Consumer Awareness Workshop on Privacy and Data Protection

CUTS International

Presented by:
Rahul Sharma
Country Leader – India, IAPP
Founder - The Perspective

01-11-2019
• India among fastest growing economy and likely to remain so in 2020.

• Govt. of India has outlined an ambitious vision to accelerate current GDP growth and build a $5 trillion economy by 2025.

• Agriculture, Manufacturing and 12 service sectors have been selected for accelerating growth through focused interventions

• India’s digitalisation roadmap can create a $1 trillion digital economy by 2025 –20% of India’s GDP and accelerate GDP growth by 0.5-1%

• India’s growth story will embed inclusion as a key priority and digitalisation will enable access and affordability
How do we understand Personal Data? Concepts and Analogies

A. Unalienable Self

B. Fundamental Right to Privacy of personal information

C. Ownership of Data? Individual/Community/State ownership

D. Rights over data akin to property rights

E. Data as Natural Resource, a fuel (oil/water/gold/uranium) of digital economy
Context of Data Ecosystem

- Aggressive Digitization
- Technological Innovations
- Sharing Economy & Democratization of Society
- Everything getting captured & recorded
- Generation of Millennials – attention span, connectedness

- Technology driven Economics & GDP
- Global Trade integration, and Trade wars
- Rising Extremism & Threats
- Reactionary Laws & Regulations
- Geo-Politics; Digital Diplomacy

- Fear of Monopolies
- Regulatory Infrastructure & Enforcement
- Data Breaches becoming a norm
- Market Forces – Criminals, Innovators & Protectors
Ever Expanding Identity Portfolio

what the machine thinks about you

what your behaviour tells them

what you share
Who is Randall Stevens?
When Identification is not desirable....

March against Digitization
Concealing Identity!
Stakeholders’ Perspective(s)

- Citizens
- Employees/Contractors
- Principals
- Government
- Security & Sovereignty
- Duties & Rights
- Integrated Global Outlook; Economy, Trade & Jobs
- Business
- Data & Tech Economy
- Indigenous Startups
- MNCs – Inbound & Outbound
- Processing Economy
- Other Institutions
- Courts
- International Organizations
- Independent Regulators
Drivers of Privacy Protection

- Increasing Awareness on Exercising Privacy Rights
- Data collection, its economic value and usage by businesses
- Mass surveillance programs by nation states
- Impact of globalization and trans-border data flows
- Legal and regulatory requirements
- Increasing privacy breaches and concerns related to resulting impact on organizations’ brand value
Data Privacy is measured as one’s ability to control his/her personal information.

**Types of Privacy**

- **Information or Data privacy** of one’s personal information
- **Physical or Bodily privacy** of one’s body and self being
- **Territorial privacy** of one’s territory and environment
- **Communication privacy** of one’s communication

**Evolution of Privacy**

<table>
<thead>
<tr>
<th>1890</th>
<th>1940</th>
<th>1950</th>
<th>1967</th>
<th>1980</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Right to be let alone</em></td>
<td><em>Fundamental civil liberty</em></td>
<td><em>Universal Declaration of Human Rights</em></td>
<td><em>Modern definition, claim of individual</em></td>
<td><em>OECD Privacy Principles</em></td>
</tr>
</tbody>
</table>

- Protection from government surveillance
- Government disclosure of private databases

- Access to centralized databases - *file system or an electronic record*
- Info available online & collected thru databases - *used for profiling*
- Internet making info available in real time- *Information centric business models*
### Important privacy terms and concepts

<table>
<thead>
<tr>
<th>Data Subject</th>
<th>An individual whose personal information is being referred to. It could be collected from them directly or from another source. The individual could be an end-customer, consumer or an employee of an organization. Data Subject is a very important term in privacy and the reader will find it used frequently.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Fiduciary (Controller)</td>
<td>An organization that determines means and purpose for data processing is called a Data Controller. It may or may not be the organization that directly collects PI from a data subject but, is accountable for PI usage, security, etc. All organizations are Data Controller by default for their employees’ PI.</td>
</tr>
<tr>
<td>Data Processor</td>
<td>An organization that processes PI based on instructions of Data Controller. In some instances, it may also be the organization that collect PI directly from the individuals, on behalf of Data Controller. A BPM organization processing personal information on behalf of clients would be a data processor. Similarly, a sales agent for a bank would also come under this category.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Personal Information (PI)</th>
<th>Any information that relates to an individual</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Sensitive Personal Information (SPI)</th>
<th>Particularly sensitive category of PI - where the loss or leakage of this information can cause harm &quot;or adversely affect&quot; the person in question.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Health Information (PHI)</td>
<td>This PI category refers specifically to information pertaining to the health of an individual. Health information is considered to be sensitive.</td>
</tr>
<tr>
<td>Personal Financial Information (PFI)</td>
<td>This PI category refers with all sorts of financial information about individuals. Many Laws and regulations around the world also categorize this as SPI.</td>
</tr>
</tbody>
</table>

| Personal Identifiable Information (PII) | Information about a person that can uniquely identify a person, either on its own or when used in combination with other information. |
Privacy Principles

