Module 2: Homework 2

Harsh Siddhapura

Ira A. Fulton Schools of Engineering, Arizona State University

IFT 520: Advanced Information Systems Security

Dr. Jim Helm, Prof. Upakar Bhatta

September 01, 2023

“Review Questions”

1. **“Explain the term information privacy.”**

   Information privacy refers to the concept that a person has the ability or right to decide about how their personal information is to be collected, then how to use it and then how it should be shared. It incorporates the notion that every individual has the freedom to have control on how exactly their personal data is collected, where the data is kept and processed and then how the data is shared to the respected entities, people or the organizations. In today's era where the digital plays an vital role, it is very much important to look after information privacy to know how the enormous volumes of personal data is gathered and processed by the organizations which includes businesses, governments and internet platforms.

   Protecting the private or sensitive personal information or data from the unauthorized users that includes accessing the data, misusing the data or abusing the data is then referred to as information privacy. For protecting the data, one should secure their financial data, medical related history, browsing history and many other private data. People should be sure about whether to grant the consent for the collection or use of their data and the main motive should be people should be aware about how exactly their data is being used [1].

2. **“What is personally identifiable information?”**

   The medium through which we can easily get the information about the location, identification or try to contact the specific person is referred to as Personally Identifiable Information(PII). Through this we can get a variety of details like whether used together or separately, also can be used to identify a particular person. PII plays a crucial role in terms of gathering, using, and security of personal data by ensuring privacy and protection of data.

   Some of the examples include:

Name that is in the form of full name, last name, maiden name and so on. Contact information in terms of address of the place where the person is currently living, phone number of the person, email address. Personal details which include the person's date of birth, gender. Financial information which is the most private data that involves all credit card details including bank account details.

Organizations that gather and process PII are obliged to do so in accordance with data protection rules, such as the General Data Protection Regulation (GDPR) of the European Union and comparable legislation in other jurisdictions. By providing each individual with consent that all information provided is relevant, ensuring full security of data and preventing unauthorized access and granting them with all access, correction and deleting their PII [1].

Organizations and people must have the awareness of PII and should take all appropriate precautions to secure it since improper handling or illegal access to this information can result in privacy violations, identity theft, and other serious repercussions.

3. **“Explain the manner in which privacy by design and privacy engineering operate together.”**

Privacy by design (PbD) is a concept of designing systems that place user privacy at the center of system objectives. Most of these principles overlap security objectives of confidentiality, availability and integrity. In PbD, systems are designed to be proactive, respect user privacy, ensure full-system functionality without trading-off user privacy or the system’s security measures. Privacy engineering is a next step after PbD.

It defines the technical and administrative controls needed to implement and manage systems in a manner consistent with PbD. Both concepts, Privacy engineering and PbD, thus work together by sharing the same foundations for ensuring user privacy and having them embedded in system architectures and operations (Stallings, W., Chapter 2).

4. "What are the commonly accepted foundational principles for privacy by design?"

Below are the commonly accepted foundation principles of PbD, as guided by Stallings, W, (2019):

- Proactiveness- the system must proactively inform a user of their actions and how it can affect their privacy.
- Privacy by default - from the onset of design, systems protect PII. These protections (similar to privacy embedded in design) should not be an after-thought, but a core function in the architecture and design of IT systems.
- Full system functionality - system designers have to balance design systems that continue to operate with the least amount of PII, unless mandated by law. User consent must be highly respected.
- Transparency - systems ought to be accountable and clear about when PII is captured and processed. Users must also be able to view the policies that govern their PII and have the option to challenge their validity.
- Lifecycle protection - security principles of confidentiality, integrity and availability must remain throughout the life cycle of a system. Accurate and up-to-date records of PII also have to be maintained at all times.
- Respecting user privacy by allowing them to give consent to how the system handles PII, access to compliance framework employed and access to disclosures.

5. "What elements are involved in privacy risk assessment?"

The process of detecting, analyzing, and assessing possible privacy hazards connected with the collection, use, storage, and exchange of personal information is known as privacy risk assessment. This evaluation includes a number of components to ensure a thorough grasp of the privacy threats. These components commonly include:

- Data Inventory and Mapping: Identifying all sorts of personal data collected, processed, and stored by an organization. Understanding the sources of data, the objectives for which it is utilized, and the systems or databases in which it lives are all part of this.

- Data Flow Analysis: This is the process of mapping out the lifecycle of personal data within an organization, including its flow among multiple systems, departments, and third parties. This aids in the identification of possible places of vulnerability.
- Identifying possible privacy risks and hazards that may jeopardize the confidentiality, integrity, or availability of personal data. Unauthorized access, data breaches, poor data processing, and other hazards may be included.
- Threat assessment is the process of determining the possibility and possible effect of each identified privacy concern. This includes aspects such as data sensitivity, the possibility of an event occurring, and the possible harm to persons.
- Vulnerability analysis is the process of identifying flaws in systems, procedures, and regulations that might be exploited to trigger the identified privacy threats. This might include technological flaws as well as operational and procedural flaws.
- Legal and Regulatory Compliance: Ensuring that the organization's data processing practises are in accordance with applicable privacy laws and regulations, such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Health Insurance Portability and Accountability Act (HIPAA), and so on.

