Privacy issues in public service applications

Subhashis Banerjee, Subodh Sharma

in collaboration with
Prashant Agrawal, CSE IITD
Anubhutie Singh and Malavika Raghavan, Dvara Research

Coverage

- Privacy issues in public service applications
    - mostly government digitization
    - but also insurance, airlines…
- We will not cover in this course
    - The `legitimate interest' question
    - internet issues, browsers, cookies, apps…
    - Google, Facebook, other social media concerns

Some do’s and dont’s

- No recording please
- Please do not download and share the videos (IITD policy not clear as yet)
- No such restriction on slides and notes
- Feel free to interrupt and ask
- All are welcome to contribute to scribe notes
- Registered students should work out all details

Digitization in public life in India

- National identity
- National population and voter registry
- National health registry, Public credit registry, Income and other tax registries
- State resident data hubs (!)
- Electronic voting
- Unified payment interface (UPI)
- Biometric (FR) based access control and surveillance
- Electronic contact tracing: Aarogya Setu
- NATGRID and other surveillance

Not a smooth ride worldwide

- *The Identity Project, LSE Report* 2005
- *Dissent on Aadhaar* 2019, *Puttaswamy I* 2017, *Puttaswamy II* 2018
- *NHS care.data scheme closed after years of controversy*, Wired, 2016
- *Australians say No to Electronic Health Records*, IEEE Spectrum, 2018
- *India plan to merge ID with Health records raise privacy worries*, FT, 2019
- *Voter privacy is gone, get over it*. Wired, 2008
- *Are citizens compromising their privacy when registering to vote?*, GCN, 2018
- *Linking Aadhaar with social media*, The Hindu, 2019

Not a smooth ride at all

- *Equifax data breach*, epic.org, 2018
- *Sweden grapples with huge leak of confidential information*, FT, 2017
- *2.7M Medical calls, sensitive audio exposed online for 6 years*, Health IT Security, 2019
- *The RBI's proposed Public Credit Registry and its implications…*, Dvara Research, 2019
- *National Id register destroyed…*, gov.uk press release, 2011
- *Launch of incomes register dogged with data security concerns*, YLE Finland, 2018
- *Aarogya Setu and other contact tracing Apps*
- *IFF's legal notice to NCRB on revised RFP for National FR System*, 2020

Disorganised response

No data protection law as yet, but

- ``Indian citizens have no fundamental right to privacy", ``elitist concern", ``no hindi word for privacy", ``not even defined"
- ``Only those who have things to hide…"
- ``Unhackable"
- ``Data is safe"
- ``Privacy-by-design"
- ``India views privacy seriously"
- ``The biggest privacy risk is your smartphone"
- ``You lose much more to Google and Facebook"
- ``High grade encryption, not breakable in 1000 years"
- ``Data is anonymised"
- ``Industry best practices"
- ``13 foot wall"

Confusing terminology

- Privacy
- Security
- Data protection

The proportionality test defines the contour

Puttaswamy I and II

- Must be sanctioned by law
- Must be necessary in a democratic society for a legitimate state aim
- Extent of interference must be proportionate to the aim
    - Rational nexus with the objective
    - Least intrusive for the purpose
    - Must not have disproportionate impact (balancing)

> Optimality analysis requires a yardstick for privacy due diligence. Problematic otherwise.

- There must be procedural guarantees against abuse from such interference

Regulatory context

Move to accountability-led approaches in data protection law

- Identify grounds of processing, PRIOR to processing data
  - (Art 6 GDPR, Ch III & s. 11 PDP Bill) (subject to exceptions/ exemptions)
- Process data for specified purpose with safeguards
  - (Art 5(1) (b) GDPR, s. 4 PDP Bill, with data minimisation)
- Process personal data “fairly” throughout life cycle of processing
  - (Art 5(1)(a) GDPR, s. 5(a) PDP Bill)
- Larger focus on organizational data practices
  - (Ch. IV GDPR, Ch. VI PDP Bill)
- Heightened accountability of data-processing entities TO regulator and FOR regulators to monitor and supervise.
  - (Ch. VI GDPR, Ch IX PDP Bill)

Nature of informational privacy

Digital Person - Daniel J Solove

- **Orwellian dangers**: surveillance state; big brother; panopticon
- **Secrecy paradigm**: harm occurs when one's hidden world is uncovered to the public
- **Invasion paradigm**: intrusion into one's private world can cause harm; such as with linking of data points
- **Kafkaesque dangers**: insensitive, opaque, and uncontrollable bureaucracy; helplessness and vulnerability of individuals; dehumanisation; AI (bias and fairness)

Limitations of Information Privacy Laws

Follow Warren and Brandeis, 1890

Mainly concerned with

- Invasion of seclusion
- Public disclosure of private facts
- Projection in false light
- Appropriation

US Constitutional laws provide some protection; also Puttaswamy I

Limitations of privacy self-management

- Consent is broken, as evidenced by the customary ``*I Agree*"
- Consent can be overridden
- Unfamiliarity with legal rights, technology
- Inability to envisage or judge potential harms of digitisation use cases, both to self and society
- Unfamiliarity with privacy management tools

Need an **accountability based framework***; it must be obligatory on the data controller to protect citizens' rights*

Limitations of Market-based solutions

- Privacy as contract
    - personal information as property
    - limitations of consent
    - individuals cannot fine-tune
- Market self-regulation
    - difference in bargaining power
    - individuals need coordination to organise

Failure of privacy self-management

Asking for “consent” for data-sharing is often a meaningless or a false choice.

- Many **cognitive biases** operate on users making decisions about sharing their personal information (Solove, 2013; Acquisti & Grossklags, 2006).
- High degree of **information asymmetry** about how providers will use and share personal data.
- The **threat of denial of service** makes “taking consent” a false choice (Acquisti, 2004).

Computer Science

- Over 40 years of research in privacy protection. Extremely rich set of tools and techniques
- A different vocabulary
- Often more grounded
- Often sloppy, not only in implementation but also in theory
- Very poor practice?

Way forward?

- A bunch of sporadic lawsuits is not the best way to change our relationships with bureaucracies
- Understand nature of informational privacy
- Understand operational requirements of privacy protection
- Ex-ante rather than ex-post
- Integrate regulatory systems with digital applications
- Architectural solutions

Start with Puttaswamy