Privacy and Transparency in India

Elonnai Hickok
The Centre for Internet and Society, Bangalore, India

Why this topic?

- Reasons driving a privacy legislation in India: UID, NATGRID, changing business practices, increased collection of government data that make the individual transparent.
- Response to Report of Group of Experts of Privacy committee from the media focused in part on the envisioned relationship between the RTI and privacy.
- Increase in Government punishing what is said using social media: ramifications for the transparency of social media.

Background: Privacy in India

1. Privacy has been read into Article 21 of the Constitution of India -an essential component of personal liberty.

2. Indian judiciary has defined contours of privacy in many contexts including: wiretapping, sexual identities, HIV patients, and data protection

3. India does not have a horizontal privacy legislation, but safeguards can be found in sectoral legislation

4. Information Technology Act: Reasonable Security Practices and Procedurs and Sensitive Personal Data or Information Rules 2011

5. Two leaked drafts of a privacy bill: a right to privacy, data protection, surveillance, and spam.

6. October 2012: Report of Experts on Privacy

Report of Group of Experts on Privacy

1. Recommendations for a horizontal privacy law in India that would apply to both the private and public sector

2. Reviewed principles and regimes from: US, EU, Canada, Australia, OECD, APEC

3. Nine Privacy Principles: notice, purpose limitation, consent and choice, collection limitation, access and correction, accountability, security, openness, and disclosure of information

4. Regulatory framework, exceptions, complaints

Background to Transparency in India

The Government

1. The Right to Information Act 2005
2. The National Data Sharing and Accessibiltiy Framework
3. E-governance projects
4. Lokpal Bill 2011 and Prevention of Corruption Act 1988

The Private Sector

1. Traditional forms of financial reporting
2. Reasonable Security Practices and Procedurs and Sensitive Personal Data or Information Rules 2011

The Government and the Private Sector

1. Whistleblowing / Leaks
2. Sting operations

Government Transparency: The Right to Information

1. Right to Know has been read implicitly into Article 21 of the Constitution: 1988 Supreme Court case *Reliance Petrochemicals Ltd. v Indian Express Newspapers:* People must have the right to know in order to be able to participate in the industrial life and democracy...it is a basic right under Article 21.

2. Right to Information Act was passed in 2005: .

- Right to request information related to the workings of public authorities
- Requires proactive disclosure of information relating to the workings of public departments

Tensions between privacy and transparency:

1.What information can be requested, required for proactive disclosure, and exempted from disclosure? How is the determined?

2.Who can be brought under the scope of the provisions of the RTI Act?

Examples of these tensions

What information can be requested, disclosed, and exempted?

- Supreme Court judgement in September 2012: Information Commissions to be comprised of a two member bench, one member being a member of the Judiciary.

- In fall of 2012, Prime Minister Manmohan Singh recognized that disclosures under the RTI Act could infringe upon the privacy of an individual – Right to Know should be circumscribed if disclosure infringes on privacy.

- The 2012 Report of Experts on Privacy: Right to privacy should only be a narrow exception to the right to information, any Privacy Act in India should circumscribe the RTI Act, and that RTI applicants should not be considered data controllers and should not come under the purview of a Privacy Act in India.

- Fall 2012 Activists protested against the passing of an amendment to the RTI act that would restrict the types of ‘file notings’ that individuals can request to only those of social and developmental issues.

Examples of these tensions

Who can be brought under the scope of the RTI?:

- Act lists 25 agencies exempted from the provisions of the RTI
- This includes many security agencies
- Research Analysis Wing now partially held accountable
- Publice Private Partnerships: The CIC had originally ordered that PPPs should count as public authorities, but the Law Commission objected to “private executioners” being treated as public authorities.
- The CIC had also ordered that private distribution companies in Delhi, and the National Stock Exchange be brought under the ambit of the RTI, but this decision was stopped by the Delhi High Court.
- In a statement in 2012 the Prime Minister specifically came out against extending the scope of the RTI Act to PPPs .

How does the RTI address privacy?

