Report – Privacy Policy, and People

Leads: Shomir Wilson (shomir@psu.edu), Athina Markopoulou (athina@uci.edu)
Scribes: Rahmadi Trimananda (rtrimana@uci.edu), Umar Iqbal (umar@cs.washington.edu)

Attendance: Maximum ~42 people on Day 1

Breakout Meeting Report

1. What is the topic? Why is it important to society? to a secure and trustworthy cyberspace? in other ways?

Part of the SATC community works on developing privacy-enhancing technologies. Data protection and privacy laws (e.g. CCPA in California, GPDR in Europe) and government agencies (e.g. FTC) deal with similar problems from a policy and regulation perspective. There is currently a gap between the technology and the policy sides of privacy: laws need to be informed by technical expertise to be meaningful, and technical tools need to be developed to audit and enforce compliance with the laws. In addition, there is a gap between the privacy information that consumers receive and their ability to understand and act on this information, leading to the widely recognized failure of the "notice and choice" model of online privacy. In this breakout session, we sought to bring together researchers from both the technical and policy sides of privacy to explore interfaces that bridge these gaps. We also invited participants to discuss efforts to bring understandability, controllability, and machine assistance to privacy notices and settings on the internet. This included NLP analysis of privacy policies, personalized privacy assistants, auditing of privacy controls and data practices, standards for communicating privacy information, and any related topics.

2. Is there an existing body of research and/or practice? What are some highlights or pointers to it?

During the breakout meeting, we discussed existing and ongoing work on:

- Privacy from a tech perspective: systems (platforms, apps); privacy enhancing technologies applied to them (e.g. GPC, obfuscation, Tor, etc.); and theoretical frameworks of privacy (such as differential privacy).
- Privacy laws (such as GDPR and CCPA), including studying the widely used "Notice-and-Consent" framework.
- Privacy policies: modeling, analysis and usability. How well do users understand both the systems and the privacy policies? How informed is consent?
- The interface of the aforementioned three areas, primarily for auditing and enforcement purposes: there is less (but increasing) work on this topic. Several participants of the session are actively working on that interface and shared their thoughts.

3. What are important challenges that remain? Are there new challenges that have arisen based on new models, new knowledge, new technologies, new uses, etc?

The session identified four challenges. The first were the "gaps" we anticipated prior to the session, and the remaining two are new challenges that came up during the discussion.

(1) A gap between systems and the amalgamation of privacy policies and privacy laws. This challenge includes auditing data collection and sharing practices, measuring compliance (including both effects and effectiveness), and ensuring that data is used as stated.
(2) A gap between technology users and the amalgamation of privacy policies and privacy laws. This challenge revolves around how to formulate and interpret privacy laws and privacy policies precisely, in a way that they are more actionable for developers, users and regulators. It includes automated methods to extract privacy information from texts about privacy, methods for improving or enabling informed consent, automated privacy assistants, and measurement of risk and how people perceive it.
(3) Short term vs. long term progress. Some participants regarded privacy frameworks and privacy-enhancing technologies as short-term, in contrast with privacy by design and rethinking assumptions in the above two gaps as long-term.
(4) Data collection vs. data use. This challenge involves modeling data flows, observing data use from the edge, the cumulative effect of privacy loss over time, and issues related to machine learning and privacy.

4. Are there promising directions to addressing them? What kinds of expertise and collaboration is needed (disciplines and subdisciplines)?

Here are some research directions and open problems that participants proposed:

- Co-design of law/policy and technology so that (1) laws have the right level of specificity (general enough but actionable and enforceable), (2) companies and developers have the tools to be compliant, and (3) regulators have the tools to audit.
- Establishing frameworks for communicating privacy information: Such frameworks (e.g. GPC?) must respond to the shortcomings of prior efforts, such as P3P and Do Not Track. They should also enable informed consent and choice.
- Using artificial intelligence and natural language processing to support privacy: These fields are often criticized for their negative impact on privacy, and opportunities remain to use them instead to support consumers' privacy preferences.
- Modeling data flows inclusively: Consumers affect each others' privacy, in addition to their privacy being a function of what they share or withhold from companies.
- Encouraging companies to study the user's journey to (attempt to) understand privacy: Privacy policies and complex settings make privacy a difficult topic for many consumers.
- Metrics: Questions remain on how to quantify privacy loss and evaluate privacy protections. Additionally, communicating those metrics to users will be nontrivial.
- Automating privacy decisions for consumers (to reduce the burden on them) vs. users making individual decisions.

- Potential directions for long-term changes: Considering the business models that drive tracking and advertising (surveillance capitalism); considering the role of law enforcement; proactive privacy-by-design; campaigns to make privacy “cool” and educate the public.

Overall, there exists an opportunity for SaTC to fund testbeds and infrastructure for simulating or emulating privacy technologies and policies.

Collaboration is needed between the SaTC technical community and privacy law and policy, as well as with researchers in psychology, social sciences, public health, law, and public policy.

5. Any other topic-specific questions/issues not covered by the earlier questions.

N/A