Notice
A notice is a clear and easily accessible statement, provided by a data controller to a data subject, about its privacy policies and practices.

Choice
Choice refers to the options that a data controller gives the data subject with respect to the provision of personal information by the data subject.

Consent
Closely linked to the Choice principle, Consent requires that the data controller obtains consent from the data subject on matters related to the collection, use, and disclosure of personal information. Further, this should be done in a manner which the individual data subject clearly understands.

Collection Limitation
The collection of personal information from data subjects by an organization should be limited to the purposes identified in the notice and for which consent has been taken. Secondly, any such information should be obtained by lawful and fair means.

Use Limitation or Purpose Limitation
The Use Limitation or Purpose Limitation principle requires that the data controller may disclose, make available or otherwise use the PI collected from the individual data subject solely for the purposes identified in the notice and for which the individual has provided implicit or explicit consent or as required by the law.
<table>
<thead>
<tr>
<th>Privacy Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access and Correction</strong></td>
</tr>
<tr>
<td>The Access and Correction Principle centres around the right of an individual to know what information about them is being held by a data controller and to ensure that it is accurate, complete, relevant, and kept up to date for the purposes identified in the notice.</td>
</tr>
<tr>
<td><strong>Transparency/Openness</strong></td>
</tr>
<tr>
<td>The principle of Transparency or Openness requires that data controllers inform data subjects about their privacy related policies and practices in an easily understandable language and format. They should also be made easily and readily available to a data subject.</td>
</tr>
<tr>
<td><strong>Accountability</strong></td>
</tr>
<tr>
<td>The Accountability principle requires that the data controller should be accountable for complying with measures that give effect to Privacy Principles.</td>
</tr>
<tr>
<td><strong>Security/Safeguards</strong></td>
</tr>
<tr>
<td>The Security Principle requires that the data controller should protect personal information that they collect or have in their custody with reasonable security safeguards against loss, unauthorised access, destruction, use, modification, disclosure or other reasonably foreseeable risks.</td>
</tr>
<tr>
<td><strong>Disclosure</strong></td>
</tr>
<tr>
<td>The principle of Disclosure requires that the data controller discloses personal information to third parties only for the purposes identified in the notice, with the consent of the individual, or as required for lawful purposes. Third parties refer to not only business partners or data processors but also includes public authorities, Law Enforcement Agencies, etc.</td>
</tr>
<tr>
<td>Year</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>2008</td>
</tr>
<tr>
<td>2011</td>
</tr>
<tr>
<td>2012</td>
</tr>
<tr>
<td>2014</td>
</tr>
<tr>
<td>2015</td>
</tr>
<tr>
<td>2017</td>
</tr>
<tr>
<td>2018</td>
</tr>
</tbody>
</table>
Some easy ones!

1. yvcarpi  Privacy
2. ofifnle  Offline
3. epttnra  Pattern
4. ciyplo  Policy
5. barceh  Breach
6. cideinnt  Incident
Legal Framework in India – ITAA, 2008

• **IT Act 2000** - An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication; effective from October 17, 2000

• **IT (Amendment) Act, 2008** – IT Act 2000 amended to include (not limited to):
  - **Data Protection** – Security & Privacy
  - **Cyber Security** – Role of CERT-In, Nodal Agency for Critical Information Infrastructure Protection
  - **National Security** – information retention, interception & monitoring
  - **Computer related offences** to include cyber terrorism, identity theft, pornography, violation of privacy, etc.
  - **Role of Intermediaries** – Safe Harbor
  - **Encryption Policy**
  - **Increase in penalties**

---

**Sec 43A** – “Where a body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.”

**Sec 72A** – “Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.”
Definition of ‘Sensitive Personal Data or Information’
“(i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.”

Definition of ‘Reasonable Security Practices’
“means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.”