- **Types of information can be requested:** File notings, records, meeting transcripts.
- **Types of information must be proactively disclosed:** The particulars of its organization, function and duties, the powers and duties of its officers and employees, the procedure followed in the decision- making process etc.
- **Circumstances in which disclosure of information is exempted**: Exemptions are qualified by the condition that information which cannot be denied to the Parliament or a State Legislature cannot be denied to any person, and if public interest in disclosure outweighs the harm to protected persons.
- **One exemption that speaks specifically to privacy**: Disclosure of information which relates to personal information, when disclosure of that information would have no relationship to any public activity or interest and would cause an unwarranted invasion of privacy, unless it is determined that the larger public interest justifies the disclosure.

How does the RTI address privacy?

- 2011 case *Mr.V R Sharma v Ministry Of Labour And Employment CIC* laid down three precedents that could be used to measure if information should be considered to be ‘personal information’.
- **The information must be personal:** 'Personal information' cannot be related to institutions, organizations, or corporate entities.
- **The disclosure of information has no relationship to any public activity or interest:** Public authorities in performing their functions routinely ask for ‘personal’ information from citizens, and this is clearly a public activity.
- **The disclosure of the information would lead to an unwarranted invasion of the privacy:** The State has no right to invade the privacy of an individual except in extraordinary situations. In these circumstances, special provisions of the law must apply with safeguards.

Other provisions that speak to privacy

- If personal records of a third party are being sought to be released, the third party must be given the opportunity to oppose the disclosure.
- Prescribes how records should be maintained and catalogued by public authorities.
- If a request is rejected, the individual is provided with the reasons for rejection, the period for appeal, and the details of the appellate authority.

Open Government Data

- Tenth Five Year Plan (2002-2007) GOI commits to openeing up government data.
- February 2012: The National Data Sharing and Accessibility Policy.
- Applies to all data and information created, generated, collected and archived using public funds.
- Seeks to enable citizen access to data essential for a number of decisions.
- Databases will be integrated and a data warehouse will be setup to house current and historical data and government departments will divide data between shareable and non shareable data.

Tensions between privacy and transparency:

- Unclear how shareable and non-shareable will be determined
- Unclear how data will be disclosed, to what extent mechanisms like anonymization will be incorporated, how long it will be disclosed, how it will be deleted.

E-Governance Projects

- GOI commitments in Tenth Five Year Plan led to an increase in the number of e-governance projects in India.
- Projects are meant to increase efficiency and bring transparency into the system.
- Projects demonstrate the importance of strong privacy safeguards and information practices: errors in collection of information, errors in digitization, no harmonized standard for how transparency should be incorporated.
- **Example**: In an effort to eliminate fraudulent and duplicate ration cards, the Karnataka State Government decided to post on its website comprehensive details of (1.51 Crore) ration cardholders in the state including the ration card number, category of card, names and photographs of the head and other members of a family, address, sources of income, LPG gas connection, and number of cylinders in the town.

The Prevention of Corruption Act 1988 and the LokPal Bill 2011

- Transparency is mandated for the purposes of curbing governmental corruption and is enforced through investigative powers. In this context privacy interests need to be weighed against investigative powers.
- For example, under the Prevention of Corruption Act 1988 allows for arrests without warrants, inspection allowed if there are reasons to suspect an offence.
- In 2011 the LokPal Bill was proposed before parliament. The Bill is similar to the Prevention of Corruption Act in that it creates broad powers of investigation.
- Bill proposes safeguards such as limiting how long documents collected for investigation can be retained, allowing individuals under investigation the right of appeal, and publishing information related to cases being tried on a website for the public.

Transparency: The Private Sector

- Increased concern with changing business practices: social media companies, web hosting companies, databrokering.
- Increased punishment for comments posted on social media: 21 girl arrested for posting “People like Thackeray are born and die daily and one should not observe a bandh for that.” (Bal Thackeray was the chief of the Shiv Sena political party)
- Traditional forms of transparency requirments found under the Indian Income Tax Act 1961, the Companies Act 1956 etc. Most recently the Reasonable Security, Practices, and Procedrues and Sensitive personal data or information rules 2011

Provisions that speak to transparency:

- Privacy policies & notice at collection,
- Right to access and correct & right to withdraw consent,
- Disclosure of information only once consent is given except by request from governmental mandated agencies: verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences.

