Contextual Integrity through the lens of computer science

Sebastian Benthall
Seda Gürses
Helen Nissenbaum

Goals

- characterize the *different ways* various efforts have *interpreted and applied CI*;
- identify *gaps in both contextual integrity and its technical projection* that this body of work reveals;
- distill insights from these applications in order to *facilitate future applications of contextual integrity in privacy research and design*.

“*Making CI more actionable for computer science and computer scientists.*”
Background: Context in computing and policy

● **Contextual Integrity:**
  ○ Privacy as appropriate information flow according to contextual norms.
  ○ Norms emerge within *spheres* of human activity, balancing societal values, contextual purposes, and participant ends.
  ○ Uptake in *computer science* since 2006.

● **Context in ubiquitous computing**
  ○ An earlier computer science research tradition, pioneered by e.g. Dey in 2001 is also concerned with privacy
  ○ “Context” refers to a *situation*: facts about the user, computer, environment. Location, identity, state…

● **Context in policy**
  ○ Excitement about privacy as respect for context motivates computer science interest in Contextual Integrity...
  ○ … but within CS, multiple traditions are blended together.
Study: research questions

- RQ1. For what kind of problems and solutions do computer scientists use CI?
  - Particular subfields of CS.
- RQ2. How have the authors dealt with the conceptual aspects of CI?
  - Social contexts, norms with specific parameters...
- RQ3. How have the authors dealt with the normative aspects of CI?
  - Norms are derived from social contexts, which are adaptations of a differentiated society.
- RQ4. Do the researchers expand on CI?
  - Where do CS researchers need to fill gaps or add to CI to make concrete systems work?
Study: research method

● Developed analytic template based on research questions.
● Searched for CS papers that claim to be using CI. (We found 20)
● Applied analytic template systematically to each paper.
● Used results to derive answers to each research question.

A systematic review of computer science literature using Contextual Integrity.
Results: RQ1 Architecture

CS researchers used CI across a few classes of technical architecture.

- **User interfaces and experiences.** These focus on an individual user’s activity and preferences, rather than social norms.
- **Infrastructure.** Catering to a large set of users and diverse applications.
  - **Social platforms.** Technology that spans *multiple social contexts*.
  - **Technical platforms.** Technology that mediates many different other technologies. *What about the operators of these platforms?*
  - **Formal models.** Frameworks to be used in design, but without implementation details.
- **Decentralization.** Decentralized architectures mirror complexity of society itself. An interesting area for future research.
Results: RQ2 What did they mean by context?

CS researchers had widely varying understandings of ‘context’; e.g. sphere vs. situation.

- **Substantiality:** *Abstract:* Hospitals in general. *Concrete:* Mount Sinai Beth Israel hospital.
- **Domain:** *Social:* A classroom with a teacher and students is a social context. *Technical:* A language education mobile app.
- **Stability:** *Representational:* The Oval Office in the White House. *Interactional:* A flash mob is an interactional context.
- **Valence:** *Normative:* A conference Code of Conduct is an account of norms inherent in a context. *Descriptive:* A list of attendees, keynote speakers, and program committee members is a description of the context.
- **Epistemology:** *Model-based:* A parameterized definition of a context, e.g., context is location, time, and activity. *Empirical:* applying traffic and topic analysis to communications in order to surface contexts.
Results: RQ3 Source of Normativity

CI is specific about where norms come from: social adaptation within differentiated spheres of society.

Few CS papers used this as a source of normativity. Instead, they used others.

- **Compliance and Policy.** Goal of the system is to comply with existing laws and policies.
- **Threats.** System is designed with a Threat Model, typical of security research.
- **User preferences and expectations.** Individual user preferences and expectations solicited.
- **Engagement.** Users interact with system to determine norms dynamically
Results: RQ4 Expanding CI

- Technological **adaptation** to changing social conditions.
- Technology operating in **multiple contexts** at once, or addressing **context clash**, where activity in different contexts interact.
- Addressing the **temporality and duration** of information, and its effect on privacy
- **User decision making** with respect to privacy and information flow controls.
Findings: RQ1 Architecture

Theoretical Gaps:
- “Modular Contextual Integrity”, faceting CI and giving guidelines for design and research at specific levels of the technical stack
- Specific guidance for infrastructure design

Calls to Action:
- Be explicit about how system is situated among other actors (operators, moderators, etc.)
- Develop formal models that connect user preferences with contextual norms
Findings: RQ2 Contexts

Theoretical Gaps:
- CI needs an account of how social spheres connect to sociotechnical situations
- What about interactional contexts?

Calls to Action:
- Specifically address how ‘context’ is used, and when technology bridges two or more meanings of the term
- Detail flows of information to third parties; what context is that?
Findings: RQ3 Normativity

Theoretical Gaps:

- Connect CI’s metaethical theory with concrete sources of normativity familiar to CS
- Spheres to threats?
- Spheres to user expectations?
- Spheres to the law?

Calls to Action:

- Measuring norms, not expectations
- Supporting user engagement around identifying norms
- Technical solutions for handling conflicts over norms
### Findings: RQ4 Expanding CI

#### Theoretical Gaps:

- Develop account of normative change and adaptation
- Address the questions around multiple interacting contexts
- Address privacy and time: duration of information, forgetting, etc.
- What about user choice?

#### Calls to Action:

- More modeling CI from information theory, information flow security
- CI and differential privacy?
Thanks!

Contact: spb413@nyu.edu