Hero or Villain: The Data Controller in Privacy Law and Technologies

Claudia Diaz\textsuperscript{1}, Omer Tene\textsuperscript{2}, Seda Gürses\textsuperscript{1}

\textsuperscript{1} KU Leuven (Belgium)
\textsuperscript{2} College of Management Academic Studies, Rishon Le Zion (Israel)
Underlying assumptions

• “Informational privacy” legal framework
  – FIPPs, EU Data Protection Directive
  – “Controller” (private or public organization) as a TRUSTED party, a fiduciary for privacy rights
    • Data protection technologies: aimed at facilitating / supporting / enforcing DP principles: consent (e.g., privacy settings), subject access rights (Google Ad Preferences), data security (access control)

• PETs (Privacy Enhancing Technologies)
  – Enabling digital services while protecting individuals from surveillance (by the state or private parties)
    • prevent (default) disclosure of information
  – “Controller” as a potential ADVERSARY (not trusted wrt privacy)
Protection from surveillance

• By *surveillance* we refer to data collection and processing that leads to gaining “intelligence” on people (or groups of people, or organizations)

• Surveillance has become: cheap, (potentially) profitable, and embedded in the architecture
  
  – The private sector is currently in a better position than states to conduct surveillance
  
  – States increasingly rely on the private sector for surveillance (e.g., “third party doctrine”)
    • Kirk Herath: “government is the biggest user of commercial big data”
PETs

- Subfield of cryptography and computer security: adversarial thinking, minimize the need to trust in other entities

- Goal: only information explicitly shared by an individual is available to intended recipients

- Examples:
  - You share a picture with a group of friends in an OSN: only your friends can access it (and not, for example, the OSN provider)
  - You browse a website: the website does not learn who you are, and is not capable of tracking you, the ISP cannot determine which page you are reading
  - You send an email to your friend: no other entity learns the content of the message, or the fact that you sent it and your friend received it
A role for PETs in privacy legal frameworks?

• Goals of PETs aligned with those of “constitutional privacy”
  – ECHR Art. 8, US Constitution 4th Amendment
  – Protect individuals from surveillance by the state
    • Does it still make sense to distinguish between the state and private organizations?

• By ignoring surveillance threats, current “informational privacy” legal frameworks:
  – undermine “constitutional privacy” protections
  – are not technology-neutral: PETs do not fit the “trusted controller” model
    • are not promoted, not required for compliance, unclear how they fit in concepts of “Privacy by Design”
  – worse: promote a false sense of privacy?
How to bridge the gap?

• Cost of implementation + opportunity cost of not getting access to some data
  – Unlikely that the market or industry self-regulation will bring about change
  – Could legal frameworks be modified to account for / promote the adoption of PETs?

• Categorize PETs according to the role of the controller
  – Reason for this criteria: controller is the focal point for DPD / FIPPs
Categorization of PETs (1 and 2)

1. Controller must implement the technology for it to be viable
   – Enable services that take as input private user information without the controller becoming privy to such information
   – Strong legal requirements/incentives would be needed

2. PET implemented unilaterally by the user within a service (or two users who wish to communicate)
   – Controller in a position to obstruct the PET
     • Forbidden in terms of service
     • Design the system so that the PET does not work or becomes unusable
   – Legal protection needed: limit the ability of controllers to obstruct/disrupt the deployment of such PETs by their users
Categorization of PETs (3 and 4)

- PET implemented collaboratively by a group of people to collectively improve their privacy

3. Category 3 (e.g., Tor):
   - Controllers: ISPs and/or online services
   - Privacy-enhanced access to online services

4. Category 4 (e.g., P2P networks, distributed social networks):
   - Controllers: ISPs and other users
   - Users act both as consumers and as providers of services

- Legal protection needed: these PETs are not delegitimized and made illegal
  - Double discourse:
    - “Over there” good for promoting freedom, democracy, human rights
    - “Over here” only good for criminals and terrorists