Transparency: The Private Sector and the Public Sector

- **Whistleblowing/leaks**
  - **Nira Radia**: Exposed the 2G spectrum scam through leaked records of intercepts initiated to for the purposes of investigating tax evasion
  - **Wikileaks**: Prime Minister Manmohan Singh had offered bribes to win votes from Parliament in the U.S – India nuclear deal in 2008
  - **Mysore Mallige scandal**: In 2003, a home sex video made by a couple and was leaked. As a result, the boy was beaten by the family and eventually left the country
- **Sting operations:** In 2011 the news channel TV9 broadcast a program on the gay culture in Hyderabad. Among other things, the program showed unmorphed visuals and contained telephonic conversations between the TV9 reporter and individuals speaking about their sexual preferences. Eventually the channel was fined and penalized for violating clause 5 (sex and nudity), clause 6 (privacy), and clause 9 (sting operations) of the Code of Ethics & Broadcasting Standards.

Attempts to Regulate Sting operations and Whistleblowers

- **Sting Operations:** Addressed in the Broadcasting Codes of Ethics. Should be a last resort, should not cover sex and sleaze, should be guided by the larger public interest, should not misrepresent the truth
- **Whistleblowers**: *Public Interest Disclosure and Protection to Persons Making the Disclosure Bill, 2010.* Creates mechanisms for whistleblowers to issue complaints, for complaints to be verified, for physical protection of whistleblowers.
- 2001 recommendation from the Law Commission and a 2004 order from the Supreme Court to put in place a legal mechanism for whistleblowers.
- 2004, the Central Government notified a resolution that empowered the Central Vigilance Commission (CVC) to investigate complaints from whistleblowers.

These practices serve an important function, but privacy must be incorporated into the process for making a piece of information public inorder to protect the individual disclosing the information, and the individual who information is exposed about.

Transparency of Citizen/Resident/Consumer

- **The Unique Identification Project**: One time consent, allowing information to be collected outside of scope or setting broad standards of "necessary information", unclear storage of data -creating the possibility for tracking and profiling
- **Surveillance legislation and policy**: Broadening standards for surveillance, networking, centralizing, and working towards blanket monitoring capabiltiies
- **The Collection of Statistics Act 2008:** Broad mandatory collection of any type of information needed for the creation of statistics by the government. Penalties for noncompliance.
- **Privacy Policies:** Unclear, changing, poor user rights, etc. (private sector)

- **Raises the question:** How much/what types information does the government/organization need to function, deliver services, ensure security? How much information does the Citizen/Resident/Consumer need to know to be make informed choices? Consequences for mass collection of information?

Steps India is taking

- Specific recommendations in the *Report of Experts on Privacy* speak to transparency:
- Notice: what personal information is being collected, the purposes for which personal information, uses of collected personal information, whether or not personal information may be disclosed to third persons, processes available to data subjects to access and correct personal information, data breaches, notice to the individual of any legal access to their personal information after the purposes of the access have been met etc.
- Choice to opt in/opt out and withdraw consent
- Individuals shall have access to personal information about them held by a data controller; shall be able to seek correction, amendments, or deletion of such information where it is inaccurate; be able to confirm that a data controller holds or is processing information about them; be able to obtain from the data controller a copy of the personal data
- Data controllers must take steps to ensure that privacy practices made in an intelligible form, using clear and plain language, available to all individuals.

Conclusion

Transparency should be looked at holistically with one part focusing on if information should be disclosed or not: process behind making a piece of information transparent, reasons for the collection of information, the nature of the information collected, whether consent is to be taken at the time of collection and if this consent is withdrawable and defined within a timeframe and usage restriction.

Accuracy of the information is verified, in what format and what aspects of the information will be made publicly available, for how long the information will be made publically available, if and how the information will be destroyed.

Privacy safeguards should incorporate transparency requirements to ensure the individual is informed: Notice, annual reports, options.

Transparency and privacy needs to be actionable and followed with ways for action to be taken: redress, appeal, penalties, forums for public input etc., auditing

Thank you

Questions and Comments