to privacy research, panels, career mentoring, networking.

"VERSA: Privacy-from-Birth: Protecting Sensed Data from Malicious Sensors"

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

Challenge	Prevent (privacy-sensitive) data leakage from even fully compromised low-end IoT devices.
Solution, Scientific Impact	**Ve**rified **R**emote **S**ensing **A**uthorization (VERSA) is the first low-end IoT architecture to guarantee privacy-from-birth.



"A Comparative Study of Dark Patterns Across Mobile and Web Modalities,"

J. Gunawan, A. Pradeep, D. Choffnes, W. Hartzog, C. Wilson, ***in CSCW'21.***

Challenges	Dark patterns (DPs) can be deployed on any interface type to manipulate user behavior. How do they impact users on different interfaces?
Solution Approach	• Manual interaction analysis and annotation. • We identify cross-modality inconsistencies within the same web service.
Scientific Impact	• We reveal cross-modality problems or blind spots overlooked by designers. • Understand DPs for security/privacy: e.g., when first joining the service, configuring settings, and leaving the service.
Broader Impact	• Grad student presented in FTC Workshop on Dark Patterns. • Response to inquiries from web services. • Datasets & code available, can enable audits.

"HARPO: Learning to Subvert Online Behavioral Advertising"

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

Challenges	Privacy-invasive tracking used for user profiling & ad targeting.
Approach	• Obfuscate user's browsing history, using a principled RL-based obfuscation approach. • Develop surrogate ML (tracking) models to train RL agent w/o access to real ones.
Scientific Impact	Demonstrated HARPO's performance (2x privacy, less overhead vs. baselines), stealth, personalization, in real-world.
Broader Impact	Browser extension released. Talk on ethics of Harpo approach.

"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	Automatically audit: • data sharing practices and • consistency of practices vs. the platform's and app's privacy policies.
Solution Approach	• On-device network traffic monitoring. • Apply NLP to Privacy Policy analysis; customize for VR.
Scientific Impact	• First large-scale study of VR Advertising & Tracking Ecosystem. • Tools and Datasets available.
Broader Impact	• Disclosure to Meta, app developers. • Discussions with FTC on VR privacy.