metarouter

# Taking a Closer Look at the Data: PII

By Yetunde Abass

Compliance | Security

August 1, 2019

# Taking a Closer Look at the Data: PII

With every week there seems to be another story about a data breach or a company being held accountable for a previous one. States and jurisdictions are racing to put laws on the books to protect consumer privacy and/or mitigate damage of data exposure. But what data are these laws protecting?

In the case of consumers, regulated sensitive data is known as personally identifiable information (PII). PII includes information like social security or credit card numbers, but it is also comprised of less thought of facts about an individual. In this age of mass data collection, any bit of information about person could expose them if placed in the wrong hands.

With that in mind, we thought we'd take an in-depth look at PII broadly and in specific business and industry contexts.

# What is PII?

The Office of Management and Budget (OMB) defines personally identifiable information as “information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual.”

The European Union has a similar definition, adding that under the General Privacy Data Regulation (GDPR), “personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data.”

PII is often divided into two broad categories: Sensitive and non-sensitive information. Sensitive information refers to individual data that is not publicly available. This includes social security numbers and biometric records as listed above, in addition to data points like credit card or banking information, or a drivers license or passport number.

Non-sensitive PII is anything that can be discovered about a person through the use of publicly-available records. When multiple pieces of non-sensitive PII are combined, they can often identify a specific individual. Examples include:

- Date or birth
- Place of birth
- Address
- Home phone number (if listed in a directory)
- Business phone number

## Anonymous data

Most jurisdictions do not consider so-called anonymous data to be PII. The EU defines anonymous data as, “personal data that has been rendered

anonymous in such a way that the individual is not or no longer identifiable… For data to be truly anonymised, the anonymisation must be irreversible."

As data collection becomes more widespread and granular, it is questionable if the idea of truly anonymous data really exists. A 2015 study published in *Science* found that four points from credit card metadata were enough to identify 90 percent of individuals who had conducted a transaction. More recently, a group of researchers have developed an algorithm that they say can identify over 99 percent of Americans from almost any publicly available dataset using 15 attributes. They also published the source code and a demo online.

The lines between PII and anonymous data are blurring and companies would be wise to have secure policies in place for all types of sensitive information.

## PII Laws and Regulations

In the EU, data privacy and security falls under the umbrella of GDPR, which went into effect in May 2018. In the United States, however, there is a patchwork of federal and state laws, some of which only govern specific industries (more on those later). More broadly, the use of PII is regulated through the following laws:

- **Children's Online Privacy Protection Act (COPPA)** – The purpose of COPPA is to limit the amount of personal information that website operators can collect about children under the age of 13. The law requires companies to have clear privacy policies on their homepages and "verifiable parental consent" before collecting any information.
- **Computer Fraud and Abuse Act (CFAA) –** Although not written specifically to address data privacy, the CFAA is used for prosecutions related to hacking and cyber crimes. It has been a controversial law since its passage in 1986 namely because its concept of "unauthorized access" to a computer has never been clearly defined.
- **Privacy Act of 1974** – The Privacy Act governs how federal agencies are allowed to collect and distribute PII about private citizens. It also prohibits

the sharing of personal information of private individuals without their written consent except in specific circumstances.

- **Federal Information Security Modernization Act of 2014 (FISMA)** – FISMA is an update to the E-Government Act of 2002. It establishes a set of guidelines that federal agencies must meet to protect personal information and provide adequate digital government services.

Outside of COPPA, there is no federal law regulating data privacy for sectors outside of finance, healthcare, and education. This responsibility has fallen largely to the individual states, almost all of which have some sort of digital privacy law in place. They range from bans on employers accessing employee social media accounts to broad regulations like the California Consumer Privacy Act (CCPA) that allow consumers to opt out of most forms of digital data collection.

