Realizing Privacy through Design

Deirdre K. Mulligan UCB

Current Limitations in Privacy by Design

Two Problems

Limited Conceptual Breath

- Too few privacies
- Regulators: PbD = FIPPSbD
- HCI: privacy as control; privacy as boundary regulation

Insufficient Tools

- FIPPS and PIAs not tools for designing
- Requirements engineering

The Morass of Privacy

Sunshine walk's
http://www.flickr.com/photos/countryturtle/2178998222/sizes/l/in/photostream/

Privacy as Black Box

Tikiom's photo stream
http://www.flickr.com/photos/45786585@N00/with/790347311/

Privacy

Essentially contested concept (Gallie 1956)

concepts the proper use of which inevitably involves endless disputes about their proper uses on the part of their users and these disputes "*cannot be settled by appeal to empirical evidence linguistic usage, or the canons of logic alone*"

Positive	Negative
Importance	Slippery
Resilience	Sloppy
Generative	Fickle
Contextual	Personal

Achieving PbD

Embrace Privacy's Plurality (theoretical)

Empower designers with tools to work with multiple concepts of privacy (practical)

Leverage Power of Essentially Contested Concept

Partial Response

Multi-dimensional Privacy Analytic

- thick description of privacy
- reveal connection/divergence across theories
- enables descriptive and prescriptive work
  - understand problems
  - design solutions (technical, policy)

Privacy Dimension	Description	Interrogation	Example
Theory			
Object	That which privacy provides to those protected, i.e. *privacy provides protected agents with X*.	'What's privacy for?'	Dignity Control over Personal Info
Justification	The motivation and basis for providing privacy, i.e. *privacy is justified because of X*.	'Why should this be private?'	Individual Liberty Social Welfare
Contrast Concept	That which contrasts to privacy, i.e. *that which is private is mutually exclusive with that which is X*.	'What's not private?'	Public Open Transparent
Exemplar Problem	The archetypal threat to this concept of privacy, i.e. *privacy is violated by X*.	'What's an example?'	Personal Identity Theft Intrusive Surveillance Gossiping Neighbors

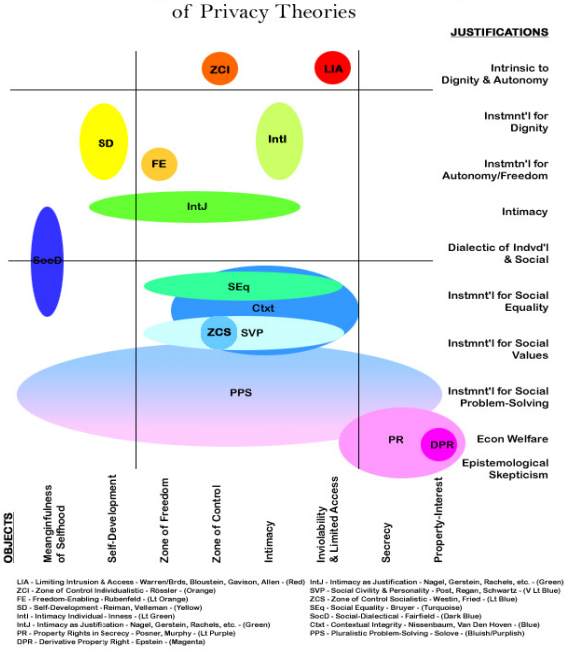
Object of Privacy

That which privacy seeks to protect, secure, achieve, facilitate, or enable

Justifications for Privacy

That which legitimates or justifies the application of a given concept of privacy

Visualizing a Multi-Dimensional Taxonomy of Privacy Theories



Privacy Dimension	Description	Interrogation	Example
Protection			
Target	That which privacy protects, i.e. *privacy protects things of type X.*	'What's privacy about? Privacy of what?'	Personal Information Body or Likeness Private space
Subject	Actor(s) or Entity(ies) protected by privacy, i.e. *privacy protects agent X.*	'Whose privacy is at stake?'	Myself, My Child Social Groups (e.g., teens) Roles (e.g., students)
Harm			
Action	The act or behavior that initiates or constitutes a privacy harm, i.e. *staring at him while he was dressing in the locker room violated his privacy.*	'What act violated privacy?'	Solove's 4 meta-harms (Collection, Processing, Dissemination, Invasion)
Offender	Actor(s) violating privacy, i.e. *privacy violated by agent X.*	'Who violated privacy?'	Government Business Entity Peeping Tom
From-Whom	Actor(s) against-whom privacy is a protection, i.e. *privacy provides protection against agent X.*	'Who is privacy protecting against?'	Everyone Government 'Friends of Friends'
Provision			
Mechanism	That which instrumentally secures privacy, i.e. *the lock on her door protected her privacy.*	'How is privacy provided?'	Legal Regulations Technical Design Social Norms
Provider	Actor(s) charged with securing privacy, i.e. *the telecommunciations provider was responsible for technically securing the privacy of her communications.*	'Who is supposed to provide privacy?'	Government Business Entity Technology
Expert	Actor(s) charged with determining privacy, i.e. *the determination that privacy should be provided should be made by X.*	'Who knows what privacy is and how privacy works?'	Policymakers Chief Privacy Officers Any Concerned Citizen
Context			
Social Context	That wherein privacy applies, i.e. *privacy applies in domain, situation, field, or site X.*	'Where is privacy found?'	Hospital or University Nation-State or Globally
Scope of Context	Extent of application of privacy, i.e. *privacy should be applied with a scope of X.*	'How widely does privacy apply?'	Universally as strict rule Casuistically as per-case

Newsfeed

Subject—the agents whom privacy is designed to protect

- 'data subject' and 'information recipient'

Object—what privacy provides

- Control over personal information
- Limited accessibility

Justification—motivation or basis

- "friendship"

Mechanism—instrumentality that secures

- technology

Goals

Understand relationships:

- theories to one another
- theories to abstract problems of today
- privacy problems on ground

Facilitate:

- productive contests over privacy
- deployment of "right" privacy in any given context

Publications and Support

Publications

Deirdre K. Mulligan and Jennifer King, *Bridging the Gap Between Privacy and Design*, University of Pennsylvania Journal of Constitutional Law, Vol. 14, No. 4, 2012.

Deirdre K. Mulligan and Colin Koopman, *Theorizing Privacy's Contestability: A Multi-Dimensional Analytic of Privacy*, (work in progress)

Ari Rabkin, Nicholas P. Doty, Deirdre K. Mulligan, *Facilitate, Don't Mandate*, IAB/W3C Internet Privacy Workshop, December 2010.

Support

Team for Research in Ubiquitous Secure Technology (TRUST), Policy Lead. NSF award Number CCF-0424422.

Institute for Information Infrastructure Protection, PI, Privacy Policies, Perceptions and Trade-offs Project (2010-11)

Berkeley Center for Law and Technology through grant from Nokia.