Contextual Integrity and Reasonable Expectations:

A Privacy Paradigm

Amin Rabinia, Daniel Nathan, Sepideh Ghanavati
University of Maine
Texas Tech University

Why is Privacy a Problem?

o Privacy is an inter-disciplinary challenge.

o Privacy is an unclear notion for developers and its implementation as a high-level, non-functional requirement is challenging

o Privacy laws are not usually accompanied with proper guidelines for interpretation and implementation.

o IT businesses are asked to be proactive regarding their customers' privacy right.

o Privacy concerns are usually met with add-on provisions and ad-hoc solutions.

o Improving the understanding of system developers about privacy is necessary.

Suggested Approach: Privacy Paradigms

o Formulating the need for a generic privacy paradigm
(Privacy theories + Development strategies and techniques)

o Theorizing the hallmark of privacy as:
Consistency of the informational behaviors of a system with the reasonable expectations of its users.

o Outlining a prototype of our Privacy Paradigm (PriPa), as an instance of privacy paradigms

Paradigms (Generic Privacy Paradigms)
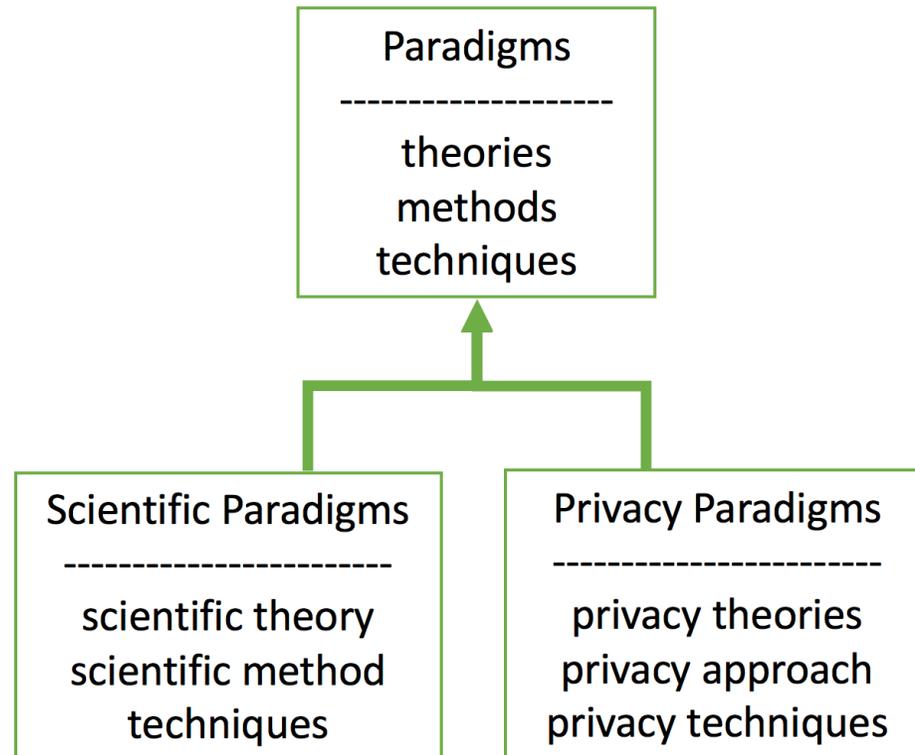
Paradigms (Examples of Privacy Paradigms)

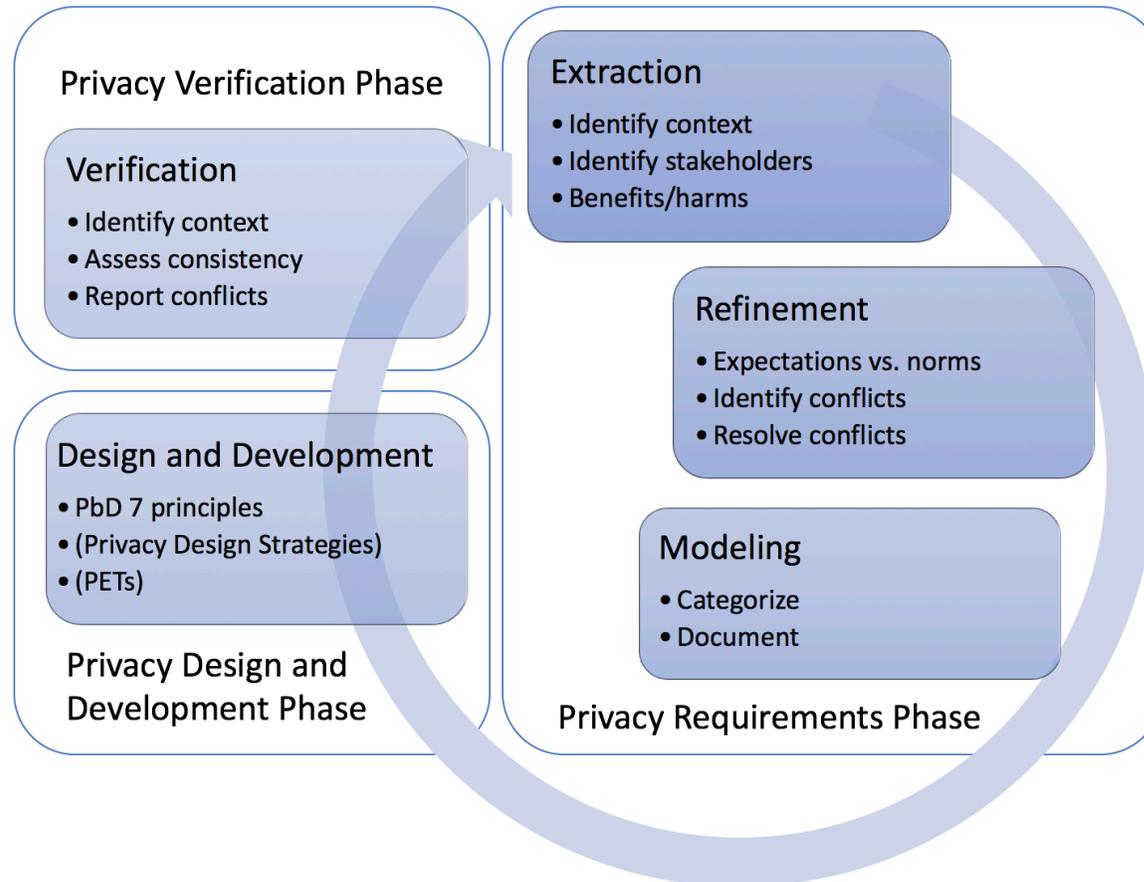| PriPa	Paradigm 2	Paradigm 3
----------------	----------------	----------------
expectations and context	control theory	N/A
PbD approach	PbD approach	Privacy Design Strategies
N/A	N/A	PETs

