Security Management - Privacy protection

Dr. Kaniz Fatema
Trinity College Dublin
Feb, 2016
Privacy? Do we care ....

Some people do, may not to others’ privacy at least their own...
It's sad yet ironic that Zuckerberg has to go through great lengths to protect his privacy. Yesterday news broke that Facebook was removing yet another privacy feature. Soon, even people who wish to remain hidden from Facebook searches will have no choice but to be searchable on the social network.
- Business Insider 11 Oct 2013

He made his fortune by persuading over a billion people to share their lives online, but when it comes to protecting his own privacy Mark Zuckerberg appears to spare no expense: the Facebook founder has reportedly spent $30m (£18.8m) buying four houses that surround his own home in California.
- The Guardian 11 Oct 2013
Any real life experience on privacy threat?
Do you think you are doing enough to protect your personal data?

Time to wake up ....
What does privacy mean to you?

Privacy = secrecy?
What is privacy?

Privacy is a fundamental human right which was first defined as “the right to be left alone” by the United States Supreme Court Justice Louis Brandeis and Samuel Warren [3].

Some other views of privacy are – the protection of an individual’s independence, integrity, dignity, secrecy, anonymity, solitude, protection against intrusion into an individual’s personal life or affairs [4].

Professor Roger Clarke has defined the different dimensions of privacy [5] – Privacy of person, which is also referred to as 'bodily privacy', is concerned with the integrity of an individual's body such as blood transfusion without consent, compulsory provision of samples of body fluids and body tissue and so on. Privacy of personal behaviour relates to all aspects of behaviour such as sexual preferences and habits, political activities and religious practices. Privacy of personal communications relates to privacy of communications using various media without being monitored. This is sometimes referred to as 'interception privacy'. Privacy of personal data is also referred to as 'data privacy' and 'information privacy', relates to controlling whether or how personal data can be gathered, stored, processed or selectively disclosed.
What is privacy?
Privacy is a legal right ...

Global Laws on Privacy & Data Security

Multi-Country
- APEC Privacy Framework
- OECD Guidelines
- European Convention for Human Rights
- EU Directives

- GLBA
- COPPA
- HIPAA/HITECH
- Safe Harbour
- FLCP
- LFTAIPG

- PIPEDA
- UK DPA
- BDSG
- Privacy Code
- JPIPA
- IT (Amendment) Act
- Privacy Act
- National Privacy Principles
- ECTA PIPB

© Achintya Agarwal
Privacy is a legal right …

By January 2015 the total number of countries with data privacy laws has increased by over 10% to 109. [10]
The privacy policy principles

Common privacy policy principles on privacy laws around the world

Australian Law Professor Graham Greenleaf finds ten elements common to all four international privacy instruments (the OECD Guidelines, Council of Europe Convention, EU Data Protection Directive, and the APEC Privacy Framework):
1. Collection - limited, lawful and by fair means; with consent or knowledge
2. Data quality – relevant, accurate, up-to-date
3. Purpose specification at time of collection
4. Notice of purpose and rights at time of collection
5. Uses limited (including disclosures) to purposes specified or compatible
6. Security through reasonable safeguards
7. Openness to personal data practices
8. Access – individual right of access
9. Correction – individual right of correction
10. Accountable – data controllers accountable for implementation
Comparison of Global Data Privacy regulations

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Choice &amp; Consent</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Collection Limitation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Use Limitation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Retention Limitation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Disclosure</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Access &amp; Correction</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data Quality</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Enforcement</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Openness</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Anonymity</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Transborder Data Flow</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Breach Notification</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Identifier Limitation</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Source Identification</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

© Achintya Agarwal
What are personal data?

According to the Data Protection information can be personal data if any of the following conditions is true:

• If the information (in conjunction with other information) can identify a living individual.
• The information relates to an identifiable living individual.
• The information is obviously about a particular individual; e.g. medical record, criminal record.
• The information is linked to an individual.
• The information informs or influences actions or decisions affecting an identifiable individual.
• The information has biographical significance in relation to the individual.
• The information focuses on the individual as its central theme.
• The information has impact (or potential to impact) on an individual.
Privacy VS Security
## Privacy VS Security

