Module 14: Homework 14

Harsh Manishbhai Siddhapura

Vaibhavi Nitin Honagekar

Arunava Lahiri

Thembelihle Shongwe

Sai Shashank Nagavaram

Anandha Krishnan Senthooraan

Group: Class96958 4

Ira A. Fulton School of Engineering, Arizona State University

IFT 520: Advanced Information Systems Security

Prof. Upakar Bhatta

December 01, 2023

Review Questions

1. **What are some of the key differences between the information privacy environment in the United States and that in the European Union?**

   The U.S. privacy landscape consists of a variety of federal and state privacy laws and regulations, some dating back to the 1970s, as well as common law created by judicial precedent. The EU depends upon a single regulation, the GDPR, which is common across all member states, each of which has a single supervisory authority or data protection authority to monitor and enforce the regulation [1].

   The differences between the information privacy environment in the United States and the European Union are significant. In the United States, privacy regulations are a patchwork of federal and state laws and regulations, often sector-specific and varying in scope. These regulations include the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Children's Online Privacy Protection Act (COPPA), among others. Additionally, privacy protection is often enforced through common law developed by court decisions.

   In contrast, the European Union has adopted a comprehensive and harmonized approach to data protection through the General Data Protection Regulation (GDPR). The GDPR applies uniformly across all member states, providing a consistent framework for the protection of personal data. It grants individuals greater control over their data, introducing concepts such as the right to be forgotten, data portability, and strict requirements for obtaining valid consent.

2. **Briefly describe the privacy aspects of the Fair Credit Reporting Act.**

   FCRA details the information that consumer credit reports may contain and how and by whom a consumer’s credit information can be used [2]. The Fair Credit Reporting Act (FCRA) governs the privacy aspects of consumer credit reports in the United States. It outlines the information that these reports can contain and stipulates who can access and use a consumer's credit information. The FCRA aims to ensure the accuracy and fairness of credit reporting and provides consumers with rights to dispute inaccuracies in their credit reports.

3. **Briefly describe the privacy aspects of the Fair and Accurate Credit Transactions Act.**

   Requires entities engaged in certain kinds of consumer financial transactions to be aware of the warning signs of identity theft and to take steps to respond to suspected incidents of identity theft [3]. The Fair and Accurate Credit Transactions Act (FACTA) complements the FCRA by addressing identity theft concerns. It requires entities involved in consumer financial transactions to be vigilant about signs of identity theft and mandates appropriate responses to suspected incidents. FACTA also introduced provisions for consumers to request and obtain free annual credit reports to monitor their credit information.

4. **Briefly describe the privacy aspects of the Right to Financial Privacy Act.**

   Entitles bank customers to a limited expectation of privacy in their financial records by requiring that law enforcement officials follow certain procedures before information can be disclosed. Unless a customer consents in writing to the disclosure of his financial records, a bank may not produce such records for government inspection unless ordered to do so by an administrative or judicial subpoena or a lawfully executed search warrant [4].

   The Right to Financial Privacy Act (RFPA) in the United States safeguards the privacy of bank customers' financial records. It establishes a limited expectation of privacy, requiring law enforcement to follow specific procedures before gaining access to such records. RFPA prohibits the disclosure of financial information without the customer's consent, except under lawful circumstances such as a court-issued subpoena or search warrant.

   These privacy laws collectively reflect the diverse and decentralized nature of privacy regulation in the United States, in contrast to the unified and comprehensive framework established by the GDPR in the European Union.

5. **Briefly describe the privacy aspects of the Family Educational Rights and Privacy Act.**

   Protects students and their families by ensuring the privacy of student educational records, while ensuring a parent’s rights to access his or her child’s education records, correct mistakes in those

records, and know who has requested or obtained the records. Educational records are agency- or institution-maintained records containing personally identifiable student and educational data. FERPA applies to primary and secondary schools, colleges and universities, vocational colleges, and state and local educational agencies that receive funding under any program administered by the U.S. Department of Education [5].

The Family Educational Rights and Privacy Act (FERPA) plays a crucial role in safeguarding the privacy of student educational records in the United States. Enacted to protect the rights of students and their families, FERPA ensures the confidentiality of educational records while allowing parents the right to access, correct errors, and be informed about who has requested or obtained these records. Educational records covered by FERPA include personally identifiable information about students and their educational history. The scope of FERPA extends to primary and secondary schools, colleges, universities, vocational colleges, and state and local educational agencies that receive funding from the U.S. Department of Education. By upholding the privacy of student records, FERPA promotes a secure educational environment and ensures compliance with privacy standards across various educational institutions.

