IoT Privacy: Emerging Frameworks and Strategies

4th Annual IoT Security Foundation Conference

Dr. Gilad Rosner
gilad@iotprivacyforum.org
http://www.iotprivacyforum.org
Internet of Things Privacy Forum
@IoTPrivacyForum @GiladRosner
December 4, 2018

THE WILLIAM AND FLORA
HEWLETT
FOUNDATION

Research Project:

Internet of Things Privacy Risk Mapping

Investigators:

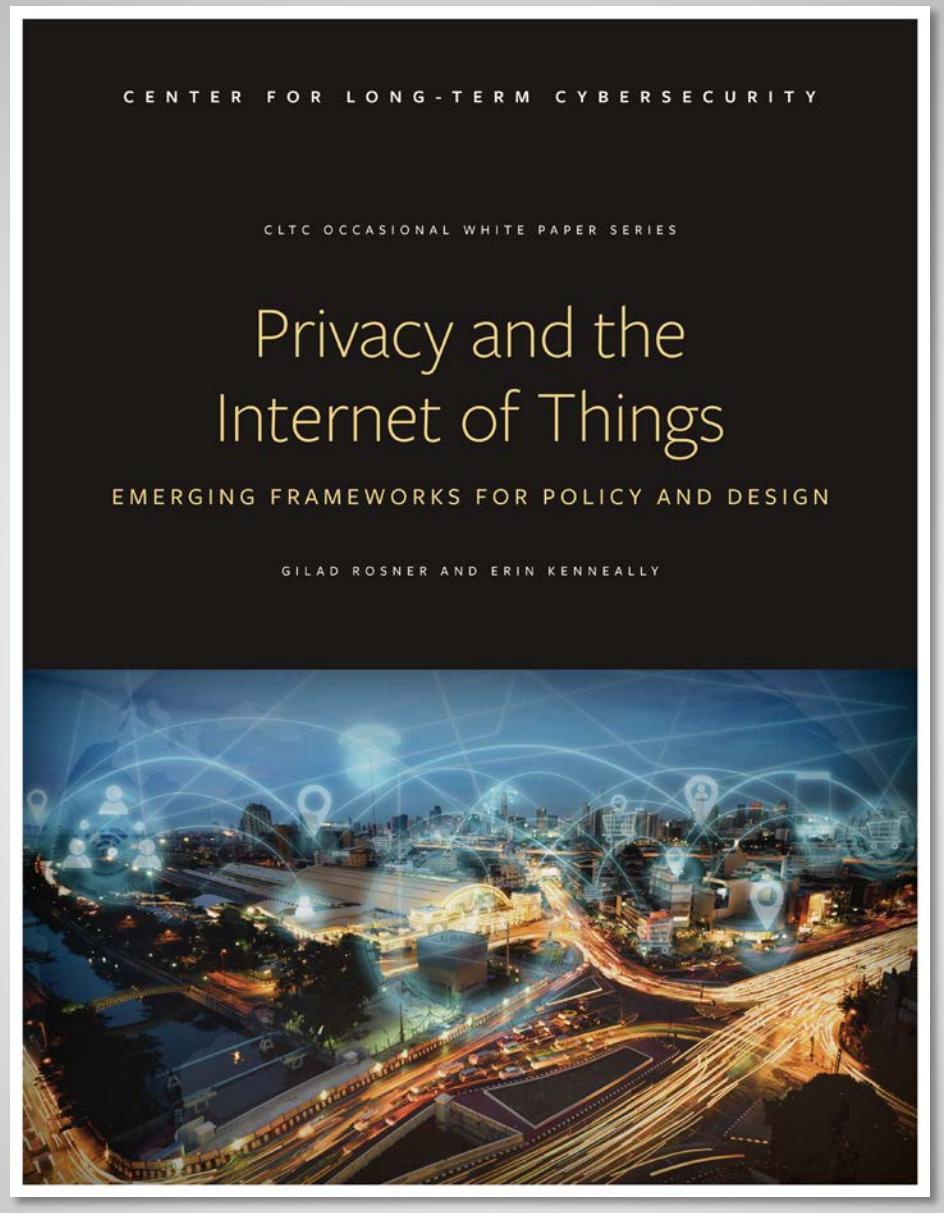
Dr. Gilad Rosner and Erin Kenneally

Research Design:

Two workshops (Bay Area, DC) and then one-on-one interviews.

