# Privacy by Design: More than Compliance with the Law

Peter Swire

Computing Community Consortium/CRA

Workshop On Privacy By Design

Berkeley

February 6, 2015

# The Truth Is Out There: Compliance and Security Are Not Enough

J. Trevor Hughes, CIPP/US

Omer Tene

Privacy Perspectives | Oct 3, 2014

# Overview on PbD & Compliance with Law

- Thesis: designing to comply with legal requirements is essential
  - (It's what lawyers do – build an argument)
  - It is not the only criterion for design
  - Intuitive to this audience, but helpful to understand why
- PbD includes need to design to meet binding legal requirements
  - Applies to relatively well-defined requirements
  - Applies to relatively vague requirements: "reasonable" or "unfair and deceptive"
- Beyond law -- role of ethics and other non-legal considerations
  - Being ethical is good
  - Instrumental reasons to be (and be seen as) ethical – brand considerations, political blowback, etc.
- How to communicate from the law to the engineers

# PbD – First, follow the law

- HIPAA/GLBA – Antón, Breaux, Massey et al.
  - Relatively detailed regulatory regimes
  - Even here, mapping the legal rules is detailed and hard
  - Research shows software engineers not very skilled in understanding regulatory requirements
  - So, will need institutional support for compliance, even for relatively well-specified rule sets

# Follow the Law: Office of Compliance

- The playbook (from discussion with a compliance officer)
  - Define a (long) series of limits
  - The limits prevent actions, and audit for violations of the limits
  - If need exception, go to SME/compliance officer for permission
    - Limited discretion by those subject to the compliance regime
- An example: NSA compliance with Section 215 orders from the Foreign Intelligence Surveillance Court
  - Fourth Amendment
  - FISA and other laws
  - Court orders from judge
  - Department of Justice guidelines
  - NSA policies
  - NSA software implementation of the policies
- Report each violation to FISC – limit discretion of the analyst

# “Reasonableness” and Other Vague Legal Terms

- Many legal rules not specified in detail
- For engineers, how give “reasonable access” or avoid “unfair and deceptive” trade practices? (Antón & Swire IAPP 2014)
  - Can’t code for that – deep frustration for engineers
  - But, laws can’t avoid these vague terms
    - Laws last a long time
    - For huge diversity of entities
    - For huge diversity of facts
- Therefore, law will continue to have these vague terms
  - Engineers and others, as a matter of legal compliance, will face vague terms

# Avoiding “Unfair and Deceptive” Practices – PbD as Seen by FTC

- Jessica Rich (Director, FTC Bureau of Consumer Protection) speech this week.
- On “Privacy by Design”, she says it isn’t that vague:
  - Do “reasonable data collection and retention limits, de-identification of data where feasible and sound data security and disposal practices.”
  - “You should bolster sound technical strategies for de-identifying data with a strong commitment and effective polices not to reidentify it. This means that companies should publicly commit not to seek to reidentify the data and should, through contract, require the same from those with whom they share data.”
- May sound good to lawyers -- how comforting to engineers about what is legally expected?

# Beyond Compliance – Ethics and Other Considerations

- Compliance with legal requirements is essential
    - It’s not the only criterion for design
- Similar to law and ethics chapter I teach for business students
    - Corporations must comply with law
    - That’s not enough
        - 2012 Dhaka fire for textiles factory
        - Bad lack of safe fire exits
        - Over 100 died, 200 injured
        - Buyers (legally) included WalMart and other big brands
    - Should WalMart consider such ethical and brand issues going forward?

# In Design, Why Go Beyond Legal Compliance?

- Ethics – decisions about what is right and wrong
- Instrumental Goals
  - Brand risk for a corporation
  - Political blowback for an agency or corporation
    - If we don’t build it right, they’ll cancel the program/ product
  - Other consequences of bad design

# Beyond Defining the Requirements

- Thus far:
  - Design for relatively well-specified laws
  - Design for vague laws
  - Design for ethical, brand, political considerations
- Next:
  - Communicate these requirements to those designing the systems – the privacy and other engineers

# PbD Includes Heuristics for Engineers

- RFC 6973 – Privacy Considerations for Internet Protocols
- 2014 paper Rutledge, Massey, Antón, Swire on privacy and security in Internet of Things (Internet of Devices)
- An example – consider an engineer designing IoT system
  - Develop heuristics for engineers to address security and privacy issues
  - Input/output:
    - Data flowing into a device typically security (DOS, malicious code)
    - Data flowing out of a device typically privacy concern
  - PII or not: industrial controls vs. PII surveillance
    - Mechanisms to reduce/eliminate PII
  - Magnitude and quality of risks vary with device type:
    - RFID to specialized object to general-purpose computer

# One Institutional Research Question for PbD

- How to design the Privacy by Design team?
  - Make the designer "bilingual" – engineer who is a privacy expert
  - Create a multi-functional team – when and how to bring the engineers and privacy experts together
  - There has been almost no work done on this challenging issue

# Conclusion

- A “minimalist” version of Privacy by Design:
  - PbD means to assure compliance with well-specified, mandatory legal requirements
- Beyond minimalism:
  - Many legal requirements are vague or contested
  - Ethical, brand, political and other considerations go beyond legal mandates
  - PbD principles embedded in software and system design, so help the engineers (non-privacy experts)
    - How the engineers can build privacy aspects themselves
    - How the engineers should consult organizational privacy experts (and other needed perspectives)
- In sum, many design issues beyond the minimalist version