Towards a privacy framework for India

Vrinda Bhandari and Renuka Sane

April 1, 2017

Outline

- Finance meets big data
- Privacy and big data
- State of privacy law in India
- Proposal
- Example of poor legal framework - the Aadhaar Act

Part I

Finance meets big data

Access to finance

- The reach of formal finance is low - including in urban areas.
- Households mostly prefer real estate and gold to formal finance
- "Financial inclusion" has been an objective of policy in India since the 1970s.
- Several problems have plagued the ability of formal finance to expand its reach
  - High transactions costs, making business unviable
  - Lack of formal documentation, KYC norms
- Problems of mis-selling, and the lack of an "advisory" market

The fintech revolution

- India has a presence of around 400 companies in the fintech space, with an investment of about $420 million in 2015.
- Market is forecasted to touch USD 2.4 billion by 2020 from a current USD 1.2 billion (KPMG, 2016)
- Five main areas of growth:
  - Payments
  - Credit
  - Insurance
  - Asset management
  - Robo advisory
- Brings into focus issues of privacy and data protection.

Part II

Privacy and big data

What is the right to privacy?

- Simplest definition: "The right to be left alone" (1890)
- Privacy as a cultural concept: Germany vs India
- Privacy as relational or an account of control and autonomy
- Not an absolute right
- Perhaps, not possible or necessary to give a single definition of privacy as long we understand its meaning and value

A Taxonomy of privacy: Solove

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

Privacy Harms

Categories of harms (Calo, 2013)

- Subjective harm
  - Flowing from the *perception* of unwanted observation
  - Examples: Discomfort, embarrassment, distress
- Objective harm
  - *Coerced or unanticipated* use of information against the person
  - Examples: Loss of employment, financial disadvantage through data mining; identity theft

Privacy from whom? From the State

- Rooted in ideas of liberal democracy, coercive power of the State, and the influence wielded in our lives
  - Law enforcement and predictive policing
- Surveillance: Can be physical; communications; data-veillance (Roger Clarke)
  - SFLC Report (2014): Central government alone taps more than 1 lakh phone calls a year
- Centralised collection and storage: e.g. Aadhaar
- Financial Intelligence Unit (FIU) in the absence of a privacy/data protection law - the Jindal case

Privacy from whom? From Private actors

- Basis is contract law: users consent to the "terms of service"
- Emergence of global corporations such as Facebook, Snapchat, Twitter whose business model relies on collection and storage of customer data
- Surveillance and data mining
- Data retention/sharing arrangements and unauthorised third party access
- Increasingly blurry distinction between the State and private actors because of "big data", and social media

Can the market solve the problem?

- Market forces may not provide adequate protection against private actors
  - Privacy paradox - private actors focus on *simulating* privacy protection rather than providing the real deal
  - Information asymmetry and imperfect competition
  - Bounded rationality

The case for a privacy law

- Big data has many benefits, but there are consequences of loss of privacy
  - Loss of breathing space and the fear of being observed changes our behaviour patterns to fit better with expected social norms
  - Chilling effect on free speech inducing self censorship (both for the State and private actors - e.g. Facebook "likes" study)
  - Possibility of discrimination and profiling by the State (e.g. PredPol or predictive policing) and private actors (e.g. credit scoring models)
  - Identity theft
- Checks and balances on the coercive power of the state, especially at a time when loss of trust in society

Part III

State of privacy law

The right to privacy in India

- There is no overarching privacy law
- Few sector-specific laws such as the IT Act
- Privacy is an un-enumerated right in the Indian constitution
- Supreme Court is currently debating whether privacy is a fundamental right as part of the Aadhaar challenge
- Meanwhile, Supreme Court to rule on the WhatsApp - Facebook data sharing policy, and Delhi High Court hearing a petition on the "right to be forgotten"

Privacy and data protection in Indian finance

The IT Act and the 2011 SPDI Rules

- Covers only "body corporates"
- SPDI includes financial information "*such as bank account or credit card or debit card or other payment instrument details*" [Rule 3(ii)] [personal information vs SPDI]
  1. Does not cover transaction records, credit card spending patterns, or bill payments
  2. Also excludes email/home addresses and electronic communication records
- No time limits for retention of sensitive data, beyond what is "required for the purpose" [Section 67C r/w Rule 5(4)]
- Disclosure of SPDI to any third party only requires prior permission from "provider of information" [Rule 6(1)]
- No right of data breach notification
- Weak enforcement - no DPA, CAT dysfunctional, Grievance Officer an "invisible man"