40 experts, businesspeople, lawyers, engineers, advocates, government officials and scholars in total.

https://www.iotprivacyforum.org/clearlyopaque



https://cltc.berkeley.edu/2018/06/07/cltc_report_privacy_iot/

Privacy Risks of the IoT

- The IoT will expand the data collection practices of the online world to the offline world.
- The IoT portends a diminishment of private spaces.
- The IoT will make it easier to identify people in public and private spaces.
- The IoT will encroach upon emotional and bodily privacy.
- The notion of privacy *invasion* may decompose; more so as people's expectation of being monitored increases.

Privacy Risks of the IoT

- When IoT devices fade into the background, we can be duped by them, and reveal more information than we might otherwise.
- Consumer IoT devices challenge, cross and destabilize boundaries, as well as people's ability to manage them.
- As more and more products are released with IoT-like features, there will be an "erosion of choice" for consumers.

Privacy Risks of the IoT

- Market shifts towards ‘smart’ features that are intentionally unobtrusive lead to less understanding of data collection, and less ability to decline those features.
- The IoT makes getting meaningful consent more difficult.
- The IoT is in tension with the principle of Transparency.
- The IoT will have an impact on children, and therefore give parents additional privacy management duties.

Emerging Frameworks & Strategies

Notification

Governance

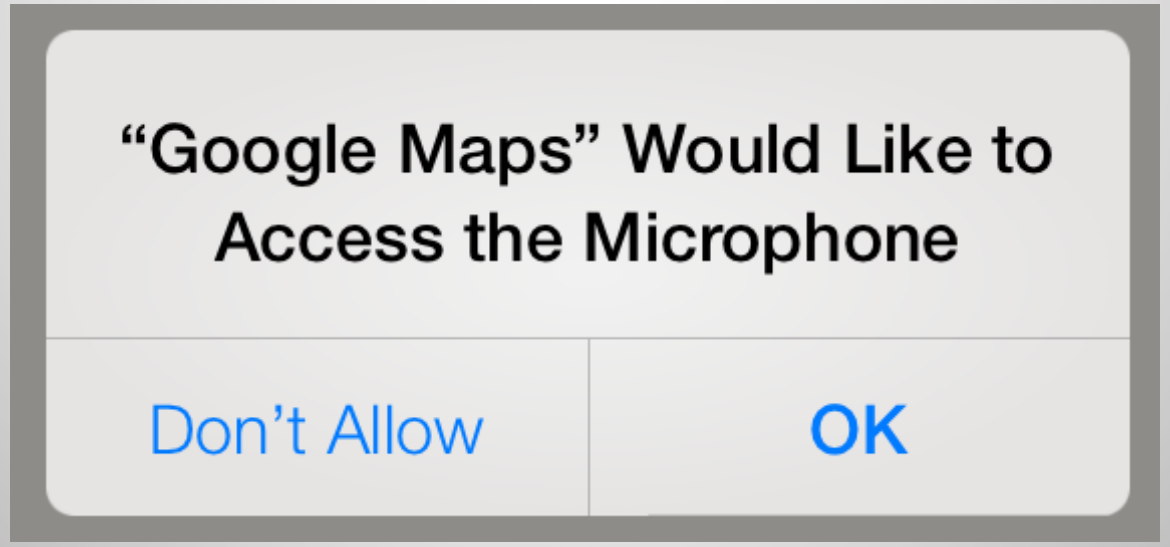
User Control & Management

Emerging Frameworks & Strategies

- Notification Strategies:
  - ***Timing*** has an impact on privacy notice effectiveness, and so we are seeing experimentation with new kinds of notices:
  - **Just-in-time, periodic, and layered notices**