6. What are the main goals of HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) encompasses several key goals aimed at improving the healthcare system in the United States. One of its primary objectives is to mandate continuous health insurance coverage for workers who lose or change their jobs, providing individuals with consistent access to healthcare coverage. Additionally, HIPAA strives to reduce the administrative burdens and costs associated with healthcare by standardizing the electronic transmission and protection of healthcare-related administrative and financial transactions. This standardization enhances efficiency, streamlines processes, and ensures the secure exchange of health information among different entities within the healthcare system.

- Mandate continuous health insurance coverage for workers who lose or change their job.

- Reduce the administrative burdens and cost of healthcare by standardizing the electronic transmission and protection of healthcare-related administrative and financial transactions [6].

7. What is the HIPAA Privacy Rule?

Officially known as the Standards for Privacy of Individually Identifiable Health Information, this rule requires safeguards to protect the privacy of patient data by setting limits and conditions on what information can be used and disclosed without patient authorization [7].

The HIPAA Privacy Rule, officially known as the Standards for Privacy of Individually Identifiable Health Information, is a crucial component of the broader HIPAA framework. This rule establishes safeguards to protect the privacy of patient data by setting specific limits and conditions on the use and disclosure of health information without patient authorization. The Privacy Rule empowers individuals by giving them greater control over their health information while ensuring that healthcare providers and other covered entities adhere to strict privacy standards. It also outlines the rights of individuals to access their health records, request corrections, and be informed about how their health information is used and disclosed. Through these provisions, the HIPAA Privacy Rule enhances the security and privacy of sensitive health data in the healthcare ecosystem.

8. To what categories of personal health information does HIPAA apply?

The HIPAA Privacy Rule protects most individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or medium, whether electronic, on paper, or oral. Individually identifiable health information, also referred Protected health information (PHI) is information that is a subset of health information (*HIPAA: Health Insurance Portability and Accountability Act | School of Dental Medicine*, n.d.) including demographic information collected from an individual, and:

- It is created or received by a health care provider, health plan employer, or health care clearinghouse.

- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual, or
    - With respect to which there is a reasonable basis to believe the information can be
    - used to identify the individual ("HIPAA: Health Insurance Portability and Accountability Act | School of Dental Medicine").

9. Under what circumstances may a HIPAA covered entity use or disclose PHI?

A covered entity is required to disclose PHI under one of the following conditions:

- The individual who is the subject of the information (or the individual's personal representative) authorizes in writing.
- HHS is undertaking a compliance investigation, review, or enforcement action.
- A covered entity is permitted to use or disclose PHI without an individual's authorization for the following purposes or situations:
    - To the individual
    - Treatment, payment, and health care operations
    - Opportunity to agree or object
    - Incident to an otherwise permitted use and disclosure
    - Public interest, law enforcement, and benefit activities
    - Limited dataset for the purposes of research, public health or health care operations, where direct identifiers relating to individuals, their families, and employers are removed.

10. Describe the two methods of de-identification permitted under HIPAA.

- Expert determination method: A person who is technically qualified applies de-identification or anonymization techniques and determines that the risk is very small that the information could

be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of the information.

- Safe harbor method: Involves the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

11. Under the HITECH Act, what risk assessment factors must a covered entity take into account in determining whether a breach notification is needed?

Under the HITECH Act, covered entities must consider several risk assessment factors when determining whether a breach notification is required. These factors include the nature and extent of the Protected Health Information (PHI) involved, taking into account the types of identifiers present and the likelihood of re-identification. Additionally, covered entities need to assess the unauthorized person who used the PHI or to whom the disclosure was made, whether the PHI was actually acquired or viewed, and the extent to which the risk to PHI has been mitigated. This comprehensive evaluation ensures that breach notifications are triggered when there is a significant risk to the privacy and security of individuals' health information, promoting transparency and timely response to potential breaches.

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the PHI or to whom the disclosure was made.
- Whether the PHI was actually acquired or viewed
- The extent to which the risk to PHI has been mitigated

12. Describe the technical measures mandated by the HITECH Act for the protection of data at rest.

- Full disk encryption: Encrypts the entire disk, except for software needed to boot the disk. This scheme uses an authentication method to enable booting. Once the device is booted, there is no protection of the data.