MeitY Draft IT (Security of Prepaid Payment Instrument) Rules 2017

- e-PPIs required to develop an information security policy and privacy police [Rules 3 and 4]
- Expanded definition of "personal information" to include contact details, financial data, and *transaction history* of customer along with authentication data [Rule 7 r/w S. 72A]
- Financial data deemed to be SPDI [Rule 10]
- e-PPI issuer to adopt "security standards" to protect "personal information", although no specification of what this entails [Rule 8]
- Discretion of the Central Government to specify the security standards to be adopted by the e-PPI issuers and time limits for retention [Rules 17 and 13]
- Focus on consent, end-to-end encryption

- Designation of a Grievance Officer by an e-PPI issuer and reporting of cyber incidents, but enforcement may continue to be weak
- MeitY draft Rules speak define "personal information" and focus on its security and access. However, the IT Act and SPDI Rules are concerned only with SPDI
- Personal information such as credit profiles and credit ratings and customer database of different credit card companies are still excluded from the ambit of the SPDI Rules and the MeitY draft Rules.
- MeitY draft Rules only cover e-PPIs, and thus exclude some of the intermediaries, banks, other personal finance apps or body corporates that have access to financial transaction data, and data broking services

RBI Guidelines

- RBI regulates PPI issuers under the Payment and Settlement Systems Act, 2007
- Various RBI notifications govern PPI issuers, including the Security and Risk Mitigation Measure - Technical Audit of PPI issuers 2016; RBI's Master Circular - Policy Guidelines on Issuance and Operation of PPI in India 2016
- RBI is currently reviewing its PPI guidelines through the RBI Draft Master Directions on Issuance and Operation of PPIs in India 2017 with a focus on safety, security, and fraud prevention
- Some overlap between the RBI Guidelines and the MeitY draft, particularly on the issue of risk assessment and security, and disclosure. Is there a need for two regulators?

Privacy in the Indian Financial Code

- IFC 2015 does not mention the word privacy
- Chapter 31 is on the requirement of disclosure - differentiates between initial and continuing disclosure
- Chapter 32 deals with protection of personal information, defined slightly broadly as information that discloses the identity of the consumer or allows them to be identified
  - No mention of SPDI
  - A financial service provider mus ensure that consumers can obtain "reasonable access" to their personal information and are given "effective opportunities" to correct any errors
  - Clause 117 leaves it to the Regulator to specify requirements for collection, storage, and protection of personal information without any timelines or guiding principles

IFC

- Chapter 33 is on redress of complaints
  - Requires the regulator to "specify mechanisms" for prompt and fair redressal of complaints
  - Needs to specify whether it envisages a DPA or an Ombudsman or the use of the courts
- Interestingly, while the FSLRC Report briefly mentions data privacy, no discussion of the same in the report

Part IV

Proposals

Privacy Principles

- Need for a governing privacy framework, especially since privacy is not an absolute right
  - Problems caused due to a lack of horizontal law - differential standards of privacy for different sectors
  - Privacy principles adopted by the Committee Report of the Group of Experts on Privacy (Justice Shah Report) to underlie the proposed privacy law
- Caveats:
  - Translating the privacy principles into enforceable rules that are able to deal with the inevitable privacy-security-big data conflict
  - Ensuring that such rules can keep pace with technology

Framework for a proposed law

- Objective of the law
  - Importance given to privacy of personal data
  - Inevitable conflicts between privacy and technology; and privacy and security
- Scope and ambit of the law
  - What constitutes personal data? What constitutes "sensitive" personal data?
  - Who does the law apply to: data controllers (both body corporates and non-profits), government agencies
- Collection, retention, use, processing, sharing of data
  - Collection limitation
  - Time limit for retention of data
  - Manner and form of preserving data
  - Use limitation
  - Data protection by design/default - to overcome the problems associated with consent frameworks

Framework

- Rights of data subjects
  - Data portability: allow users to transmit their personal data across various service providers.
  - Data breach notification: know when their data has been hacked
  - Access to, and correction of, personal data: kept informed about where and how their personal data is being used.
- Supervision and redress mechanisms
  - Grievance redress mechanism
  - Focus on enforcement