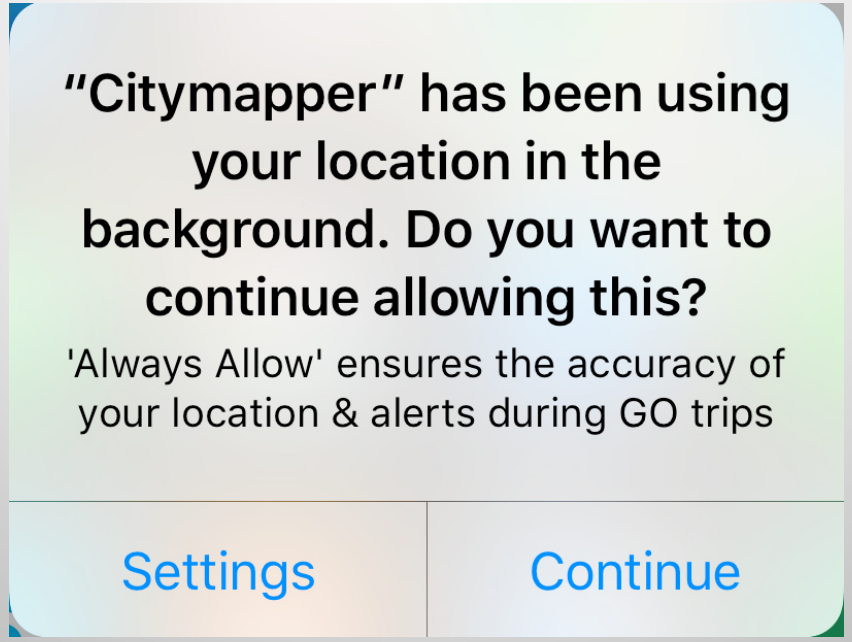
Emerging Frameworks & Strategies

- Notification Strategies:
  - *Just-in-time notices*



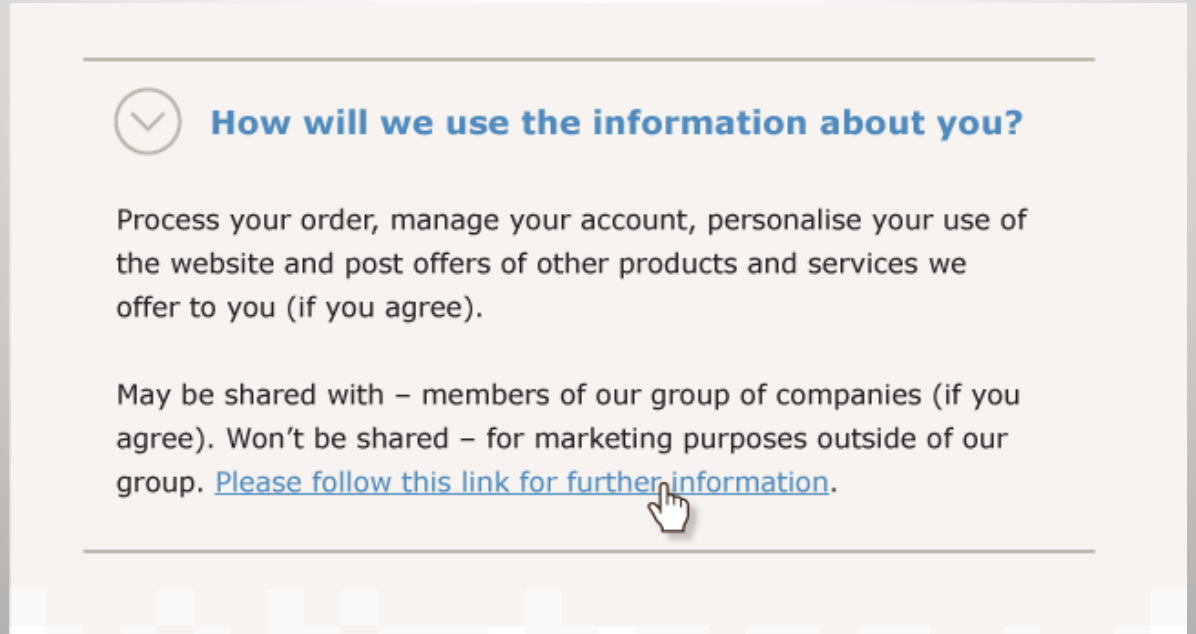
Emerging Frameworks & Strategies

- Notification Strategies:
  - *Just-in-time notices*
  - *Periodic notices*



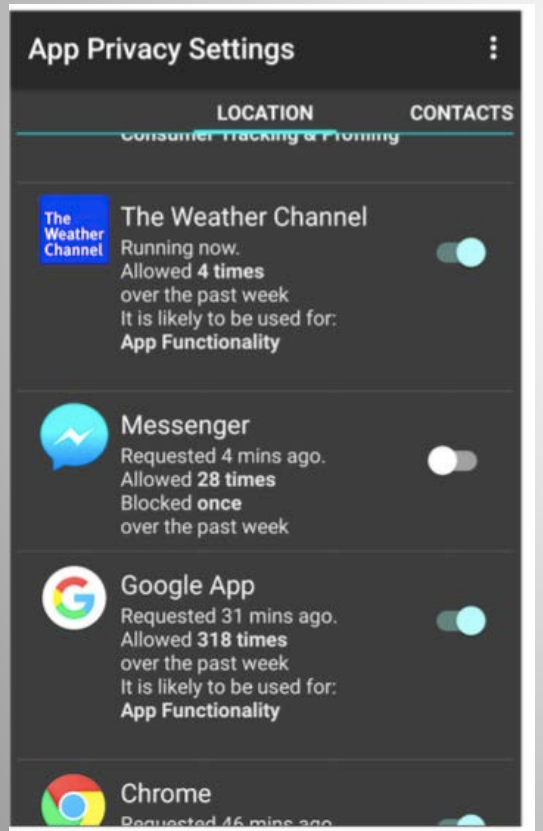