Further to this definition of Reasonable Security Practices, the central government notified certain rules under Section 43A namely The Information Technology (Reasonable Security Practices and Procedures and Sensitive personal data or Information) Rules, 2011. Rule 8 under these rules talks more in detail about the definition of Reasonable Security Practices and Procedures as follows:

- Security Program having managerial, technical, operational & physical controls commensurate with assets being protected
- Referenced: ISO 27001 or Codes of Practices by industry associations approved by the government (self-regulation)
- Audit once a year by independent auditor, duly approved by the central government
Privacy Principles

**Notice**
A notice is a clear and easily accessible statement, provided by a data controller to a data subject, about its privacy policies and practices.

**Choice**
Choice refers to the options that a data controller gives the data subject with respect to the provision of personal information by the data subject.

**Consent**
Closely linked to the Choice principle, Consent requires that the data controller obtains consent from the data subject on matters related to the collection, use, and disclosure of personal information. Further, this should be done in a manner which the individual data subject clearly understands.

**Collection Limitation**
The collection of personal information from data subjects by an organization should be limited to the purposes identified in the notice and for which consent has been taken. Secondly, any such information should be obtained by lawful and fair means.

**Use Limitation or Purpose Limitation**
The Use Limitation or Purpose Limitation principle requires that the data controller may disclose, make available or otherwise use the PI collected from the individual data subject solely for the purposes identified in the notice and for which the individual has provided implicit or explicit consent or as required by the law.
**Privacy Principles**

**Access and Correction**
The Access and Correction Principle centres around the right of an individual to know what information about them is being held by a data controller and to ensure that it is accurate, complete, relevant, and kept up to date for the purposes identified in the notice.

**Transparency/Openness**
The principle of Transparency or Openness requires that data controllers inform data subjects about their privacy related policies and practices in an easily understandable language and format. They should also be made easily and readily available to a data subject.

**Accountability**
The Accountability principle requires that the data controller should be accountable for complying with measures that give effect to Privacy Principles.

**Security/Safeguards**
The Security Principle requires that the data controller should protect personal information that they collect or have in their custody with reasonable security safeguards against loss, unauthorised access, destruction, use, modification, disclosure or other reasonably foreseeable risks.

**Disclosure**
The principle of Disclosure requires that the data controller discloses personal information to third parties only for the purposes identified in the notice, with the consent of the individual, or as required for lawful purposes. Third parties refer to not only business partners or data processors but also includes public authorities, Law Enforcement Agencies, etc.
Privacy risks include, but not limited to:

- failure to have the appropriate legal authority to collect, use or disclose personal information;
- excessive collection of PII (loss of operational control);
- unauthorized access to PII (loss of confidentiality);
- unauthorized modification of the PII (loss of integrity);
- loss, theft or unauthorized removal of the PII (loss of availability);
- unauthorized or inappropriate linking of PII;
- failure to keep information appropriately secure;
- retention of personal information for longer than necessary;
- processing of PII without the knowledge or consent of the PII principal (unless such processing is provided for in the relevant legislation or regulation); and
- sharing or repurposing PII with third parties without the explicit informed consent of the data subject.
### Types of PETs

**General Privacy Controls**
- Users control over their data
- Identity Protection

**Types (PETs that provide)**

**Anonymity and Anonymization**
- Anonymity techniques keep the identity of a user under wraps, thus ensuring privacy of the user. Anonymization, on the other hand, is a technique of stripping the identity of an individual or a set of individuals from the data.

**Data loss prevention**
- Also known as Data Leakage Prevention, or Information Leak Detection and Prevention, it is a technical solution that helps an organization to govern and control what data can be transferred across organizational assets and networks, based on predefined rules and policy configurations.

**Encryption**
- Encryption is a process that alters data in a way that makes it illegible and completely different from the original data. There are various ways in which this can be done. The hallmark of a good algorithm is that even if the algorithm is known to a hacker, he would still not be able to decrypt the data if he does not know the key used for encryption.

**Data masking**
- Data masking is the process of de-identifying (masking) specific data elements while rendering the data from data stores to users. Data masking often comes up as a solution to conflicting requirements.
Now time for some Challenging Stuff!

1. **fmnirtoonia** Your Personal __? **Information**
2. **vnstiesei** Sec 43A talks about protecting **Sensitive**
3. **mttiyaru** Standards Advocate __ of Practices **Maturity**
4. **oicnctelol** Orgs should limit ____ ? **Collection**
5. **ontstoridanem** Synonym for Show / Exhibit **Demonstration**

Lastly

6. **trngaielou** Compliance with ____ ? **Regulation**
Questions?

Thank You

Rsharma@iapp.org
ThePerspective.Rahul@Protonmail.ch