Keeping It Under Wraps: Personally Identifiable Information (PII)

Will Robinson
Assistant Vice President
Information Security Officer & Data Privacy Officer
Federal Reserve Bank of Richmond

March 14, 2018

FEDERAL RESERVE BANK OF RICHMOND®
Richmond ▪ Baltimore ▪ Charlotte

Disclaimer: The views expressed are mine and not necessarily those of the Federal Reserve Bank of Richmond or of the Federal Reserve System.

Topics

- What is Data Privacy – A Sectoral Approach
- What is PII?
- Mitigating the Risks

What is Data Privacy?

- "Privacy" as a distinct legal and compliance objective emerged in the second half of the twentieth century, but is rooted in concepts stretching back as least as far as medieval England

- The most concise definition of "privacy" is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*

- Balancing individual and group interest in limiting disclosure against commercial, social, and legal demands for information is at the heart of contemporary American privacy practices

**Adapted from Alen Westin's Privacy and Freedom (1967)*

Privacy in the United States: A Sectoral Approach

There is no comprehensive data protection legislation or omnibus regulatory enforcement agency in the United States

Privacy in the United States: A Sectoral Approach

- Instead, America has taken a "sectoral approach" to privacy protection, adopting a mosaic of laws at the state and federal level covering:
  - Collection, use and disclosure of health information (HIPAA)
  - ***Collection, use and disclosure of financial information (GLBA + FCRA)***
  - Collection and use of information about minors (COPPA)
  - ***Improper disclosure of "personally identifiable information" (Breach Notification laws)***

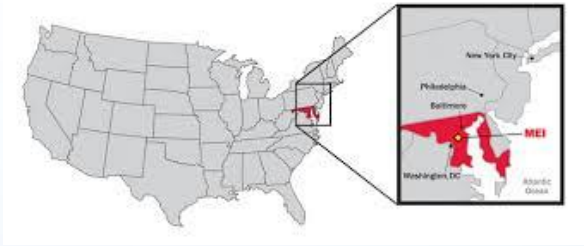
- **Graham Leach Bliley Act:** Security Rule & Safeguard Rule
- **Fair Credit Reporting Act:** Consumer Transparency

Privacy in the United States: A Sectoral Approach

- The sectoral approach requires careful analysis when determining what information about individuals is subject to legal or regulatory limitations

- For instance:
  - The GLBA imposes requirements on the collection of “nonpublic personal information” collected in connection with the individuals interactions with a financial institution for a personal, family, or household purpose

  - Maryland’s Personal Information Protection Act (PIPA), applies to disclosure of “personal information” defined as an individual's first and last name in combination with a:
    - Social Security Number
    - Driver's License Number
    - Financial Account Number (or)
    - Individual Taxpayer Identification Number



**unless the information is encrypted, redacted or otherwise rendered unusable*

What is PII?

PII: Graham Leach Bliley

Focuses on the protection of “nonpublic personal information”

Maryland’s Personal Information Protection Act

An individual's first and last name in combination with a:

- Social Security Number
- Driver's License Number
- Financial Account Number (or)
- Individual Taxpayer Identification Number