Organizations may undertake a thorough privacy risk assessment by taking these components into account, allowing them to proactively identify and manage any privacy issues related with their data processing operations.

6. “Describe the various types of privacy controls.”

Privacy controls are safeguards put in place to protect persons' personal information and guarantee compliance with applicable privacy laws and regulations. These controls are roughly classified as technological, administrative, and physical. The following is a breakdown of the numerous sorts of privacy controls found within each category:

1. Technical Controls:

a. Encryption: Encrypting sensitive data both at rest and during transmission to prevent unauthorized access.
b. Access Controls: Implementing mechanisms that restrict access to personal data based on roles and permissions. This includes user authentication, authorization, and access logs.
c. Anonymization and Pseudonymization: Removing or substituting personally identifiable information (PII) to reduce the risk of re-identification while still allowing data analysis.
d. Tokenization: Replacing sensitive data with tokens that have no intrinsic value, reducing the risk associated with storing actual PII.
e. Data Masking: Replacing parts of sensitive data with masked characters to limit exposure while maintaining data usability.
f. Audit Trails: Maintaining logs of data access and modifications for accountability and tracking purposes.
g. Secure APIs: Implementing secure application programming interfaces (APIs) for controlled data sharing between systems.
h. Firewalls and Intrusion Detection Systems: Implementing network security measures to prevent unauthorized access and detect potential breaches.
i. Data Loss Prevention (DLP) Tools: Monitoring and preventing the unauthorized movement or transmission of sensitive data.
j. Secure Data Storage: Employing secure databases and storage solutions with built-in encryption and access controls.

2. Administrative Controls:
    a. Privacy Policies and Procedures: Establishing clear guidelines for how personal data should be handled, processed, and shared within the organization.
    b. Data Classification: Categorizing data based on its sensitivity to determine appropriate handling and protection measures.
    c. Employee Training: Providing regular training to staff on privacy policies, data handling best practices, and recognizing social engineering attempts.

d. Privacy Impact Assessments (PIAs): Conducting assessments to identify and mitigate privacy risks before implementing new projects or processes.
e. Incident Response Plan: Developing a plan to respond effectively to privacy breaches and data incidents, including communication strategies.
f. Data Retention and Disposal Policies: Establishing guidelines for how long data should be retained and how it should be securely disposed of once it's no longer needed.
g. User Consent Management: Implementing mechanisms to obtain and manage user consent for data collection and processing activities.

3. Physical Controls:
    a. Access Controls: Restricting physical access to areas where personal data is stored or processed.
    b. Surveillance Systems: Implementing security cameras and monitoring systems to deter unauthorized physical access and detect potential breaches.
    c. Secure Facilities: Storing physical records and data in secure environments with limited access.
    d. Visitor Logs and Identification: Maintaining records of visitors to controlled areas and verifying their identities [2].

7. "What issues should be considered in selecting privacy controls?"

Privacy control deals with the measures taken by the organization or individual to protect PII (Personally Identifiable Information) from theft. There are a few considerations to be taken care of when privacy control is concerned.

- Organizations must check how sensitive the data is in terms of privacy. If the data is a biological trait or other important information, then it must be handled with care.
- The data must be handled with proper care from collection to destruction so that CIA is maintained.

- The collected data should be anonymized and tokenized to prevent others from disclosing the identity.
- There should be a continuous process of testing and monitoring to determine the effectiveness of privacy controls.
- The implementation of privacy controls should be portable and scalable with the business architecture.

8. "Explain the difference between privacy risk assessment and privacy impact assessment."

Privacy risk assessment and privacy impact assessment slightly differ from each other. Privacy risk assessment refers to the level of preparedness for an organization if any privacy incident happens. This risk assessment depends on four elements. These are Privacy – related assets, Privacy threats, Privacy vulnerabilities, and Privacy controls. Privacy assets are anything that organizations own and need to be protected from potential threats. A privacy threat is the potential violation of privacy that is harmful to organizations or individuals. Privacy vulnerability means a weakness or flaw in design that can be used by a threat to compromise personal data. Privacy controls refer to the measures that are taken into consideration to prevent and detect privacy incidents.

On the other hand, privacy impact assessment refers to the combination of privacy risk assessment and privacy control. A privacy impact assessment helps identify potential costs and value lost if privacy intrusion occurs. It also helps to identify the livelihood of a privacy incident. Moreover, it helps to determine the risks involved in violations of privacy and the possible threat to privacy related assets.

9. "What are the types of privacy testing?"

It involves a range of testing techniques and methods aimed at evaluating diverse aspects of privacy within an application or system.Types of privacy testing are:

- Data privacy testing:Assessing data encryption, data anonymization, and data retention policies.