- Virtual disk encryption: Encrypts the contents of a container, which are protected until the user is authenticated for the container.
- Volume encryption: The same protection as virtual disk encryption, but for a volume instead of a container.
- File/folder encryption: Protects the contents of encrypted files (including files in encrypted folders) until the user is authenticated for the files or folders.

13. Describe the technical measures mandated by the HITECH Act for the protection of data in motion.

- Transport Layer Security (TLS): TLS is designed to make use of the Transmission Control Protocol (TCP) to provide a reliable end-to-end secure service. TLS is a complex protocol that allows users to authenticate each other and to employ encryption and message integrity techniques across a transport connection. SP 800–52 (Guidelines for the Selection and Use of Transport Layer Security Implementations) is the NIST specification.
- Virtual private networks (VPN) using IPsec: A VPN is a private network that is configured within a public network (a carrier's network or the Internet) in order to take advantage of the economies of scale and management facilities of large networks. VPNs are widely used by enterprises to create wide area networks that span large geographic areas, to provide site-to-site connections to branch offices, and to allow mobile users to dial up their company LANs. From the point of view of the provider, the public network facility is shared by many customers, with the traffic of each customer segregated from other traffic. Traffic designated as VPN traffic can only go from a VPN source to a destination in the same VPN. It is often the case that encryption and authentication facilities are provided for the VPN. IPsec is a set of Internet standards that augment the Internet Protocol (IP) and enable the development of VPNs at the IP level. SP 800–77 (Guide to IPsec VPNs) is the NIST specification.
- Virtual private networks (VPN) using TLS: An TLS VPN consists of one or more VPN devices that users connect to using their Web browsers. The traffic between the Web browser and TLS

VPN device is encrypted with the TLS protocol. TLS VPNs provide remote users with access to Web applications and client/server applications, and with connectivity to internal networks. They offer versatility and ease of use because they use the SSL protocol that is included with all standard Web browsers, so the client usually does not require configuration by the user. SP 800–113 (Guide to SSL VPNs) is the NIST Specification.

14. Describe the three technical measures authorized by the HITECH Act for media sanitization.

- Clear: Applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
- Purge: Applies physical or logical techniques that render target data recovery infeasible using state of the art laboratory techniques. This can be achieved by performing multiple overwrites. For a self-encrypting drive, cryptographic erasure can be used. If the drive automatically encrypts all user-addressable locations, then all that is required is to destroy the encryption key, which could be done by multiple overwrites.
- Destroy: Renders target data recovery infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the media for storage of data. Typically, the medium is pulverized or incinerated at an outsourced metal destruction or licensed incineration facility.

15. How is PII defined for the purposes of COPPA?

The law defines personal information as any information that identifies, relates, to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The Children's Online Privacy Protection Act (COPPA) defines Personally Identifiable Information (PII) broadly for the purposes of protecting children's privacy online. According to COPPA, personal information includes any data that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or

household. This expansive definition ensures that a wide range of information that could potentially identify or be linked to a child is covered by COPPA, enhancing the protection of children's privacy in the online environment.

16. What are the main requirements imposed by COPPA?

The California Consumer Privacy Act (CCPA) outlines several enforceable consumer rights concerning their personal information. Californians have the right to know what personal information is being collected about them, whether their personal information is sold or disclosed and to whom, the right to opt-out of the sale of personal information, access to their personal information, and the right to equal service and price, even if they exercise their privacy rights. These rights empower consumers to have greater control over their personal information and make informed decisions about its use, promoting transparency and accountability among businesses operating in California.

CCPA lists the following as enforceable consumer rights with respect to their personal information:

- The right of Californians to know what personal information is being collected about them.
- Californians have the right to know whether their personal information is sold or disclosed and to whom.
- The right of Californians to say no to the sale of personal information.
- The right of Californians to access their personal information.
- The right of Californians to equal service and price, even if they exercise their privacy rights.

References

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

UK Information Commissioner's Office (2023), *How do we do a DPIA?* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/, Online publication

Hannabuss, S. (2010, August 17). Understanding Privacy 20103 Daniel J. Solove. Understanding Privacy. Cambridge, MA and London: Harvard University Press 2008.

What are the Differences Between Anonymization and Pseudonymisation - Blogspot. (n.d.). https://www.privacycompany.eu/blogpost-en/what-are-the-differences-between-anonymisation-and-pseudonymisation

Wang, J., Du, K., Luo, X., & Li, X. (2018, June 29). Two privacy-preserving approaches for data publishing with identity reservation. *Knowledge and Information Systems*, *60*(2), 1039–1080. https://doi.org/10.1007/s10115-018-1237-3