PII: Generally Accepted Definition

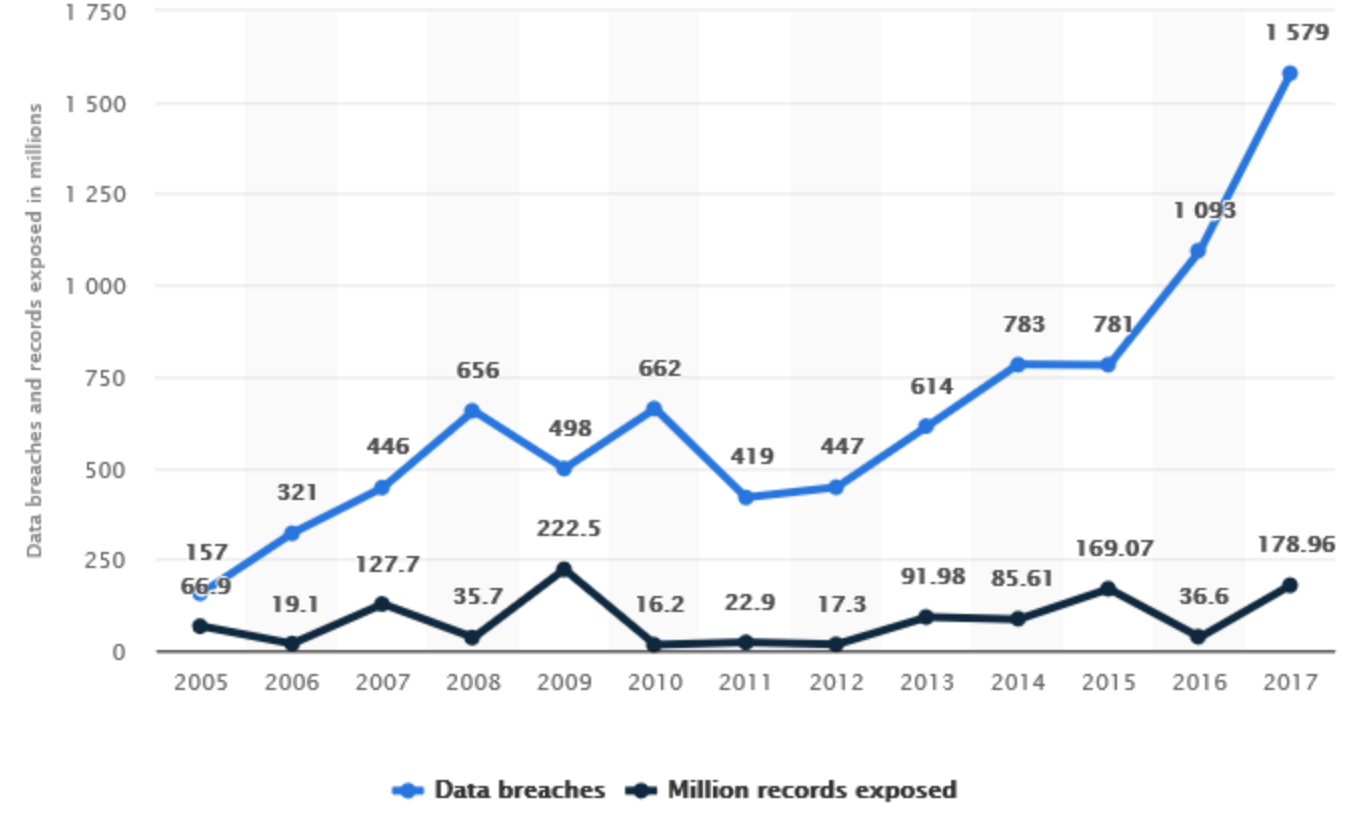
Any information about an individual maintained by an agency, including:

- Any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and,
- Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information

What is PII?

Data Element	PII?
Name	
Name and SSN	
Work email	
Personal email	
Name and bank account	
Name and work address	

Protecting PII: the Risks



- Recorded number of data breaches and records exposed in the United States between 2005 and 2017
- In the last measured year, the number of data breaches in the United States amounted to 1,579 with close to 179 million records exposed

**Source: Ponemon Institute 2017 Cost of Data Breach Study*

Protecting PII: the Risks

- Between 2016 and 2017, the average cost of a U.S. data breach rose from $6.69 million to $7.35 million dollars
- Root causes remain largely internal (52% of incidents)
- On average, a privacy related breach affects 28,512 U.S. consumers
- For financial services companies, the average cost per compromised record is $245 dollar (a 10% year over year increase)

