UC Berkeley School of Information

Privacy by Design

Deirdre K. Mulligan

Privacy by design, why now? Legal Drivers

E- Government Act of 2002 and OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

Resolution on Privacy by Design, Data Protection and Privacy Commissioners, October, 2010

Consumer Data Privacy: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, White House, February 2012

Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, Federal Trade Commission March 2012

General Data Protection Regulation 2016

Privacy by design, why now? Technical Drivers

Sensors

Big Data

Machine Learning

AI

Privacy by design, why now?Socio-political Drivers

Global data flows

Data for Good: Education, criminal justice, health

Terrorism

Snowden Revelations

Privacy by design: Early Examples

Platform for Privacy Preferences, World Wide Web Consortium 1995-2002 (machine readable notices)

Tor, Syverson, Dingledine, Mathewson 2002

Geopriv Requirements, IETF, February 2004

More recent efforts to move privacy into practice

Engineering: ENISA Privacy and Data Protection by Design-from Policy to Engineering (2015); NIST Privacy Engineering Objectives and Risk Model draft (2014); Microsoft Privacy Guidelines for Developing Software Products and Services (2007)

Technical Standards: IETF Privacy Considerations for Internet Protocols (RFC 6973) 2013; W3C ongoing since mid-90s; Oasis Privacy Management Reference Model, Privacy by Design Documentation for Software Engineers

Conceptual: Academic work: Solove, Nissenbaum, Mulligan; *Draft NIST Interagency Report (NISTIR) 8062, Privacy Risk Management for Information Systems (May 2015).*

Compliance: Global Network Initiative Principles; Privacy by Design Certification Program: Assessment Control Framework, Deloitte & Ryerson University

Education and Certification: CMU Master of Science in Information Technology—Privacy Engineering; IAPP CIP Technologist and CIP Manager

Privacy by design: CCC Project

Workshop Series proposed in 2014 by diverse team of academic researchers:

- Deirdre Mulligan (Chair), UC Berkeley
- Annie Anton, Georgia Tech
- Ken Bamberger, UC Berkeley
- Travis Breaux, Carnegie Mellon
- Nathan Good, Good Research
- Peter Swire, Georgia Tech
- Ira Rubinstein, New York University
- Helen Nissenbaum, New York University

Additional Members of Organizing Committee:

- Fred Schneider, Cornell University
- Susan Landau, WPI
- Susan Graham, UC Berkeley / CCC

Privacy by design: CCC Project

State of Research and Practice
February, 2015 UC, Berkeley

Privacy Enabling Design
May, 2015 Georgia Tech

Engineering Privacy
August, 2015 Carnegie Mellon University

Regulation as Catalyst
January, 2016 Georgetown University

http://cra.org/ccc/visioning/visioning-activities/privacy-by-design

Privacy by Design: What is it?

Unclear Objective: What does it mean to design *for* privacy?

- Privacy….
- By….
- Design…

Privacy by Design: What is it?

Unclear Objective: What does it mean to design *for* privacy?

- development method involving the adoption of certain processes—such as human or value-centered design, or PbD (Cavoukian)?
- adoption of decisional tools—such as privacy impact assessments?
- the use of privacy protective mechanisms—such as TOR and other privacy enhancing technologies?
- the achievement of specific privacy objectives—such as reduced collection of personal information?

Privacy by design: CCC Project Preview

The goal of privacy by design:

building systems that inherently protect the privacy of users.

This requires that

machines, policies and processes advance the relevant concept of privacy for the specific use case.

Privacy by design: CCC Project

Privacy by design requires organizations to:

- Identify the privacy concepts, and risks, relevant to a system;
- Design the system to respect those concepts, and to mitigate threats to them;
- Assign responsibility for meeting privacy related objectives to system components; and,
- Evaluate the efficacy of different system configurations for meeting privacy objectives.

Privacy by design: CCC Project

Privacy by design requires regulatory approaches that support internal and external environments that motivate and support it.

