CONTEXT MATTERS: GUIDANCE FOR APPYING FAIR INFORMATION PRACTICE PRINCIPLES IN THE INTERNET OF THINGS

Paula Bruening, Sequel Technology and IP Law

Heather Patterson, Intel Labs

Symposium on Application of Contextual Integrity

September 13-14, 2018

PROBLEM TO BE SOLVED

- How to apply longstanding principles of fair information practices in complex environments, particularly the Internet of Things?
    - Interest in continued reliance on FIPPS as recognized, relied upon and trusted guidance for data protection and the basis for privacy law – a "common language for privacy."
    - Recognition that principles of fair information practices are challenged by new technologies, applications, and data environments
- Intel's "Rethink Privacy" project proposed considering how FIPPs could be used as levers to be pushed and pulled, applied in weighted fashion to address risks and circumstances.
- **Query: How to apply the FIPPs in a way that provides protections by supporting prevailing social norms in emerging, complex, data-rich tech environment.**

WHY CONTEXTUAL INTEGRITY?

- Inserts discipline, some level of predictability about how FIPPs should be applied.
- Promotes decisions that align with prevailing social norms, or that default to practices that attempt break prevailing social norms.
- Is sufficiently flexible to adapt to changed norms when they evolved organically.
- Motivates and accounts for questions about social settings, values, actors, types of information and transmission principles, as well as normative impact of change in data practice.

CONTEXTUAL INTEGRITY ANALYSIS/ FAIR INFORMATION PRACTICE PRINCIPLES GUIDANCE

- **Contextual Integrity** – helps identify potential sources of unease associated with information collection, use and disclosure.
- **Fair Information Practice Principles -** provide concrete policy guidance to help head off or mitigate those concerns.

AGING-IN-PLACE AND THE IOT MONITORING THE ELDERLY AT HOME

- Aging in place: "the ability to live in one's own home and community safely, independently, and comfortably, regardless of age, income, or ability level."
- We considered: Which flows of consumer data in the Internet of Things are appropriate for the social context of elder care in the aging-in-place environment – do these comport with, or strengthen that context's underlying aims and values?
  - How well defined is the social context?
  - What are the underlying aims and values of this social context?
  - Which data flows support which of these aims and values? Which conflict with contextual values?

Process

I. Social context: What are the social settings in which a new technological system will be deployed? Examples: home life, law enforcement, medical care, education, employment, transportation

II. Human values: What physical, emotional, social, and/or financial values are most strongly associated with the social setting(s) indicated above? Examples: freedom from scrutiny, physical safety, trust, exploration and learning, independence. What sources guide these values? Sources include laws, regulations, codes of ethics, professional oaths or codes, religion, narratives or myths, or even proverbs or popular expressions (e.g., "stranger danger," "nothing to hide," "need to know basis," etc.)

	A. Current practice	B. Novel practice
What types of information are at issue?	Prior to the installation of the proposed IoT system, what data has been collected by technologies that already exist in this social context? What information is currently knowable or inferable about the data subject(s)?	What data would be collected with the introduction of the new technology or practice? What information would be newly knowable or discoverable about the data subjects? How the form of the data, or the technologies used on it, alter what can be learned from it?
What actors are at issue?	Who are the current SUBJECTS, SENDERS, and RECIPIENTS of data?	Who will the SUBJECTS, SENDERS, and RECIPIENTS of data be with the introduction of the new technology or practice?
What transmission principles are at issue?	How is information understood to be shared with others, if at all (e.g., confidential, reciprocal, voluntary, mandatory)? What laws, rules, social norms, and practical considerations currently inform end-users' understandings of data sharing?	With the implementation of the new service, how will data be understood to be shared with others?

Normative impact of the novel practice: How will any <u>changes</u> between Column A and Column B affect the values identified as being associated with the social context in #s 1 and 2, above? Example: Improve physical safety; introduce fears of embarrassment or economic harm

Connecting Contextual Integrity and the FIPPs: How do insights about weakened and strengthened contextual values translate to the application of the FIPPs?

AGING IN PLACE CASE STUDY: COLLECTION LIMITATION PRINCIPLE

- **CI ANALYSIS:** What are prevailing expectations about what, how and by whom information about the elderly is collected in the health care setting?
- **FINDING:** What creates unease is not introduction of new types of information, but introduction of novel actors – third parties who collect and process it, and how they will use it
- **FIPPS RESPONSE:** If collection is not the issue, then important to enhance openness, use limitation, data security.

AGING IN PLACE CASE STUDY: OPENNESS PRINCIPLE

- **CI ANALYSIS:** What are the expected information flows? Who are the subjects, senders and recipients of the data? Which flows comport with social norms that underlie the aging-in-place environment and which do not?
- **FINDING:** Openness must address a range of data subjects; notice as traditionally envisioned may not serve in the IOT aging in place environment**.**
- **FIPPs RESPONSE:** Broader approach to openness that expands notice to creation of an environment characterized by transparency.

CHALLENGES

- Multiple systems in a single space are deployed and operated by many different entities present questions about how to address competing interests with respect to norms.
- Profit motivation of companies still influences; how can this be addressed?
- Systems are not closed and can involve a complex constellation of actors – whose interests do the FIPPs protect?
- How can companies be held accountable for their decisions with respect to CI analysis? Can current approaches to accountability serve in this analysis?

FUTURE WORK

- Testing this approach in practical IoT implementation.
- Development of similar case studies across variety of IoT environments
- Inquiry into how to approach CI-based decision-making when environments present conflicting norms.
- Exploration of practical design and technical challenges a contextual integrity approach to FIPPs implementation would present for developers, and how design and technology can work together to address these challenges.

Thank you

- For further discussion and information:
- Paula Bruening – paula@sequeltechlaw.com
- Heather Patterson – heather.m.patterson@intel.com
- See also related paper: Bruening, Paula and Patterson, Heather, A Context-Driven Rethink of the Fair Information Practice Principles (September 23, 2016). Available at SSRN: https://ssrn.com/abstract=2843315 or http://dx.doi.org/10.2139/ssrn.2843315

PRINCIPLES OF FAIR INFORMATION PRACTICES

- 1. Collection Limitation
- 2. Data Quality
- 3. Purpose Specification
- 4. Use Limitation
- 5. Security Safeguards
- 6. Openness
- 7. Individual Participation
- 8.Accountability