- Permission and Consent Testing:Guaranteeing that users are properly informed about the use of their data and have the choice to either provide consent or decline.
- Third party integration testing:Assesses the privacy protocols of third-party components and services integrated into the application.
- User testing:Engages actual users to offer input on the application's privacy functionalities, configurations, and overall user experience.
- Cross-Browser and Cross-Platform Testing:For assessing the performance of an app or website on various browsers and platforms, we perform cross-browser and cross-platform testing as needed.
- Regression Testing:A development cycle that is executed after each change to confirm that the alteration doesn't unintentionally introduce any issues.
- Performance testing:evaluates an application's ability to sustain its stability, speed, scalability, and responsiveness when exposed to a defined workload.
- Load testing:Simulating concurrent access by multiple users to model the expected usage of a software program.

10. **“What are the overlapping and non-overlapping areas of concern with respect to information security and information privacy?”**

Overlapping area of concern:

- Data protection:It is the crucial endeavor of safeguarding sensitive information from potential harm, loss, or corruption. In today's rapidly expanding digital landscape, where data generation and storage are surging at unprecedented rates, the significance of data protection has never been more pronounced. Furthermore, the smooth functioning of businesses now heavily relies on data, and even a brief interruption or minor data loss can trigger significant repercussions for an organization.
- compliance:The process of guaranteeing an organization's compliance with industry regulations, standards, and legal requirements pertaining to information security and data privacy.

- Availability:Ensuring that information is readily available and can be accessed and utilized in a dependable manner. This property entails that data or information is accessible and usable whenever required by an authorized individual.

Non-overlapping areas of concern:

1. Information security:
    - Confidentiality:maintaining authorized restrictions on access and disclosure, which includes methods for safeguarding both personal privacy and proprietary information.
    - Integrity:preventing unauthorized alterations or destruction of information, and this includes measures to ensure the credibility and non-repudiation of information.
    - Availability:Guaranteeing that information is consistently accessible and can be used reliably and promptly when needed.
2. Information privacy:
    - Collecting of personal information:Obtaining permission from individuals prior to gathering and processing their personal information. It also encompasses offering transparent notifications regarding data collection procedures.
    - Data minimization:the importance of acquiring solely the essential data required for a particular purpose, thus diminishing the potential for excessive collection or misuse.
    - Purpose limitation:Personal data must be gathered solely for clearly defined, explicit, and lawful purposes and should not undergo subsequent processing that is inconsistent with those original purposes.

11. “Explain the trade-off between privacy and utility.”

Balancing privacy and utility are a crucial contemporary challenge. Privacy, a fundamental human right, emphasizes safeguarding personal information and preserving autonomy to prevent data misuse. Conversely, utility focuses on data's benefits, including improved services, better decision-making, and innovation. Achieving equilibrium requires thoughtful, ethical choices.

This balance varies by sector and context. Healthcare, for example, demands strict privacy measures to maintain trust and uphold ethics. Still, sharing de-identified patient data can advance medical research. E-commerce relies on data analysis for personalized recommendations, but transparency is vital for privacy.

Navigating this equilibrium means considering technology, ethics, and public sentiment's influence on data handling. As technology advances and norms evolve, the privacy-utility trade-off remains a challenge. Solutions involve regulatory frameworks, ethical guidelines, responsible data practices, and open dialogue. Striking this balance is crucial for harnessing data's potential while preserving the fundamental right to privacy. [4]

12. “What is the difference between usability and utility?”

Usability primarily concerns the ease with which users can interact with a product or system to accomplish specific tasks. It includes elements like user-friendliness, efficiency, learnability, and overall user satisfaction. Essentially, usability assesses how efficiently users can navigate a system or interface, emphasizing factors such as intuitive layouts, clear menus, and responsive design. A highly usable product ensures that users can easily understand its features, perform tasks efficiently, and leave with a satisfying experience.

Utility, on the other hand, focuses on the tangible value or practicality of a product or system in meeting users' needs and solving their problems. It evaluates whether the product serves a meaningful purpose or provides a solution to users' issues. Utility takes a broader perspective, considering the inherent functionality and relevance of the product or system. While usability concentrates on the effectiveness of user interaction, utility questions whether the product genuinely meets users' requirements and delivers actual value

References

[1] https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy

[2] ISO 27701, NIST Privacy Framework, regional regulations (e.g., GDPR, CCPA), and cybersecurity best practices from organizations like NIST (National Institute of Standards and Technology) and ISACA (Information Systems Audit and Control Association).

[3] Stallings, W. (2019). *Information privacy engineering and privacy by design: Understanding privacy threats, technology, and regulations based on standards and best practices* (1st ed.). Pearson Education, Inc.

[4] Hannabuss, S. (2010, August 17). Understanding Privacy20103Daniel J. Solove. Understanding Privacy. Cambridge, MA and London: Harvard University Press 2008.

[5] Komninos, A. (2023, September 1). *An Introduction to Usability*. The Interaction Design Foundation. https://www.interaction-design.org/literature/article/an-introduction-to-usability#:~:text=While%20usability%20is%20concerned%20with,become%20useful%20to%20their%20users.