PRIVACY BY DESIGN AND THE LAW

TLA

Advocates & Legal Consultants

Bangalore

Network Offices

Chennai ▪ Delhi ▪ Hyderabad ▪ Mumbai

Privacy

- What is privacy? What do people consider private?
- Ability of a person to keep to themselves.
- Informational privacy- ability of a person to withhold information of himself/herself i.e. information that is related to their person.
- Many socio-cultural factors on how privacy is interpreted.
- Predominantly a western concept.

Technology and privacy

- Growth of technology- increase in intrusion into the privacy or private lives of people.
- Increased ability to gather or collect information about a person, leading to knowledge of intimate details of the person.
- Technology has primarily led to the intrusion of informational privacy of an individual.
- Negative implications for retaining privacy- law steps in.

Right to privacy

- Right to be let alone;
- Recognised as a fundamental right in the Constitution of India and therefore is a legal right.
- Importance of informational privacy- stressed by the Supreme Court.
- Data Protection Bill, 2018 – separate legislation to protect informational privacy.

Privacy by Design

- Developed as an approach to systems engineering.
- Privacy of an individual to be taken into account throughout the engineering/ designing process.
- Formalized as a framework and widely accepted in the field of privacy enhancing technologies or PET. Eg: encryption technologies.
- Translated into law recently so that privacy laws could catch up with technology.

What is privacy by design

- Privacy and data protection must become an organization's default mode of operation.
- Applied to all types of personal information i.e. any information that has the ability to identify an individual.
- Objective: Ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage.
- Consists of 7 foundational principles.

Foundational Principles

- Proactive not reactive; Preventative not Remedial
- Privacy as the Default Setting
- Privacy Embedded into Design
- Full Functionality — Positive-Sum, not Zero-Sum
- End-to-End Security — Full Lifecycle Protection
- Visibility and Transparency — Keep it Open
- Respect for User Privacy — Keep it User-Centric

1. Proactive not reactive; preventive not remedial

- Anticipates and prevents privacy invasive events before they happen.
- Does not wait for privacy risks to materialize.
- Does not offer remedies for resolving privacy infractions once they have occurred.
- Practice: Recognition of poor design and making correction before negative impact can be realized.

2. Privacy as the Default Setting

- Built into the system by default- individual does nothing.
- No action is required on the part of the individual to protect their privacy.
- Practices such as purpose limitation, collection limitation, become pertinent.
- Practice: Determine the context, nature and purpose of processing the data collected beforehand.

3. Privacy Embedded into Design

- Embedded into the design and architecture of IT systems and business practices.
- Not an add-on or patch to the main architecture of the system or product.
- Privacy becomes a component that is essential to the core functionality of the system.
- Practice: Carry out privacy impact assessments.

4. Full Functionality — Positive-Sum, not Zero-Sum

- Accommodate all legitimate interests and objectives in a positive-sum "win-win" manner.
- Avoids the pretence of false dichotomies, such as privacy versus security, demonstrating that it is possible to have both.
- Practice: Make privacy a core functionality and not as an afterthought only for compliance purposes.

5. End-to-End Security — Full Lifecycle Protection

- Extends securely throughout the entire lifecycle of the data involved.
- Ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion.
- Practice: Strong encryption, access controls and logins and secure destruction.

6. Visibility and transparency – keep it open

- Assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives.

- Practice: Privacy related practices and policies must be documented and users must be made aware. Key is transparency.

7. Respect for User Privacy — Keep it User-Centric

- Architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.
- Keep it user-friendly.
- Making processing of data subject to consent.

Translation into law

- Was initially adopted as a resolution by the International Assembly of Privacy Commissioners and Data Protection Authorities in 2010.
- Adopted by the European Union under General Data Protection Regulation (GDPR)- first time as a legal mandate.
- Data Protection Bill, 2018
- Translated in the form of specific legal obligations.

GDPR

- Article 25- Data protection by design and data protection by default.
- Implementation of appropriate technical and organisational measures to protect the privacy rights of individuals.
- Specifically refer to data minimisation and pseudonymisation.
- Data minimization by default is mandated.

Data Protection Bill, 2018

- Implementation of policies and measures that protect the data subjects;
- Obligations under law are embedded in organisational and business practices.
- Legitimate business interests achieved without compromising privacy interests.
- Privacy is protected throughout processing from point of collection to point of deletion.
- Interest of individual accounted at every stage of processing.

Practical PbD- a guide to designers

- Conduct Privacy impact assessment •
- Review contracts with 3rd party data processors you interface with •
- Don’t require unnecessary app permissions •
- Review the security of your system.

How do we implement?

- No “checklist” approach.
- Should be approached contextually in light of the product or service, the data type and the nature of processing.

Implementation Approach- Case Study

Case Study: A fitness wearable device that measures the number of steps and sleep patterns of an individual.

Requirement: Collection of the relevant data to measure the parameters of the individual, which will be done at central servers.

Privacy Issue: Transmission of sensitive data of an individual that enables his/her identification and inference of health.

Approach: Anonymization and encryption of data at the time of transmission to the server and processing.

Vidyut Bedekar, Partner and Co-Founder, TLA
Contact: vidyut@tlaindia.com

Anjana Ravi, Associate, TLA
Contact: anjana@tlaindia.com

TLA

Advocates & Legal Consultants

Bangalore

Network Offices

Chennai ▪ Delhi ▪ Hyderabad ▪ Mumbai