Making Privacy Humanly Tractable

*Norman Sadeh, PhD, CIPT*
Professor of Computer Science
Co-Director, Privacy Engineering Program
Carnegie Mellon University

https://normsadeh.org

Usability as the Biggest Privacy Challenge

- Regulations like GDPR or CCPA/CPRA represent significant progress towards protecting people's privacy

- Yet in some ways they have also made privacy even more challenging

  - **Longer privacy policies**

  - **More privacy choices to manage**

- The above is compounded by the exploitation of **cognitive and behavioral biases** (e.g. "dark patterns")
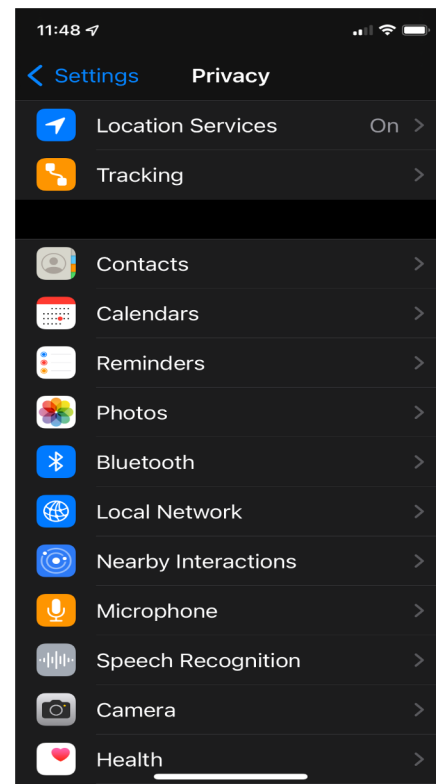
The Human Bottleneck

Lack of:

- **Expertise/Understanding**

- **Time**

- **Attention**

- **Motivation**

- **etc.**

Source: https://www.datanami.com/2016/09/13/sas-goes-back-future-cognitive-computing-viya/

Making Privacy Humanly Tractable

Our Research

- (How) can we **empower people** to derive the full benefit of new regulations?

- What are the **limits of what people can** realistically be expected to **do/understand**? How can we **help** them?

- What does this say about the **need to refine/extend** some of our **existing regulations – informing public policy**

- How can we **motivate and empower industry** to act as better stewards of people's data

- How can we help regulators enforce **compliance at scale**?

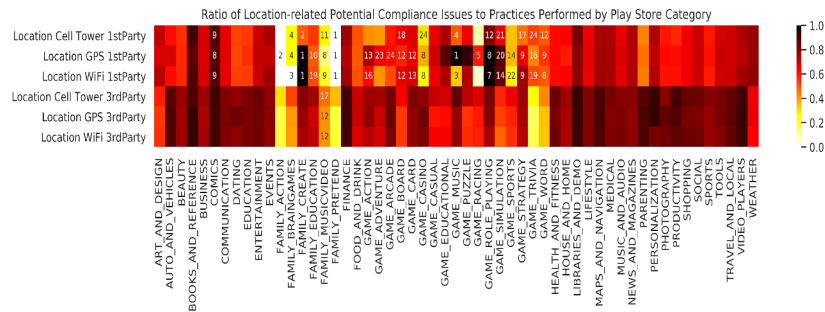- How do we reconcile AI, privacy & broader **ethical questions**?

Making Privacy Humanly Tractable

What If Computers Understood the Text of Privacy Policies?

National Science Foundation Frontier project started in 2013 – Collaboration between CMU, Fordham School of Law, Stanford Center for Internet and Society, University of Michigan, Columbia University, Penn State University, University of Cincinnati

Making Privacy Humanly Tractable

Examples of Techniques and Tools

- Collection of NLP/ML **classifiers** capable of **automatically extracting and analyzing** a variety of privacy policy disclosure statements

- Browser extension tools to automatically **identify and categorize opt-out choices** buried deep in the text of privacy policies – available in **Google chrome and Firefox stores**

- **Mobile app privacy compliance tools** comparing privacy policy disclosures and actual practices revealed by the code of mobile apps – tools prototyped with **industry and regulators** – incl. **analysis of over 1 million Android apps**

- **Tool to help developers write privacy policies** through static code analysis and wizard functionality

- **Privacy Question Answering assistant**

Ratio of Location-related Potential Compliance Issues to Practices Performed by Play Store Category

What If Computers Could Help Users Configure Privacy Settings?

PRIVACY**ASSISTANT**.ORG
the personalized privacy assistant project

Making Privacy Humanly Tractable

Examples of Models, Techniques and Tools

- **Mobile App Permission Manager, Mobile App Privacy Nudges, Privacy Preferences Modeling** – influenced development at Google and Apple (e.g. background privacy notices introduced in iOS13, expressiveness of permissions)

- **Mobile App Permission Assistant** – available in Google Play store for several years

- **Mobile App Privacy Labels** (2013CHI paper…2020 introduction in iOS14)

- Models of People's **Privacy Expectations and Notification Preferences for video analytics**

- **Privacy Infrastructure for the Internet of Things** – hosting over 100,000 discoverable IoT resource descriptions + APIs for privacy choices