Addressing the privacy by design challenge requires attention to how economics, organizational arrangement, legal, and regulatory environment can support and hinder its adoption.

Privacy by design: Disconnects

Missing Bridges

- Concepts
- Methods
- Measurements
- Experts from multiple disciplines
- Incentives

State of Research and Practice

49 Participants: 23 academia; 11 industry; 6 civil society; 9 government (US St/fed)

Background Knowledge

- Privacy is an "essentially contested" concept
- Privacy laws reflect different conceptualizations of privacy
- CS research and solutions solving different privacy problems and offering new definitions
- Standards setting bodies are doing privacy work
- Interdisciplinary work is essential

State of Research and Practice : Key Insights

4

- Need for precise definitions of different privacy properties and tools to match definitions to context
- Composability challenges
- Measurement: metrics for privacy and privacy by design, risks, harms
- Uncertainty about optimal organizational arrangements
- Interdisciplinary work needs languages, tools, to aid collaboration
- Incentives often missing

Reports from the Field: Government

- Using mathematical tools to protect privacy
- Using contextual non-legal limitations to design
- Implementing technical standards for the protection of information
- Setting controls on use of data through internal standards
- Wrestling with open data and privacy commitments
- Wrestling with potential for "data for good" research to *go bad*

Reports from the Field: Industry

- Implementing cross-functional privacy teams
- Engaging in multiple types of research to better understand privacy
- Developing educational tools for end users
- Agile development process is a double-edge sword
- Creating privacy resources within organizations
- Developing access and use-based controls for data to protect privacy

Conceptual Challenges

Regulators: privacy as control or self-determination

Technical community: privacy as anonymity (Tor); privacy as control (P3P); privacy as obfuscation (Geopriv)

Public: ambiguous concept (all the above + limited access, expectations, security etc.)

Concepts: Law & Philosophy

- Right to be let alone
- Limited Access to the Self
- Secrecy
- Control over Personal Information
- Zone of Autonomous Decision Making
- Intimacy
- Personhood
- Anti-totalitarianism
- Contextual Integrity

Concepts: Computer Science Research

- Anonymity
- Confidentiality
- Requirements derived from privacy laws
- Controls
- Boundary regulation
- Differential privacy

…and Information Science etc…..

Privacy: Essentially contested concept

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"

(Gallie 1956)

Ex. Facebook Emotional Contagion Study

Privacy Concepts: Solution Spaces

Decisional Interference
--altering presentation to mess with mental state

Misrepresentation/Distortion
--misrepresenting people to their friends

Information loss
--extracting information users hadn't disclosed

Violation of expectations
--informed consent for research

Protecting "information state" of brain
--limited access to the self; personhood

Is that the *right* privacy?

What do individuals mean when they talk about privacy?

- What do they want it to protect?
- From whom are they seeking protection?
- What harms do they want it to prevent?
- What actions/designs lead people to feel violated?

And...

How do the answers to these questions relate to

- theory?
- regulatory definitions and aims?

How can they be translated into design and practice?

Solutions must be aimed at the *right* privacy.

Privacy-enabling design

49 Participants: 27 academic;18 industry (several design firms); 4 government (18F)

Privacy *WITHOUT* Design

Privacy WITH Design?

Where are the designers?

What are they doing?

Why haven't they been part of the public conversation?

What could their role be in the future?

How do we make it happen?

Privacy-enabling design: Background Knowledge

- Designers largely absent from conversation
- Regulators focused on design
- Privacy varies by context
- Organizations focused on trust, privacy as component

Privacy-enabling design: Key Insights

- Lack of adequate heuristics
- Privacy varies within context because it is relational
- Technical design and business models that conflict with users' mental models create privacy challenges
- Users trust themselves to protect their privacy
- Economic incentives are missing

Privacy-enabling design: Key Research Issues

- Mental models and privacy
- Tools to assist users—cognitive biases, over confidence
- Tools for communication (ML, automation)
- Methods best aligned with privacy work
- Context—and within it multiple audiences
- Role designers should play in privacy by design
- Team structure that work best in specific contexts
- Tension between complexity of data collection and use and usability, simplicity, comprehension
- Given that privacy is often a lower concern, building it into other processes
- Aligning technical infrastructure with users mental models

Privacy as Engineering Practice

65 Participants: 36 academia 14 industry 8 government 7 nonprofit

Background Knowledge

- Privacy must be addressed at design time
- Privacy is distinct from security and requires additional engineering approaches.
- Engineering should increase transparency, empower users, and recognize the liability of collecting personal data.

