Privacy by Design: Research and Action

Deirdre K. Mulligan
Privacy by Design: Legal Drivers


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

Privacy by Design: Early Examples

(machine readable notices)

Tor, Syverson, DINGLEDINE, Mathewson 2002

Geopriv Requirements, IETF, February 2004
Privacy by Design: Disconnect

Definitional issues
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.)

Orientation (what does it mean to design for privacy)
Checklist legal orientation (FIPS) (aspirational legal language and tools for lawyers)
PETS orientation (tools but how to leverage to produce privacy?)

Missing Bridges
Concepts
Languages
Methods
Markets
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


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 through Design: CCC Project

Clarification of Goals…what is being called for; how do we measure it?

- development method involving the adoption of certain processes—such as human or value-centered design, or PbD (Cavoukian)?
- adoption of 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?

Not mutually exclusive, but some are, and surely clarity is required if we expect organizations to pursue and broader range of professionals to figure out the opportunities, roles, and responsibilities.
The goal of privacy by design is:

to build systems that advance relevant concepts of privacy, by leveraging machines, policies, and processes for its protection and assurance.

This requires an intentional decision to understand privacy in the context of the system and to discharge privacy obligations where they can be most effectively met.
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 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 through 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 through 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
State of Research and Practice

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

Key Insights

• Privacy is an “essentially contested” concept
• There are many sources of privacy law, which reflects different conceptualizations of privacy
• Research in CS has produced a large variety of solutions for privacy, which operate at different levels of use and reflect different concepts of privacy
• Standards setting bodies have begun engaging more with privacy
• Engaging academics and practitioners from multiple disciplines and sectors is essential to develop a privacy research strategy that addresses the complexity of privacy in practice
Privacy-enabling design

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

Key Insights

• Designers lack adequate heuristics for designing applications
• Users want control of their privacy for different relationships
• Designs likely to engender trust should be preferred
• “Encroaching Externalities” limit the freedom to support privacy in system designs
• Users trust themselves most to protect their own privacy
• Even non-traditional interfaces should support privacy because they could become widespread
• There is a lack of economic incentive for designing with privacy
Key Insights

- Privacy must be addressed at design time.
- Formal specifications of systems must balance abstraction and realism, improve transparency and ensure humans are involved in privacy-critical decisions.
- Definitions of privacy and how they support users and designers must be clear at the outset.
- Privacy is distinct from security and requires additional engineering approaches.
- Quantifying privacy and privacy risk can inform the allocation of limited design resources.
- Privacy design patterns offer promise for sharing design knowledge and have emerged from both academia and industry.
- Market incentives have made it difficult to achieve practical privacy standards.
- De-identification techniques should be tailored to the privacy risk and legal context.
- Engineers should increase transparency, empower users, and recognize the liability of collecting personal data.
Regulation as Catalyst

71 Participants: 38 academia 14 industry 10 government 9 nonprofit

Key Insights

- Multiple factors confound privacy investments in the market place.
- Regulatory choices influences whether privacy is viewed as part of design.
- Lack of information and information asymmetries can undermine privacy investments.
- Environmental field may offer some useful tools and regulatory approaches.
- Professionals can play an important role.
Example: from concept to design
Airport Screening Technology

Privacy objectives?
Privacy concerns?
What harms?
What concepts?
What design solutions make sense?
people, process, technical
Working With Privacy
Airport Screening Technology

Privacy Objectives

DHS Privacy office...

PIAs should determine the risks and effects of collecting, maintaining, and disseminating information about individuals; and evaluate protections and alternative processes that mitigate privacy risks.

and

Privacy protections should aim to minimize intrusiveness into the lives of individuals; maximize fairness in institutional decisions made about individuals; and, provide individuals with legitimate, enforceable expectations of confidentiality.
What concepts?

**Objects of protection:**
- information about individuals
- the lives of individuals
- enforceable expectations of confidentiality

**Targets of protection:**
- any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual

**Subject of protection:**
- individual
“(images) do not present sufficient details that the image could be used for personal identification.” (target, action)

“TSO who views the image will be located remotely from the individual being screened…” (from whom + action)

“If there is an anomaly (the TSO at the checkpoint) will (see) highlight (of) the anomaly location on a generic figure…” (target, action)

“…capability of collecting and storing an image…those functions are disabled…and (cannot be reactivated).” (action)
“Images…on the screen only for as long as it takes to resolve any anomalies…” (action, time)

“… TSOs will be prohibited from bringing any device into the viewing area that has any photographic capability, including cell phone cameras.” (from-whom, action)

“the millimeter wave image rotates and both technologies place a blur over the face as the front appears in view.” (harm, target)
All these privacy protections built in yet, concerns remain.

Partial conceptual mismatch?
What were people concerned about?
Working With Privacy
Airport Screening Technology

Were people concerned about this?
Airport Screening Technology

Or was this the concern?

Privacy from the ogling man in the booth, not government data analysts.

Different concepts of privacy:
Access to the physical self
Exposure of naked body
Dignity interests

Cagle Cartoons)
Working With Privacy

Airport Screening Technology

New concept: New solution space
Airport Screening Technology
....but, new problems emerge...

“I am being held by the TSA in Orlando because of an "anomaly"”
---Shadi Petofsky
Future
Complex work Professional expertise is required across fields

Conceptual work required
• Design methods important to unearthing privacy
• Control (FIPS) insufficient, at times counterproductive

Bridges required
• Translating between concepts, language, system requirements
• Objectives and Properties
• People required to fill niche
• Education and training

Research Essential to all
• NITRD, National Privacy Research Strategy (NPRS) Ongoing
• CCC, Towards a Privacy Research Roadmap for the Computing Community May 2015

CCC Report on Privacy by Design Visioning Series Fall 2016