Module 3: Homework 3

Harsh Siddhapura

Ira A. Fulton School of Engineering, Arizona State University

IFT 520: Advanced Information Systems Security

Prof. Upakar Bhatta

September 10, 2023

Review Questions

1. **“What is the GDPR definition of personal data?**

   Any information pertaining to a name or distinguishable as an identifiable natural person (data subject) is referred to as personal data under the General Data Protection Regulation (GDPR). An identifiable natural person is one who can be determined, either directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location information, an online identifier, or one or more factors particular to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. Essentially, personal data is any information that may be used to directly or indirectly identify a specific person which can happen when it is linked with other data or identifiers which not only consists of identifiable information like names and contact information, but also less blatant information like IP addresses, biometric data, and even specific online behaviors or preferences when they may be linked to a specific individual.

   The GDPR imposes strict obligations on the processing of personal data to protect individuals' rights and privacy, including getting individuals' unambiguous and informed consent for processing, granting them access to their data, and maintaining the security and confidentiality of personal data.

2. **Explain the distinction between sensitive PII and non-sensitive PII.**

   The distinction between the PII is in the severity of consequences that can follow from such data being compromised. For example; a family member’s medical records, financial information and social security number are highly sensitive PII, capable of bearing severe consequences if compromised. On the other hand, non-sensitive PII can be disclosed without causing severe harm to one’s privacy, for example, one’s name and work email address being shared on public platforms. Extra effort would be required to use non-sensitive PII to harm an individual.

3. Describe four categories of information that may relate to individuals.

Four types of information relating to people are medical records, government issued identification records, geographical location and property/asset ownership information. Financial information can be included, however, banks have made significant leaps to hide PII linking individuals to accounts. Thus, a fitting description for the various categories of PII is the ability to directly link the identity of a person (net worth, educational background, medical history, citizenship and much more using sample data.

4. What is re-identification? How is it accomplished?

Re-identification, often known as re-ID, is a crucial aspect of surveillance and security systems. It involves tracking individuals as they move across different camera views, enhancing security and awareness. To achieve re-ID, deep learning models like Convolutional Neural Networks (CNNs) extract unique features from individuals' images, such as clothing patterns and facial characteristics. These features are used to create a similarity metric, measuring how similar individuals are based on their features.

Re-ID systems use two image sets: a gallery set of known individuals and a probe set of those to be matched. Tracking algorithms maintain identities as people move between cameras, and models are fine-tuned for accuracy. Post-processing techniques refine the results.

Despite real-world challenges, ongoing research advances the re-identification role in surveillance and security. [4]

5. Describe the FIPPs defined by OECD?

The OECD's Fair Information Practice Principles (FIPPs) stand as a pivotal global framework for preserving data privacy in our ever-more digital world.

In the initial set of principles, there is a strong focus on the responsible acquisition of data, underscoring the importance of collecting data for valid reasons while ensuring full transparency.

The subsequent set of principles places significant emphasis on the use and safeguarding of data, obligating data to be employed exclusively for predetermined purposes while maintaining rigorous security measures to deter unauthorized access. These principles serve as the cornerstone for transparency, individual engagement, and organizational accountability, shaping the evolution of data privacy regulations worldwide. [5]

6. Give a brief overview of GDPR.

The General Data Protection Regulation (GDPR) is a comprehensive data protection and privacy regulation that was implemented by the European Union (EU) on May 25, 2018. It was designed to harmonize data protection laws across the EU member states and provide individuals with greater control over their personal data [1]. Here's a brief overview of GDPR:

- **Scope:** GDPR applies to organizations, both within and outside the EU, that process the personal data of individuals residing in the EU. It covers a wide range of personal data, including names, email addresses, financial information, and more.
- **Principles:** GDPR is built upon several key principles:
    - Lawfulness, fairness, and transparency: Data processing must be legal, transparent, and fair to individuals.
    - Purpose limitation: Data should only be collected for specific, legitimate purposes.
    - Data minimization: Organizations should collect only the data necessary for the intended purpose.
    - Accuracy: Data must be accurate and kept up-to-date.
    - Storage limitation: Data should not be retained longer than necessary.
    - Integrity and confidentiality: Organizations are required to ensure the security and confidentiality of data.
- **Rights of Individuals:** GDPR grants individuals several rights over their personal data, including:

    - Right to access: Individuals can request access to their data.
    - Right to rectification: Individuals can request corrections to inaccurate data.
    - Right to erasure: Individuals can request the deletion of their data under certain conditions.
    - Right to data portability: Individuals can obtain and reuse their data for different services.
    - Right to object: Individuals can object to the processing of their data in certain situations.
    - Rights related to automated decision-making: Individuals have the right to opt out of decisions based solely on automated processing.
- **Accountability and Governance:** Organizations are required to demonstrate compliance with GDPR through documentation, data protection impact assessments, and appointing Data Protection Officers (DPOs) in certain cases.
- **Data Breach Notification:** GDPR mandates that organizations report data breaches to relevant authorities and affected individuals within specific timeframes, depending on the severity of the breach.
- **International Data Transfers:** GDPR regulates the transfer of personal data outside the EU to ensure that the data protection rights of EU citizens are not compromised.
- **Penalties:** Non-compliance with GDPR can result in substantial fines, with penalties varying depending on the severity of the violation.
- **Consent:** GDPR sets strict standards for obtaining and managing consent for data processing, requiring clear and unambiguous consent from individuals.
- **Data Protection Impact Assessments (DPIAs):** Organizations are required to conduct DPIAs for high-risk data processing activities to assess and mitigate potential risks to individuals' data privacy.
- **Cooperation and Consistency:** GDPR established the European Data Protection Board (EDPB) to promote cooperation among EU data protection authorities and ensure consistent application of the regulation across member states.