Privacy as Consistency of Behaviors & Expectations
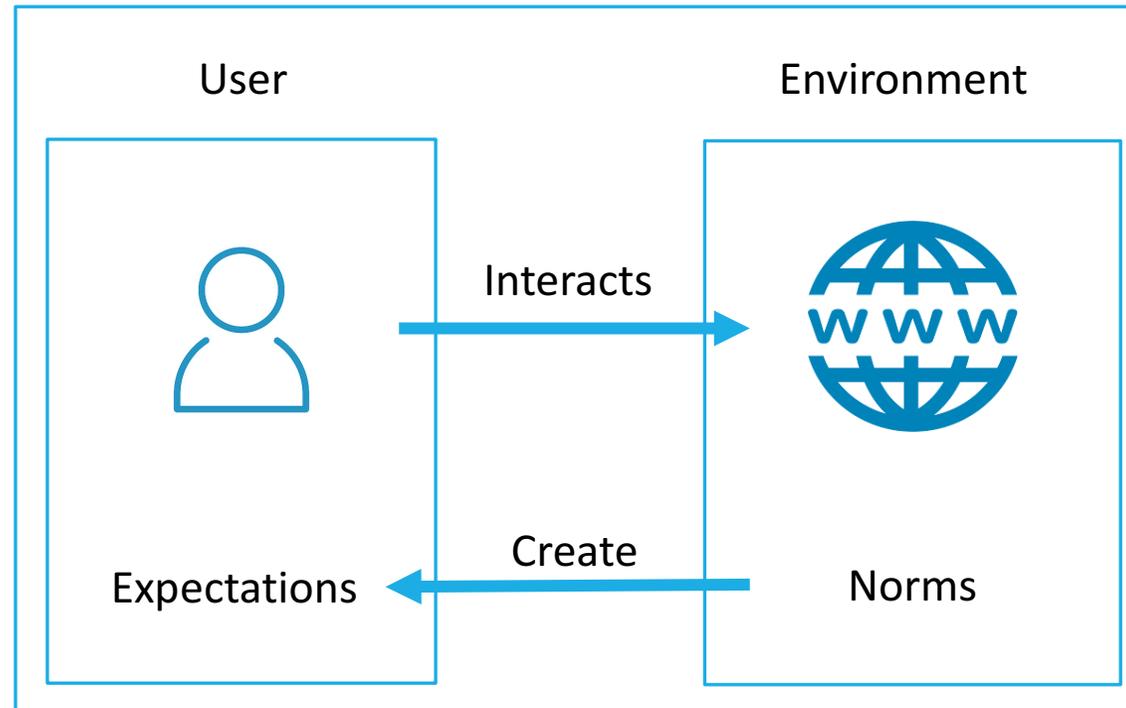
Consistency of the informational behaviors of a system with the reasonable expectations of its users.
Which expectations are reasonable?

PriPa's Privacy Engineering Life Cycle

Privacy Verification Phase

Verification
- Identify context
- Assess consistency
- Report conflicts

Extraction
- Identify context
- Identify stakeholders
- Benefits/harms

Refinement
- Expectations vs. norms
- Identify conflicts
- Resolve conflicts

Design and Development
- PbD 7 principles
- (Privacy Design Strategies)
- (PETs)

Modeling
- Categorize
- Document

Privacy Design and Development Phase

Privacy Requirements Phase

Future work

1. How does contextual integrity help/challenge capturing user's expectations?

2. What are the steps needed for implementation of CI/Expectations in the system?

3. How to test the functionality of the paradigm? Is the theoretical part really working?