Emerging Frameworks & Strategies

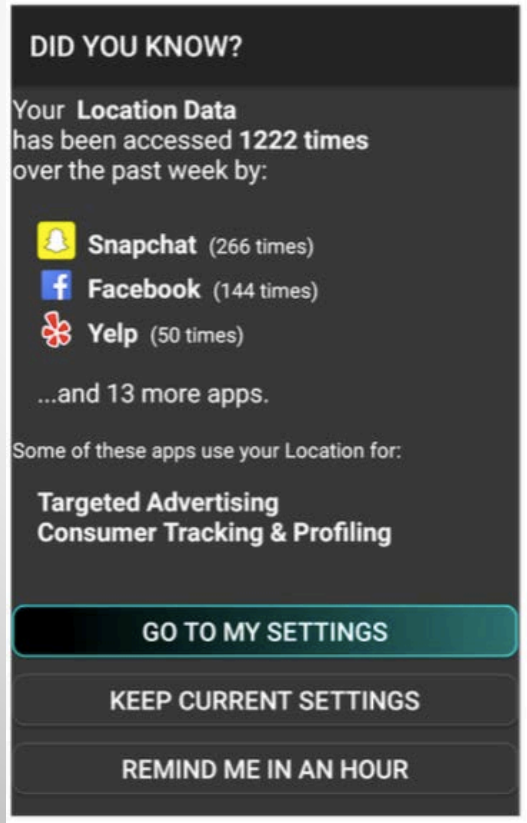
- Notification Strategies:
  - *Just-in-time notices*
  - *Periodic notices*
  - *Layered notices*

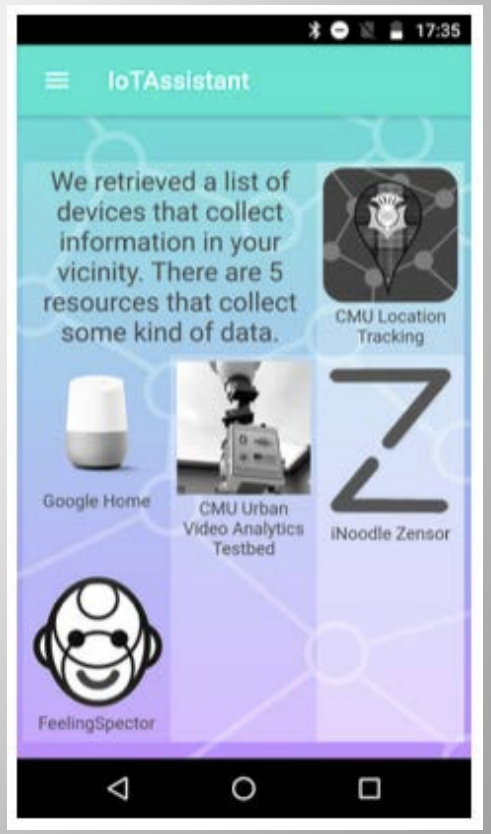


Emerging Frameworks & Strategies

- Notification Strategies:
  - *Automation (see https://www.privacyassistant.org/)*







