KU LEUVEN

COSIC

In PETs we trust: Gaps between privacy enhancing technologies and information privacy law

Claudia Diaz

KU Leuven – COSIC

RWC, January 6, 2015

Claudia Diaz, Omer Tene, and Seda Gürses. ”Hero or Villain: The Data Controller in Privacy Law and Technologies.” Ohio State Law Journal 74(6), 2013.

“Constitutional privacy” (a.k.a. “fundamental rights” approach)

- Privacy protections under ECHR and the US Constitution:
  - ECHR Art. 8: “Everyone has the right to respect for their private and family life, their home and their correspondence”
  - 4th Amendment US Constitution: Right of protection against “unreasonable searches and seizures”
- High-level, abstract rights, independent of technology
- Emphasis on the protection of individuals from unlawful or disproportionate government surveillance
  - Only applicable to “public authorities”

“Surveillant Assemblage” (Haggerty & Ericson, 2000)

- Surveillance capabilities are no longer restricted to the realm of states
  - Private sector organizations have gained the ability to conduct surveillance at an unprecedented scale

- Governments increasingly assert surveillance powers in concert with private sector entities
  - PRISM, telecom metadata, introduction of backdoors, etc.
  - ACLU: “The government is not just dipping into a preexisting commercial marketplace to purchase data; companies are actually creating and reshaping their products to meet the needs of government security agencies.”

- **Result**: highly efficient and largely unaccountable surveillance infrastructure

“Informational privacy”

- FIPPs and EU Data Protection (DP)
- Technology-oriented: construct of the technological age
- Emphasis on setting minimum standards so that information can freely flow (data economy)
  - Aims at providing individuals with *control* over their data, and put *stewardship* and *transparency* obligations on data controllers
  - **Principles**: notice and choice (informed consent), subject access rights, collection limitation, purpose limitation, data security, accountability…
  - Not really addressing surveillance concerns
    - Explicit exemptions for national security and law enforcement
    - Data controllers as “information fiduciaries” (implicitly high degree of trust)

(Terminology: “Data controller” = “Service provider”)

Privacy Enhancing Technologies (PETs)

- **Our scope**: Technologies aimed to protect individuals' communications and information from surveillance
  - "allow individuals to determine what information they disclose and to whom, so that ***only*** information they ***explicitly*** share is available to ***intended*** recipients."

- Service provider as an "adversary" in the model (threat model driven)
  - Also for the protection of the service operation (Tor relays, SecureDrop, Lavabit)

- Principles:
  - *minimizing data collection*
  - eliminating the *single point of failure* inherent in a single trusted data controller
  - subjecting systems, protocols, and implementations to community-based *public scrutiny*

Privacy technologies that are out of our scope

- Technologies that rely on a model with a centralized trusted entity
  - Privacy-preserving data publishing, differential privacy
- Technologies that offer no technical enforcement of privacy guarantees:
  - P3P, DNT
- Technologies to assist users in privacy-relevant decision-making
  - Grouping of friends in FB to facilitate audience segregation, nudges
- Technologies to block intrusive information being shown to the user
  - Ad blockers

- We take into consideration the *application context* of a technology; namely, the roles and power relations of the stakeholders involved.
  - Encryption algorithms (personal vs. corporate or military use)

Trust assumptions

- Constitutional privacy:
  - Based on suspicion of power and distrust in the state
- Informational privacy:
  - Public and private entities are (de facto) "trusted": seen as stewards of individuals' rights, or "information fiduciaries"
- PETs:
  - Service provider as an "adversary" wrt privacy
    - Maliciousness but also: data breach, coerced gov access (protection of service operators), rogue employee…
  - Might still be trusted to provide a good service and for availability
    - I may trust my electricity provider to provide a reliable supply of electricity, but not trust it to only use my consumption data for billing purposes

PETs and the legal frameworks

- Objectives and trust assumptions more aligned with “constitutional privacy” (non-tech oriented) than with “informational privacy” (tech-oriented)

- PETs are trapped in a regulatory limbo between a framework that recognizes their goals but not their means, and one that recognizes their means but not their goals.

- Some distinctions:
  - PETs in fact go further than constitutional privacy in that they do not allow for “exceptions” (key escrow, backdoors)
  - Protection not only towards public institutions but also (equally) towards private sector service providers
    - Most private info collected by the private sector
    - Collusion public-private sector (illustrated by NSA programs)
    - 3rd party doctrine (aligned with view of SP as adversary)

Categorization of PETs

- What sort of legal incentives/protections would be necessary for different types of technologies?

- "PETs would have to be mandated by law to be deployed, because SPs will otherwise not implement them."

- Classification criteria:
  - Emphasis in the informational privacy legal framework on the obligations of SPs
  - Role and involvement of the service provider in the implementation and deployment of the technology

Category 1

- SP must implement the PET as part of the service
  - Enable services that take as input private user data without the SP becoming privy to such data
  - Practical viability: mandate or strongly incentivize
    - Particularly for (de-facto) mandatory/monopoly systems to avoid turning these into surveillance infrastructures

- Advanced crypto protocols
  - Private Information Retrieval (PIR)
  - Private search protocols
  - Privacy-enhanced smart metering protocols
  - Anonymous credential systems
  - …

Category 2

- SP must tolerate the PET
  - Client-side software unilaterally deployed by the user to enhance her privacy in a service offered by a SP
  - Practical viability: discourage or prevent the blocking of these PETs; eg, unfair terms of service.
    - New incentives for industry since the Snowden revelations? (FB Tor hidden server, E2E encryption for Google and Yahoo)

- End-to-End encryption
  - GPG encrypted email, OTR protocols for instant messaging, plug-ins to encrypt social media posts (e.g., Scramble!)

- Obfuscation
  - TrackMeNot

- Anonymity
  - Tor: conceptualized as a client-side tool from the perspective of the web page
  - When looking at the system itself, anonymity requires collaborative a system

Category 3

- No actual SP – except for ISPs
  - Collaborative (P2P) applications in which users also act as service providers
  - Collaborative approaches are required to protect from traffic analysis and create anonymity sets (avoiding single points of failure)
  - Practical viability: protect the ability of individuals to fed off surveillance – do not outlaw them
- Anonymous communication networks
  - Tor, Mixmaster, I2P
- Distributed (P2P) social networks

Conclusions

- Informational privacy framework undermines constitutional privacy protections by (implicitly) placing strong trust assumptions on SPs
  - DP not “tech-neutral” because of implicit assumptions about the trust model
  - This can be recalibrated by embracing the principles of PETs
  - Easy to be DP-compliant while ignoring surveillance concerns
  - Not by chance: anti-surveillance capabilities of PETs clash with powerful state and business interests.
  - Incentives dependent on the specific roles of stakeholders

- Information privacy law deals with other important privacy issues (preventing information flow not always desirable)
  - Sharing health information with your medical doctor
  - PETs only address a one aspect of the privacy problem, but an important one