PRIVACY PRINCIPLES FOR TECHNOLOGY

Shukun Tokas

Research Scientist,

Trustworthy Green IoT, SINTEF Digital

(shukun.tokas@sintef.no)

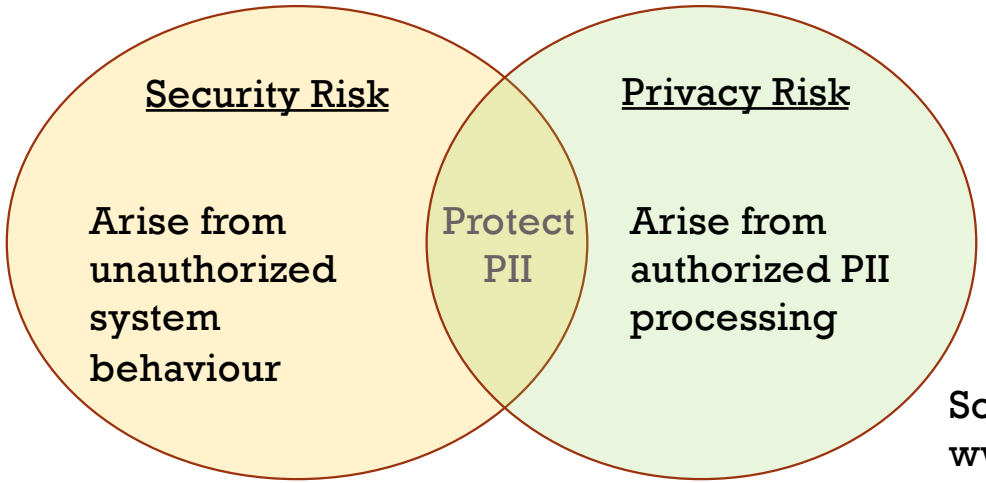
What does privacy mean to you?

PRIVACY

- A fundamental human right (EU)
  - Respect for private life, family life, communications
- Privacy is a subset of security?
  - Confidentiality alone increases person's sense of privacy?
    - Subject's ability to control access
- Several interpretations
  - Alan Westin's 4 states of privacy, Daniel Solove's taxonomy of privacy, Ryan Calo's harm dimensions

SECURITY VS PRIVACY

- The protection of personal information involves:
  - **Information security**: measures to prevent unauthorized access
  - **Information privacy:** regulate the access to a narrower set of the authorized uses with respect to regulatory requirements



Source: www.nist.gov/system/files/documents/2018/03/29/iot_roundtable_3.29.pdf

Personal data is everywhere!!









PRIVACY RISKS

- Likelihood that a privacy threat will exploit an IT vulnerability
- Impact of this exploit on the data subject and organization retaining information


PRIVACY RISKS ?

1. Surveillance

2. Aggregation

3. Decisional Interference

CAMBRIDGE ANALYTICA: CASE

- Was a political consulting firm. Worked on Trump campaign.
- Facebook exposed data on 87 million users.
- A researcher, Aleksandr Kogan built a FB app that was a quiz.
- The app exposed a loophole in Facebook API, and that allowed it to collect data from friends of quize takers.
- Data used for profiling and targetting US voters for Trump campaign.


General
Data
Protection
Regulation

GDPR

1. 99 articles and 173 recitals
2. Personal Data (Article 4(1))
3. Principles relating to processing of personal data (Article 5)

PERSONAL DATA

- **Personal data**, in terms of building blocks
  - 'Any information'
  - 'Relating to'
  - 'An identified or identifiable'
  - 'Natural person'

  - E.g., name, identification number, location data
- **Sensitive data**, processing could create significant risks to privacy
  - E.g., political beliefs, ethnic origin, health data

DATA SUBJECT

- Benefits from privacy
- Parenthically defined as and identified or identifiable natural person

DATA PROCESSING

- Operation or set of operations
  - Collection
  - Storage
  - Disclosure by transmission
  - Dissemination

Principles Relating to Processing of PII

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Confidentiality and integrity
7. Accountability

1. LAWFULNESS, FAIRNESS, AND TRANSPARENCY

- Lawfulness, if one of legal grounds exists

1. Consent
2. Contract performance
3. Legal obligation
4. Vital interest of individual
5. Public interest
6. Legitimate interest (processing is not required but is beneficial, e.g., fraud detection)

1. LAWFULNESS, FAIRNESS, AND TRANSPARENCY

- Fairness: Individual's awareness of processing
  - Sometimes, processing permitted by law and so is deemed fair
  - E.g., Data obtained by tax authorities from employer
  - E.g., Travel agency collecting behavioral data, fair?

1. LAWFULNESS, FAIRNESS, AND TRANSPARENCY

- Transparency: honest usage and communication with individuals about their personal data.

2. PURPOSE LIMITATION

- Collection and processing of personal data for
  - Specific
  - Explicit
  - Legitimate
- **Example:** A GP uses patient's information for diagnosis

2. PURPOSE LIMITATION

- Collection and processing of personal data for
  - Specific
  - Explicit
  - legitimate
- Example: A GP discloses patient list to his wife, who runs a travel agency, so that she can offer tailored holiday packages to patients needing recovery. (purpose limitation followed?)

3. DATA MINIMIZATION

- Only collect and process personal data that is relevant, necessary and adequate to accomplish the purposes.

- Example: An employer holds details of the blood groups of some of its employees. These employees do hazardous work and the information is needed in case of accident. But, if the employer holds the blood groups of the rest of employees, such information is irrelevant and excessive as they do not engage in the same hazardous work. (Violation of data minimization.)

4. ACCURACY

- Ensure data is accurate, and not misleading.
- Inaccuracies may have adverse implications for the individuals.

- **Example:** If an individual moves house from Oslo to Trondheim a record saying that they currently live in Oslo will be inaccurate.

5. STORAGE LIMITATION

- Personal data must not be kept longer than necessary for purposes it was collected for.
- (Irreversibly) Anonymized data may be kept for unlimited period.

- **Example:** Personal data may be needed for recruitment process and during the empoyment. Once recruitment process ends, controllers must not keep personal data of unsuccessful candidates.

6. CONFIDENTIALITY AND INTEGRITY

- ‘processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures’ -GDPR

7. ACCOUNTABILITY

- Different obligations with which an organisation must comply in order to show and evidence their compliance with the data protection framework.
- Implementing appropriate technical and organizational measures to demonstrate that processing is in accordance with regulation.

GDPR

CCPA

UK GDPR

PIPDEA

HIPPA

COPPA

Multi-jurisdictional privacy law compliance.

What does privacy mean to you NOW?

REFERENCES

- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434
- https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/
- https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal
- https://teachprivacy.com/category/cartoons-gdpr/
- https://teachprivacy.com/privacy-harms/


THANK YOU