

Framing harms: Surveillance, (In)security, and impacts upon Privacy and Competition

Rohan Samarajiva

Madrid

8 October 2016



Civil Law (Continental Europe & fmr colonies) versus Common Law (UK and US & fmr colonies)

- Unlike top-down Civil-Law approach that derives remedies for concrete problems from abstract principles, the Common-Law approach is bottom up
 - A specific case is decided → similar cases are similarly decided (Stare Decisis)
→ general principle is established
 - Common Law can be seen as a discovery mechanism to identify actual harms that are emerging in multiple jurisdictions
 - Solove (2008) provides a good basis
- US definition of privacy is extraordinarily broad. Harms associated with privacy in US also include surveillance and security

Harms associated with privacy (broad definition) according to Solove

- Information collection (comprising surveillance and interrogation)
- Information processing (comprising aggregation, identification, insecurity, secondary use and exclusion)
- Information dissemination (comprising breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation and distortion)
- Invasion (intrusion and decisional interference)

Harms relevant to big data

- Information collection (comprising surveillance and interrogation)
- Information processing (comprising aggregation, identification, **insecurity**, secondary use and exclusion)
- Information dissemination (comprising breach of confidentiality, **disclosure, exposure, increased accessibility**, blackmail, appropriation and distortion)
- Invasion (intrusion and decisional interference)

Blue = harms not addressable by inform and consent

Surveillance

- Passive (by-product of another activity; “data exhaust”; “bread crumbs”) v active (surveillance is primary purpose)
 - Not binary, but a continuum

Insecurity

- “Glitches, security lapses, abuses and illicit uses of personal information all fall into this category [of] insecurity, . . . a problem caused by the way our information is handled and protected”
 - “Inform-and-consent” has no solution
 - Solutions would include
 - Standards, insurance, SLAs, etc. (ex ante)
 - Damages, regulatory punishments and mandates to prevent recurrence (ex post)

Harms related to privacy (narrow)

- Identification
- Secondary use, etc.

Group harms

- Some claim groups have “privacy rights”
 - Rights usually belong to individuals, not to groups. Only group/collective right recognized in international law is that of peoples having the right of self-determination
 - A prejudice against actions based on group attributes would nullify efforts of the state to improve the functioning of society in systematic, evidence-based ways through public-policy instruments

Examples of competition harms

- Entity has access to data from a platform
 - An entity without access to that data suffers harm when it competes against an entity that does
 - If entity with access to data is affiliated to platform, violative of competition law (where it exists)
 - If strict privacy rules prohibit giving to 3rd parties, none will get data
- When mergers and acquisitions are driven by data
 - In same industry
 - In different industries