SOUPS 2019 – Half a Day Tutorial

Contextual Integrity: From Theory to Practice

Serge Egelman (ICSI), Helen Nissenbaum (Cornell Tech) and Norman Sadeh (CMU)

Background: Recognizing the endemic failures of the current privacy framework of "notice and consent," regulators and policymakers are increasingly looking to the Theory of Contextual Integrity (CI) to reason about privacy. Concurrently, there has been a stream of research to better understand and model individuals' privacy attitudes and expectations through the CI lens, as well as to inform the design of technological solutions that operationalize the theory. Yet, this shift remains relatively nascent; there are many unanswered research questions about how to best apply varying research methodologies and how to best transition research findings into practice. This tutorial will provide **a unifying view of contextual integrity, from basic concepts to emerging methodologies to current application areas**.

Objective: Our specific goal is to introduce the Theory of Contextual Integrity to the broader SOUPS community, as well as to serve as a forum for discussion of how future research might benefit from applying the theory and how the community might also contribute to refining CI principles and methodologies.

Content and Format: This tutorial will be organized around the following *four interactive sessions*, where each session will include a succession of **short presentations with opportunities for participants to add to the discussions**. Each session is expected to be one hour in length, including time for discussions. The sessions will cover the following topics:

(1) **Contextual Integrity: Motivations and Fundamental Concepts**
This will include a discussion of how CI can help lift some of the limitations associated with the current "notice and consent" privacy framework, how it can help inform public policy and legal interpretation (e.g., expectations of privacy), how it can be used to inform the design of novel technologies (e.g., what settings to expose to users, how to recommend possible settings, tradeoffs between functionality and privacy, etc.)

(2) Methodological Challenges and Approaches
Here the instructors will discuss different sets of questions required to populate CI models in support of different objectives (e.g., norms versus preferences).

This will include discussing approaches available to overcome inherent cognitive and behavioral biases associated with the collection of privacy expectations and preferences from participants in different contexts, including the impact of framing and the use of nudges to motivate users to carefully reflect about privacy decisions. This part of the tutorial will also compare the use of different methodologies to collect user data such as factorial Vignettes and Experience Sampling, including a discussion of tradeoffs and open research questions.

(3) **System Design**
This will include a discussion of how contextual integrity can be operationalized, with presentations and discussions focused on both user and developer perspectives. Important considerations include what settings to expose to users, as well as how developers can reason about the appropriateness of the data flows in the apps and services that they develop.

(4) **User Interface Issues**
This will focus on open research questions that are relevant to implementing CI in user interfaces: how to present privacy information to users, while balancing user burden and control. This will include privacy setting recommendation technologies and associated issues of autonomy and agency.

Prerequisites: This tutorial is intended for a broad audience of SOUPS participants. There are no prerequisites except for general familiarity with basic privacy concepts.

About the instructors: The instructors are well known for their seminal contributions to the development of models, methodologies and technologies aimed at defining and enhancing privacy. This tutorial will build on their many contributions in this area as well as those of others. This includes recent research results from the instructors in the context of mobile apps and the Internet of Things and work conducted as part of an ongoing collaboration under a joint NSF Secure and Trustworthy Computing (SaTC) project to extend and operationalize contextual integrity.