**Source: Ponemon Institute 2017 Cost of Data Breach Study*

Mitigating the Risks

- It has become a cliché in cybersecurity circles, but it bears repeating—EVERY ORGANIZATION EVENTUALLY SUFFERS A SECURITY BREACH THAT EXPOSES PII

- But there are proactive numerous steps every organization can take to mitigate the threats discussed, and to minimize the impact of the inevitable breach, including:
  - Appropriate Encryption
  - Privacy by Design
  - Vendor Management
  - Incident Response Planning

Mitigating the Risks: Encryption

Appropriate Encryption

- Many of the statutes and regulations requiring notices of incidents involving the theft or loss of PII do not require affected parties to give notice where the information is encrypted
- This has lead to the generic advice: “encrypt everything with PII”
- This advice can be seen as glossing over certain technical, performance, and business impacts of universal encryption
- Encryption can solves many problems, but like everything in privacy, it requires appropriate balance that measures the risks faced by the data, against the impacts posed by encryption
- In essence, the key to deciding what data to encrypt is the risk profile and sensitivity of that data
- We call this “appropriate encryption”

This recommendation conforms to the FFIEC Information Security Booklet, Section II.C.19 on Encryption. The Booklet states: “Management should implement the type and level of encryption commensurate with the sensitivity of the information.”

Mitigating the Risks: Privacy by Design

- Privacy by Design is an approach to systems engineering which takes privacy into account throughout the whole engineering process
- In essence, it is less about data protection, and more about designing systems that use data in ways that do not need to be protected*
- The key is using these design principles to build an organization that takes privacy and data protective controls into account at every phase of the business process
- In it most common form, Privacy by Design has 7 principles:
    - Proactive not Reactive
    - Privacy as default setting
    - Embed Privacy by Design
    - Retain full functionality
    - End to end security
    - Visibility and Transparency
    - User-centric policies and procedures

**GDPR Article 25 and 42 now require privacy by design*

Mitigating the Risks: Vendor Management

- Third parties are increasingly relied upon to meet critical business needs
- This reliance has allowed data to move freely between entities that could have dramatically different privacy and data security standards
- Different standards create significant risks that can be difficult to manage
- This requires careful attention to a number of domains:
  - Contracts—these should include appropriate privacy provisions
  - Vendor selection—a vendor's privacy practices should be scrutinized during diligence (not after the fact)
  - Ongoing monitoring—a one and done approach does not suffice

A 2016 study by Deloitte found that 26.2% of respondents had suffered reputational harm because of a security incident at a supplier, with 20.6% reporting that a vendor or supplier suffered a breach involving personally identifiable or confidential information

Mitigating the Risks: Incident Response Planning

- Given the near inevitability of an incident occurring, it is important to proactively plan to respond to an incident involving PII
- Start with an incident response plan, but make sure it is not too prescriptive—each incident is unique and flexibility in approach is required
- Make sure the plan has clearly defined roles and communication cadences, and addresses the appropriate times to bring in outside lawyers and consultants
- Determine up front whether and to what extent you plan to work with law enforcement, and identify law enforcement contacts in advance
- Practice simulated incidents at multiple levels, including senior management

Mitigating the Risks: Incident Response Planning

PIPA Incident Response Requirements

- Once a security breach is detected, a business must conduct in good-faith a reasonable and prompt investigation to determine whether the information that has been compromised has been or is likely to be misused

- If the investigation shows that there is a reasonable chance that the data will be misused, that business must notify the affected consumers
  - Description of the information compromised
  - Contact information for the business
  - Toll-free numbers and addresses for each of the three credit reporting agencies: Equifax, Experian and TransUnion
  - Toll-free numbers, addresses and websites for the Federal Trade Commission (FTC) and the Office of the Attorney General (OAG)
  - A statement that the individual can obtain information from these sources about steps to avoid identity theft

Questions?

FEDERAL RESERVE BANK OF RICHMOND®

Richmond ▪ Baltimore ▪ Charlotte