Privacy as Engineering Practice: Key Insights

- Formal specifications must balance abstraction and realism, improve transparency and ensure human involvement
- Definitions of privacy, and relation to users and designers must be clear upfront
- Quantification of p and risks can inform resource allocation
- Privacy design patterns useful to capture, share knowledge.
- Market incentives in tension with practical p standards
- De-identification techniques should be tailored to the privacy risk and legal context

Privacy as Engineering Practice: Research Questions

Concepts

What are the definitions of privacy, and how can we establish a unified lexicon of privacy-related terminology so that we can advance the state of the art?

Need for rigorous definitions of privacy and system properties that align with them that address sensors, machine learning, and AI. (differential privacy, fairness, need more…)

Privacy as Engineering Practice: Research Questions

How do we measure and quantify privacy?

- What are the dimensions of privacy risks?
- How do we measure success or failure of privacy technologies or design?
- How do we design and implement techniques for detecting and measuring flows of personal information, and other forms of privacy loss such as what is revealed through inference?
- Can we develop a more complete, quantitative understanding of the privacy risks of aggregate data?

Privacy as Engineering Practice: Research Questions

What is the extent of the relationship between privacy and security?

- How much does privacy and security intersect?
- What is the difference, if any, between a privacy tool and a security tool?
- Is there a shared lexicon of terms between the two domains?

Privacy as Engineering Practice:Research Opportunities

Systems research on tools and methods for building and verifying to different concepts of privacy, including

- Definitions and properties
- Policy languages,
- Requirements engineering from law and policy,
- Information flow analysis
- Composability
- Accountability

Regulation as Catalyst: Background Knowledge

71 Participants: 38 academia 14 industry 10 government 9nonprofit

- Multiple factors confound privacy investments in the market place
- Regulatory choices influences whether privacy is viewed as part of design
- Burgeoning profession—regulatory choices influential

Regulation as Catalyst: Key Insights

- Multiple factors confound privacy investments in the market place.
- Regulatory choices influences whether privacy is viewed as design.
- Lack of information and asymmetries undermine privacy investments.
- Environmental protection systems offer insight
- Collective privacy, surveillance issues pressing.
- Professionals of many kinds play important roles.

Regulation as Catalyst: Research Questions

- What regulatory approaches incentivize privacy during the design process rather than privacy generally?
  - What regulations would do this best? Process oriented? Performance orientation? Risk management approaches? Technology oriented?
- Viewing technology as potential solution space.
  - Transparency, accountability, auditability.
- Technology as source of problem.
  - How to address competing issues of trade secrecy, performance, black boxes?
- Privacy as societal level problem.
  - Need for better definitions, measurement, and protections.

Regulation as Catalyst: Big Questions

- Designers largely absent from conversation
- Regulators talk about design, but neither law or corporate activity seems design driven
- Economic incentives are missing

What can regulators and regulators do to empower designers?

Cross Cutting

Complex work, progress depends upon research across multiple fields

Conceptual work required

- Rigorous definitions, reduction to system properties
- Design methods important to unearthing which privacy is relevant
- Dominance of Control (FIPS) problematic—poorly suited to tomorrows challenges

Bridges required

- Tools to facilitate cross disciplinary work
- Translating between concepts, language, system requirements
- Methods for Discovery and Design
- Objectives and Properties
- People required to fill niches Designers, Engineers, Data Scientists, Tech/policy
- Education and training