Part V

Example of poor legal framework: Aadhaar

Current legal framework on Aadhaar

- The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
- Regulations
  - Aadhaar (Enrolment and Update) (First Amendment) Regulations, 2017
  - Unique Identification Authority of India (Transaction of Business at Meetings of the Authority) Regulations, 2016
  - Aadhaar (Enrolment and Update) Regulations, 2016
  - Aadhaar (Authentication) Regulations, 2016
  - Aadhaar (Data Security) Regulations, 2016
  - Aadhaar (Sharing of Information) Regulations, 2016

Gaps in the Act: Scope and ambit

- The word privacy does not even find mention in the Act
- Covers interactions between the State and its residents as a condition for receipt of a subsidy, benefit or service. Also facilitates interactions between body corporates and residents
- Scope of the Act is unclear since the working of key provisions have been left to regulations. Examples:
  - Definition of biometric information [Section 2(g)],
  - The procedure for sharing information [Section 23(2)(k)],
  - Publication of an Aadhaar number holder's information [Section 29(4)]
- Delegates essential legislative functions, including important decisions on policy, to the Executive, and lacks sufficient control over its exercise

Gaps in the Act: Collection, retention, rights of users

- Does not provide an opt-out clause in consonance with the "choice and consent principle"
- No time limit for retention
- Only permits a court hearing to be given to UIDAI, and not to Aadhaar card holders, when a judicial order is sought seeking disclosure of information
- Blanket exception on the disclosure of information made in the interest of national security pursuant to a direction by an officer not below the rank of a JS.
- User can only "request" the UIDAI to get access to her identity information. May be rejected
- Fails to prescribe data breach notification, data portability requirements

Gaps in the Act: Supervision and redress mechanisms

- No provision for exclusions - Cases such as Rajasthan where biometric information was wrongly entered or not accounted for
- Only the UIDAI or its authorised officer can file a criminal complaint under the Act (for e.g. for unauthorised disclosure or access of information), and not the aggrieved Aadhaar number holder
- No standard of satisfaction prescribed and no penalty for failure to act on the UIDAI
- No provision for an Aadhaar number holder to escalate an issue

Gaps in the Regulations: Scope and ambit

- Multiple aspects of the functioning of the Aadhaar Scheme left to be "specified by the Authority", i.e. to be specified by the UIDAI at a future undetermined date.
  - Example: *"standards" for collecting biometric and demographic information, required for enrolment*
- The phrase"to be specified by the Authority" has been used 51 times through the four substantive regulations.
- Powers delegated to the UIDAI have in a sense been 'delegated' to its future self, to be notified when the UIDAI deems it fit
- For further information see https://ajayshahblog.blogspot.in/2017/03/is-aadhaar-grounded-in-adequate-law-and.html

Gaps in the Regulations: Data protection

- No requirement of notice or consent of parents to enroll children between 5-18 years
- The transmission of core biometric information by the requesting entity over a network through encrypted PID blocks remains "to be specified" by the UIDAI itself
- Right of an Aadhaar number holder to access their authentication records subject to unspecified "conditions"
- Logs of authentication transactions have to be maintained for a total period of 7 years, without any standards for storage, archiving, or security laid down
- Time limit for storage of an Aadhaar number for "lawful purpose" not mentioned

Gaps in the Regulations: Poor grievance redress

- Actual processes of redress, including the procedure for raising a grievance, the composition of the grievance redressal/contact centre, and the timelines envisaged unspecified.
- Silent on the identity/qualifications of the final decision maker, on whether the enquiry process will be administrative or quasi-judicial in nature
- No grievance redress mechanism is specified in the case of Aadhaar (Authentication) Regulations and the Aadhaar (Data Security) Regulations
- RTI replies reveal that no record is maintained for offline grievances

Gaps in the Regulations: Weak enforcement

- Largely silent on enforcement
- Probably a result of the lack of power to enforce penalties in the Aadhaar Act itself.
- Apart from a "penalty", no other prescribed liability - in terms of a monetary fine or imprisonment - for failure to comply with the code of conduct or any of the other Regulations
- Even the application of this penalty is unclear and left to the complete discretion of the UIDAI

Thank you