Emerging Frameworks & Strategies

- Governance Strategies:
  - Greater use of the ‘precautionary principle’ in IoT policy
  - Creation of baseline, omnibus privacy laws for US
  - Regulations restricting IoT data from certain uses
  - Expand “personally-identifiable information” to include sensor data in the US
  - Policymaker discussions of the collapse of the ‘reasonable expectation of privacy’ standard

Emerging Frameworks & Strategies

- Governance Strategies:
  - Guidance from regulators on how companies can innovate with privacy policy language and presentation
  - Regulatory requirement to test privacy policies for user comprehension
  - More technologists embedded with policymakers
  - Exploration of Trusted IoT labels and certification schemes

Emerging Frameworks & Strategies

- User Control & Management Strategies:
  - *Pre-collection*
  - *Post-collection*
  - *Identity Management*

Emerging Frameworks & Strategies

- User Control & Management Strategies:
  - *Pre-collection*
    - Data Minimization
    - Build in Do Not Collect ‘Switches’ (e.g., mute buttons or software toggles)
    - Build in wake words, like “Hey Siri” and “OK Google”, or manual activation, for data collection, such as with a button
    - Perform Privacy Impact Assessments

Emerging Frameworks & Strategies

- User Control & Management Strategies:
  - *Post-collection*
    - Make it easy for people to delete their data
    - Make it easy for data to disappear after a set period of time – a *biodegradability* option
    - Make it easy to withdraw consent
    - IoT data should not be published on social media or indexed by search engines by default
    - Raw collected personal data should exist for the shortest time possible
    - Encrypt everything to the maximum degree possible.

Emerging Frameworks & Strategies

- User Control & Management Strategies:
  - *Identity Management (IDM)*
    - Unlinkability – the intentional separation of data events and their sources, breaking the 'links' between the different places users go online or between different devices
    - Unobservability – systems that are blind to user activity

"My car / fitbit/ voice-assistant (and therefore, the manufacturers and intermediaries) do not need to know which websites I visit, or which other devices I use."

Emerging Frameworks & Strategies

Machine identity in the IoT context:

- Device authentication
- Inventory management
- Security
- Machine trust
- Patching and updates
- Data provenance

Emerging Frameworks & Strategies

Human identity in the IoT context:

- Who is the device owner?
- Are there additional users?
- Is there an option for unidentified Guest Users? Or pseudonymous use?
- Can users be given partial control rights? (E.g., change the thermostat but not turn it off)
- Who can access data stored on a device or direct sensor feeds?
- Can device owners see other users' data?
- Can two users see one another's data or change each other's settings?
- Can data from a device be verifiably associated with a particular user?
- How do users disconnect/disassociate themselves?

Emerging Frameworks & Strategies

- User Control & Management Strategies:
  - *Identity Management (IDM)*
    - Unlinkability
    - Unobservability
    - Give people the option for pseudonymous or anonymous guest use
    - Design systems that reflect the sensitivity of being able to identify people

Emerging Frameworks & Strategies

- User Control & Management Strategies:
  - *Identity Management (IDM)*
    - Use ***selective sharing*** as a design principle
      - Meaning design for fine-grained control of data use and sharing
      - Make it easy to "Share with *this* person but not *that* person"
    - Create dashboards for users to see, understand and control data that's been collected about them
    - Design easy ways to separate different people's use of devices from one another

Challenge Question:

- You are renting out your place on AirBnB
- You have:
  - 5 Smart light bulbs by 3 different manufacturers
  - Smart thermostat
  - Smart lock
  - Smart bathroom scale
  - Connected coffee maker
  - Smart TV
- You want to give access & partial control rights
- *HOW?*

Thank you!

Dr. Gilad Rosner
gilad@iotprivacyforum.org
http://bit.ly/grosner
Internet of Things Privacy Forum
http://www.iotprivacyforum.org