<table>
<thead>
<tr>
<th>Privacy Criterion</th>
<th>Reporting of processing</th>
<th>Transparent processing</th>
<th>&quot;As required&quot; processing</th>
<th>Lawful basis of data processing</th>
<th>Data quality conservation</th>
<th>Rights of the parties involved</th>
<th>Data traffic with countries outside EU</th>
<th>Processing personal data by processor</th>
<th>Protection against loss and unlawful processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Availability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Time for brushing up your awareness on privacy
Privacy breach payoff

By LISA W. FODERARO  SEPT. 29, 2010

Tyler Clementi, left, is thought to have committed suicide, days after he was secretly filmed and broadcast on the Internet. Mr. Clementi’s roommate, Dharun Ravi, center, and another classmate, Molly Wei, have been charged in the case. Center and right, The Star-Ledger
There can be a number of negative consequences that can be occurred due to the lack of or poor privacy protection. For example –

- Harm to the person whose data are used or disclosed inappropriately.
- Become Victim of identity theft
- Damage to an organisation’s reputation.
- Financial loss.
- Loss of business due to negative publicity.
- Violation of privacy laws with the possibility of paying huge penalties.
- Destruction of confidence and trust in the industry.
Cloud computing

It offers computing as an on demand, location and device independent service over the internet.
Cloud introduces new privacy challenges?

• Data are shared among multiple providers. Multiple providers can have different terms of service, policies and location.

• Lack of organizational control over employee- more possibility of insider threats.

• Service provider typically do not have control over the physical location of the data.

• Possibility of leaving multiple copies of the same data- leading to more data management problems and possibilities of disclosure.

• Identity management for a number of providers.

• Conflicting laws from different jurisdictions.
Consumer VS Provider perspective

Where are my data going?
Data life cycle in the Cloud

Phase 1  Generation
Phase 2  Transfer
Phase 3  Use
Phase 4  Share
Phase 5  Storage
Phase 6  Archival
Phase 7  Destruction

[16, 17]
Phase 1: Data generation

1. Data collected about individuals, e.g., during registration process for a service.
2. Data can be created by themselves, e.g., file or picture uploaded by individuals.
3. Data can be gathered from the context, e.g., time of using a cloud service, location and device used for the service.
4. Inferred data deduced from the own data and monitoring data, for example, a person’s credit score from his transaction records.
Phase 1: Data generation

Things to consider at this stage

1. Data ownership
2. Data classification
3. Collection Limitation
4. Purpose specification
5. Consent
Phase 2: Data transfer

Things to consider at this stage

Encryption: While transferring via public network encryption is necessary to protect confidentiality and integrity of data.
Phase 3: Data use

Things to consider at this stage

1. **Appropriateness**: The use of information should be consistent with the purposes for which it was collected and the commitments made to the consumer by the provider.

2. **Access control**: Proper access control should be enforced.

3. **Legal compliance**: Information needs to be managed in way that the compliance with the legal requirements can be verified.
Phase 4: Data share

Things to consider at this stage

1. **Consent:** While sharing data with a third party consent of the data subject needs to be considered.
2. **Access control:** Access control mechanism should allow only the authorised party to access the data.
3. **Location control:** While sharing data the location of data where it is going would be an important factor to consider due to compliance requirement.
4. **Sharing granularity:** Sharing granularity depends on the sharing policy and the granularity of content.
Phase 4: Data share

Things to consider at this stage

5. **Data transformation**: Before sharing personal data, some transformation might be necessary, e.g., isolation of sensitive information, ensure anonymity and unlinkability.

6. **Notification**: Some regulations require the data subject to be notified when data is shared. Therefore, notification mechanism needs to be considered.
Phase 5: Data storage

Things to consider at this stage

1. **Encryption or transformation**: Data stored in the cloud can be encrypted. It might be difficult to process or doing search in the encrypted data. Other forms of transformation might be used, e.g., isolation of sensitive information, ensure anonymity and unlinkability.

2. **Access control**: Proper access control should be enforced also should consider insider attack.

3. **Location control**: While storing data the location of data where it is being stored would be an important factor to consider due to compliance requirement.
Phase 6: Data archival

Things to consider at this stage

1. **Storage media:** Portability of storage media might increase the possibility of losing data.
2. **Duration of storage:** Data can be stored only for the time necessary for which it was collected.
Phase 7: Data destruction

Things to consider at this stage

**Complete erasure of all copies**: Proper care should be taken to ensure all the copies of the unwanted data are deleted.