- Design of **CCPA/CPRA Opt-Out Notice** adopted by California Attorney General
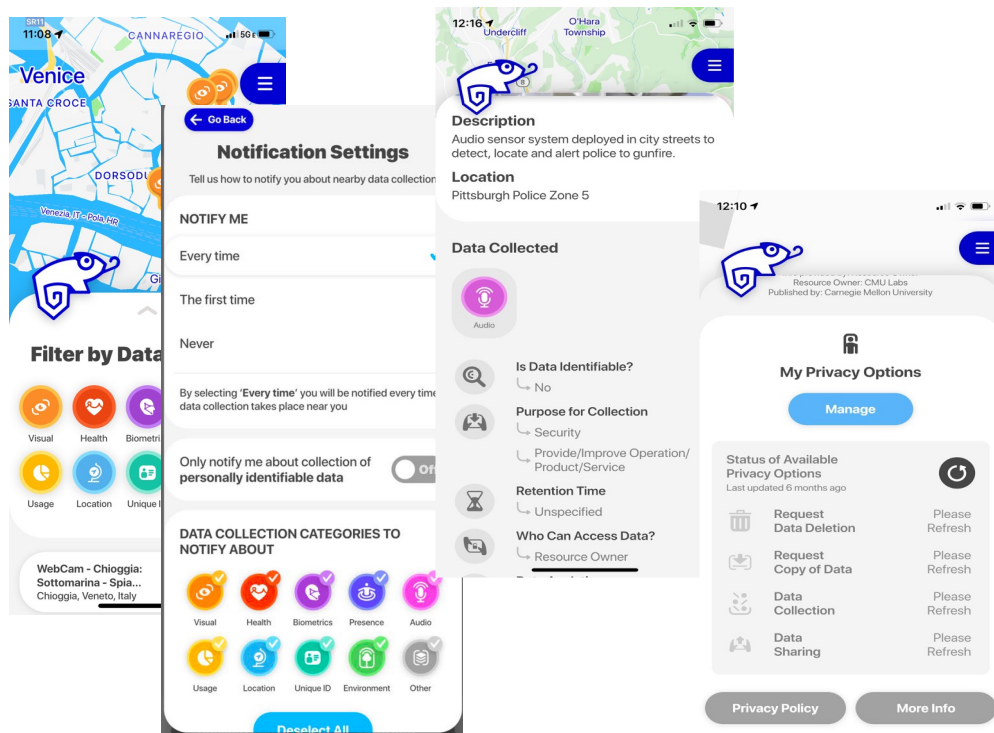
IoT Assistant app available in iOS and Google Play stores
See: https://www.iotprivacy.io

Informing Public Policy

- We are regularly called to inform public policy discussions based on our research (mainly US but also EU)

- Current focus includes emphasizing unrealistic user burden associated with privacy choices (GDPR and CCPA/CPRA) and advocating, <u>based on our research</u>, for open APIs to allow privacy assistants to help users take advantage of their privacy rights (e.g., opt-in, opt-out, deletion, etc.)

FTC Privacy Conference

Think about your **browser communicating your cookie preferences** to websites you visit, your **mobile app assistant configuring your permission preferences** for individual apps, your **IoT Assistant** selectively **notifying** you and communicating your **opt-in/opt-out preferences rather than requiring you to tediously enter the same choices over and over again** (e.g., videoanalytics, WiFi tracking, etc).


International Conference of Data Protection and Privacy Commissioners

Making Privacy Humanly Tractable

Educating the Workforce - https://privacy.cs.cmu.edu/

First of its kind privacy engineering program in the world started in 2012

– Both full-time and part-time master's programs

– Professional certificate degree – 4 cohorts per year (up to 40 students per cohort)

– **Informed by our research**

Carnegie Mellon University

Privacy Engineering Program

Masters Program   **Certificate Program**

Making Privacy Humanly Tractable
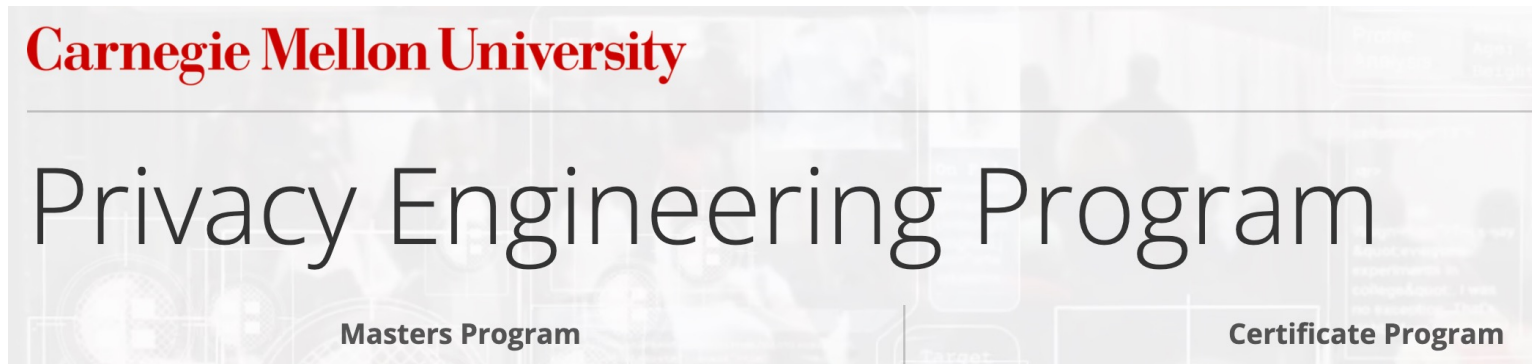
The **Usable Privacy Policy Project** and the **Personalized Privacy Assistant Project** involve collaborations with a number of individuals

This includes European collaborators – always keen to have more collaborators

More details at:

https://usableprivacy.org

https://privacyassistant.org

https://explore.usableprivacy.org

https://www.iotprivacy.io

https://privacy.cs.cmu.edu/

https://www.normsadeh.org/