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 data.

Impact
- Demonstrated HARPO’s performance (2x privacy loss over RL vs. baseline; stealth, personalization) in real-world experiments.
- Browser extension released to public.

Highlight: Protecting Sensed Data from Malicious Sensors with VERSA

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

Highlight: OVRSen: Auditing Network Traffic and Privacy Policies in Oculus VR
R. Trimananda, H. Le, N. Cui, J. T. Ho, A. Shuda, A. Markopoulos, 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.

Highlight on Broading Participation in Computing
Research Exploration Workshop on Privacy and IoT, May 2021

- Participants: 60 URM undergrad students, from our institutions and community colleges.
- Organizer: 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 Science, Space, and Technology.

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

Highlight on A Comparative Study of Dark Patterns Across Web Modalities
J. Gunawan, A. Pradeep, D. Choffnes, W. Hartzog, C. Wilson, in CCSW 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.

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.

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

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 modulations 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

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

Highlight: ONVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR
R. Trimananda, H. Le, N. Cui, J. T. Ho, A. Shuda, A. Markopoulos, 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.

Highlight: Protecting Sensed Data from Malicious Sensors with VERSA

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

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 data.

Impact
- Demonstrated HARPO’s performance (2x privacy loss over RL vs. baseline; stealth, personalization) in real-world experiments.
- Browser extension released to public.