GDPR represents a significant shift in the way organizations handle personal data and has had a global impact on data protection and privacy regulations. It emphasizes transparency, accountability, and individuals' rights, aiming to empower individuals and protect their personal information in an increasingly data-driven world.

7. **List some of the major privacy-related laws in the United States.**

In the United States, there are several privacy-related laws and regulations that specifically address internet and technology-related issues. Here are some of the major ones:

- **Electronic Communications Privacy Act (ECPA):** ECPA governs the interception of wire, oral, and electronic communications and restricts unauthorized access to stored wire and electronic communications and transactional records. It includes provisions related to email privacy and government surveillance.
- **Computer Fraud and Abuse Act (CFAA):** The CFAA makes it illegal to access computer systems and networks without authorization. It has been used to prosecute a wide range of cybercrimes, including hacking and unauthorized access.
- **Children's Online Privacy Protection Act (COPPA):** COPPA regulates the online collection of personal information from children under 13 years of age. It requires websites and online services to obtain parental consent before collecting data from young users.
- **California Consumer Privacy Act (CCPA):** While not exclusively focused on technology, the CCPA includes provisions related to online data collection, data access, and opt-out mechanisms. It grants California residents specific rights over their personal information.
- **Biometric Information Privacy Laws:** Some states, like Illinois and Texas, have enacted biometric information privacy laws that regulate the collection and use of biometric data, such as fingerprints and facial recognition technology.
- **Electronic Signatures in Global and National Commerce Act (ESIGN):** ESIGN validates electronic signatures and records, making electronic transactions legally enforceable.

- **Video Privacy Protection Act (VPPA):** VPPA restricts the disclosure of an individual's video rental or sale records. It has implications for online streaming and video services.
- **Wiretap Act:** The Wiretap Act, part of the ECPA, governs the interception of electronic communications and includes provisions related to internet wiretapping.
- **California Privacy Rights Act (CPRA):** CPRA builds on CCPA and introduces additional privacy protections, including new rights related to sensitive personal information and further regulation of data sharing and processing by businesses.
- **Health Information Portability and Accountability Act (HIPAA):** While primarily focused on healthcare, HIPAA has implications for the privacy and security of electronic health records and healthcare information online.
- **Gramm-Leach-Bliley Act (GLBA):** GLBA applies to financial institutions and includes provisions related to the security and confidentiality of customer information, which can be relevant to online banking and financial services.
- **Data Breach Notification Laws:** Many U.S. states have their own data breach notification laws, which require organizations to notify individuals in the event of a data breach. These laws often apply to breaches involving online and technology-related data.

These laws and regulations aim to protect the privacy of individuals and regulate the collection, storage, and use of personal information in the context of the internet and technology. It's important to note that the legal landscape for internet and technology privacy is continuously evolving, with ongoing discussions about the need for federal legislation to address these issues comprehensively [2].

8. What role does NIST play with respect to information privacy?

NIST, a U.S. federal agency focused on standards and technology, plays a global role in information privacy. Its Computer Security Resource Center (CSRC) provides essential resources in three categories: privacy controls, engineering, and a framework. Notably, SP 800-53 and SP 800-53A are pivotal. The former offers detailed privacy controls, while the latter outlines assessment procedures.

These controls span 20 families, addressing diverse privacy aspects and offering guidance for implementation and assessment. NIST's influence on information privacy extends internationally, helping organizations safeguard data and comply with regulations.

9. What contribution has ISO made to privacy standards?

ISO (International Organization for Standardization) has played a significant role in setting standards for privacy. These standards provide guidelines for organizations to protect personal information and ensure data privacy. Here are some key ones:

- ISO/IEC 27001: It's a general standard for information security that includes personal data protection.
- ISO/IEC 27018: Focuses on safeguarding personal data in cloud computing.
- ISO/IEC 27701: An extension of ISO 27001, specifically for managing personal data privacy.
- ISO/IEC 29100: Defines privacy concepts and terms.
- ISO/IEC 29151: Provides guidance on privacy notices, consent, and data access requests.

10. Explain the purpose of the ISF Standard of Good Practice for Information Security.

The ISF Standard of Good Practice for Information Security serves as a manual for organizations to safeguard their digital information effectively. It assists them in several crucial areas:

- **Adopting Best Practices**: It guides them on implementing the most effective methods to secure their data and computer systems.
- **Risk Management**: It aids in identifying and addressing potential security risks and threats.
- **Compliance**: For organizations subject to specific security regulations or laws, it helps them adhere to these requirements.
- **Promoting Security Awareness**: It emphasizes the importance of digital information security throughout the organization.

- **Continuous Improvement**: It provides instructions on how to enhance security measures over time and handle security incidents when they occur.
- **Collaboration with Partners**: It offers guidance on ensuring that their business partners and suppliers also maintain high levels of information security.
- **Crisis Preparedness**: It assists in planning for and responding to significant security events like cyber-attacks or disasters.

In essence, it acts as a valuable reference guide for organizations to protect their digital information and navigate the complexities of cybersecurity effectively.

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, *Chapter 3, Lecture not*es, Pearson Education, Inc.

[4] *Re-Identification of "Anonymous" Data is Scarily Simple - Anonyome Labs*. (2022, April 17). Anonyome Labs. https://anonyome.com/2020/12/re-identification-of-anonymous-data-is-scarily-simple/

[5] Fair Information Practice Principle(n.d.). https://iapp.org/resources/article/fair-information-practices/