# Financial PII

Financial PII refers to an individual's credit, credit card, and banking information that is not publicly available. This includes:

- Credit card number
- Bank account number
- Customer/account ID
- CVV/CVC
- Chip or magnetic strip data
- Card PIN

## Federal Financial Privacy Regulations

In the US, the Federal Trade Commission (FTC) is charged with enforcing the following financial privacy related laws:

- **Gramm-Leach-Bliley Act (GLBA)** – The Financial Privacy Rule under GLBA requires financial institutions to disclose their data sharing practices to consumers prior to beginning a transactional relationship. Companies must also have measures in place to protect sensitive information.
- **Fair Credit Reporting Act (FCRA)** – The FCRA governs how consumer credit information is collected and used. Those who fall under the jurisdiction of the law include credit reporting agencies, organizations that collect consumer credit information, and organizations that use consumer credit information in their businesses. Consumers also have the right to view their credit files and dispute inaccuracies.

## PCI-DSS

The payment card industry has its own set of data security standards known as PCI-DSS. In order to work with card processors, merchants and financial institutions must agree to comply with 12 specific PCI-DSS requirements some of which include:

» Maintaining a secure network

» Maintaining an information security policy

» Developing a vulnerability management program

PCI-DSS is not mandated by federal law, but its stipulations are included in some state laws. In addition, merchants do not have to validate their compliance (in most situations), but if a merchant does have a security breach and was found to be non compliant, they may be subject to penalties and fines from the PCI Security Standards Council.

# Personal Health Information (PHI)

Under US law, personal health information (PHI) is any information about health care or health status that can be linked to an individual person.

Regulations for PHI are specified under the following two laws:

- **Health Insurance Portability and Accountability Act (HIPAA)** – HIPAA is a broad law that addresses issues related to health insurance coverage and costs. Title II of the law specifically addresses patient privacy and access of PHI. The HIPAA Privacy Rule and the HIPAA Security Rule establish a set of standards on how PHI is collected and transferred on paper or electronically that protects patient confidentiality while also allowing providers to serve patients effectively.
- **Health Information Technology for Economic and Clinical Health Act (HITECH)** – The HITECH Act was passed in 2009 in an effort to accelerate the adoption of electronic health records (EHR). Subtitle D of the law addresses privacy. The law establishes guidelines for the accounting of shared PHI, data breach notification, and imposes fines for health related data breaches.

# Education Privacy

On the surface, personal information related to education may not seem as sensitive as financial or health data. However, the amount of data collected by educational institutions on an individual starting from kindergarten through college, and possibly post-grad is immense. This includes information like grades, behavioral and developmental issues, and parental and personal income.

The Family Educational Rights and Privacy Act (FERPA) is a law enforced by the US Department of Education (ED). It applies to any school, public or

private, that receives funds from ED programs. The law gives students (or their parents, if under the age of 18) the right to review and dispute information recorded in educational records. Schools must also have written consent from the student or parent to release records to a third party.

FERPA was passed in 1974 when most educational records were on paper, meaning it would have been difficult to inadvertently share unauthorized information. Now with the emergence of more edtech platforms and services, it is easier than ever to unintentionally violate FERPA.

Cornell University has provided guidance to its instructors on FERPA and the use of digital technology in the classroom. The university notes that violations often stem from instructors uploading student information into unauthorized cloud services.

## Being a PII Steward

Companies will continue to collect more and more personal data. This is not necessarily a bad thing, as more information typically results in efficiency and better service. What's important is to keep in mind that personal data is valuable and should be protected. Keeping up with laws and regulations and having a real understanding of the different types of data is key.

data data regulation personal data pii

**Yetunde Abass** / About Author

› More posts by Yetunde Abass

## Related Posts

CCPA: What You Need to Know
30 May 2019

CCPA: Where We Go From Here
11 Jul 2019

CONTACT US

CAREERS

## Enterprise

ABOUT

PLATFORM

STATISTICS

GET STARTED

## Cloud

ABOUT

PRICING

SIGNUP

LOGIN