A Complete Guide for Businesses on Securing Personally Identifiable Information (PII)

GROUND LABS

The Index

1 What is Personally Identifiable Information?

Personally identifiable information (PII) is any data that can be used to identify a person, either on its own or when combined with other personal information.[1] Many types of data can be considered PII, and the kinds of data that constitute PII can vary from industry to industry, company to company, and individual to individual.

Some examples of PII include, but are not limited to [2]

- Names and Addresses
- Email addresses
- Telephone numbers
- Handwriting
- Driver's license numbers
- Social security numbers
- Tax identification numbers
- Passport numbers
- Military identification numbers
- Financial account numbers
- Credit card and debit card numbers if combined with any required security code, access code, or password that would allow someone access to your account
- Medical or health insurance information

2 Why PII Matters

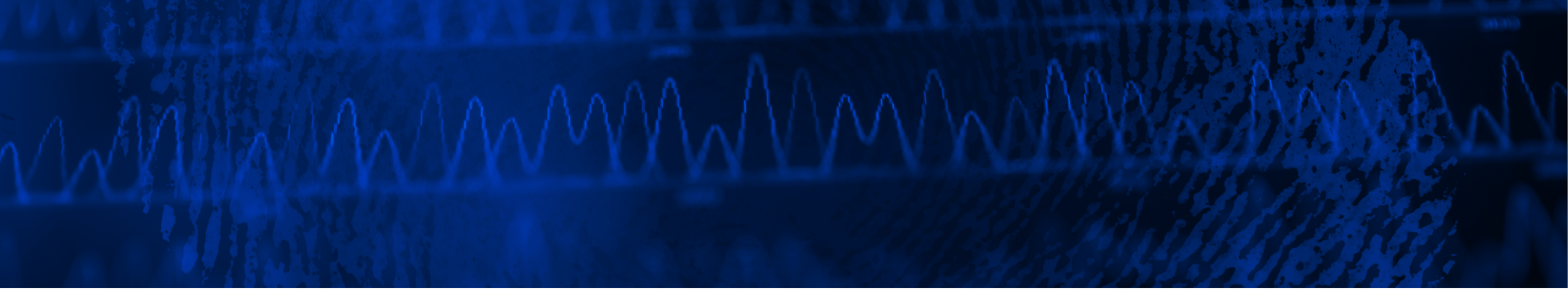
Companies can accumulate PII from many kinds of stakeholders, such as employees, customers, clients, patients, students, partners, and more, depending on the business and industry.[3] If an organization isn't aware of where it's storing PII, or isn't storing PII securely, it could be putting itself and its customers at significant risk.

Many types of bad actors might be motivated to steal PII, including hackers and internal disgruntled employees. Once an unauthorized party gains access to PII, there's a wide range of nefarious things they can do with it. This can include selling the data on the black market, making purchases with stolen credit card numbers, impersonating the individual to commit fraud, and filing stolen tax returns.[5]

Between 2018 and 2019

...there was a 17% increase in data breaches[4]

In January 2020, for example, hackers stole payment data from customers of the convenience store chain Wawa and sold millions of Wawa customers' credit and debit card numbers on the dark web.[6] Another example was the Capital One data breach in July 2019. In this incident, a former Amazon Web Services employee with insider knowledge of Capital One's data storage infrastructure stole personal data on more than 100 million Capital One customers.[7]



3 PII in Privacy Law

Many countries and regions around the world have regulations in place to protect PII. Even within a single country, there can be multiple laws. For example, the U.S. has many laws and regulations around PII data privacy, including the California Consumer Privacy Act (CCPA) and the Federal Trade Commission Act (FTCA). Most companies conduct business across multiple regions and countries, which makes compliance a complex endeavor. For example, a New York-based company doing business in Canada, California, Texas, and Michigan would have to ensure all organizational data privacy policies meet the security standards for regulations in all markets in both countries, not just in New York, where it is based.

Here's an overview of some of the privacy laws and guidelines that protect PII today:[8]

The United States:

- The FTCA
- The CCPA
- The National Institute of Standards and Technology's Guide to Protecting the Confidentiality of PII
- Health Insurance Portability and Accountability Act (HIPAA)

Europe:

- General Data Protection Regulation (GDPR)

Australia:

- Privacy Act

Canada:

- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Privacy Act

4 PI vs. PII

Personal information (PI) is a much broader category than PII, but all PII falls under the PI label. Generally, PI is information about an individual that, alone, cannot necessarily be used to identify the individual (for example, a person's birth date), while PII could, on its own, be used to identify the individual (a person's birth name).[9] However, multiple pieces of PI about the same individual could potentially be used to identify that person (for example, a person's birth date and zip code).

UNDERSTANDING PI AND PII:

Some forms of personal data can be used to identify an individual, while others cannot

PI: Birth date
02/02/1886

PI: Zip Code
15767

PI: City/State
Punxsutawney, PA

PII: First & Last Name
Punxsutawney Phil

PII: Address
Town Square,
Punxsutawney, PA

2 Pieces of PI (identifiable when combined) DOB & Zip
02/02/1886; 15767

Exact definitions of PI and PII can vary across countries and privacy regulations. For example, the CCPA created one of the most expansive definitions of PI: "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[10]

5 PII in GDPR and CCPA

PII is defined and treated differently within different privacy regulations, and it's important for businesses to understand and comply with all of the relevant laws and regulations that impact how they store and handle PII.

PII in CCPA

While CCPA has a broad definition of PI, its provision that allows consumers to file a lawsuit for a data breach applies to a narrower subset of PII. Specifically, CCPA regulations allow an individual to file a lawsuit against a company if his or her first name or first initial and last name are stolen in combination with one or more pieces of information from the list below, when the company failed to encrypt or redact either the name or the data elements:

Under CCPA, consumers can file a lawsuit against a company if their first and last name are stolen along with one or more of the following pieces of information in an unencrypted, unredacted format:[11]

- Social security number
- Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account

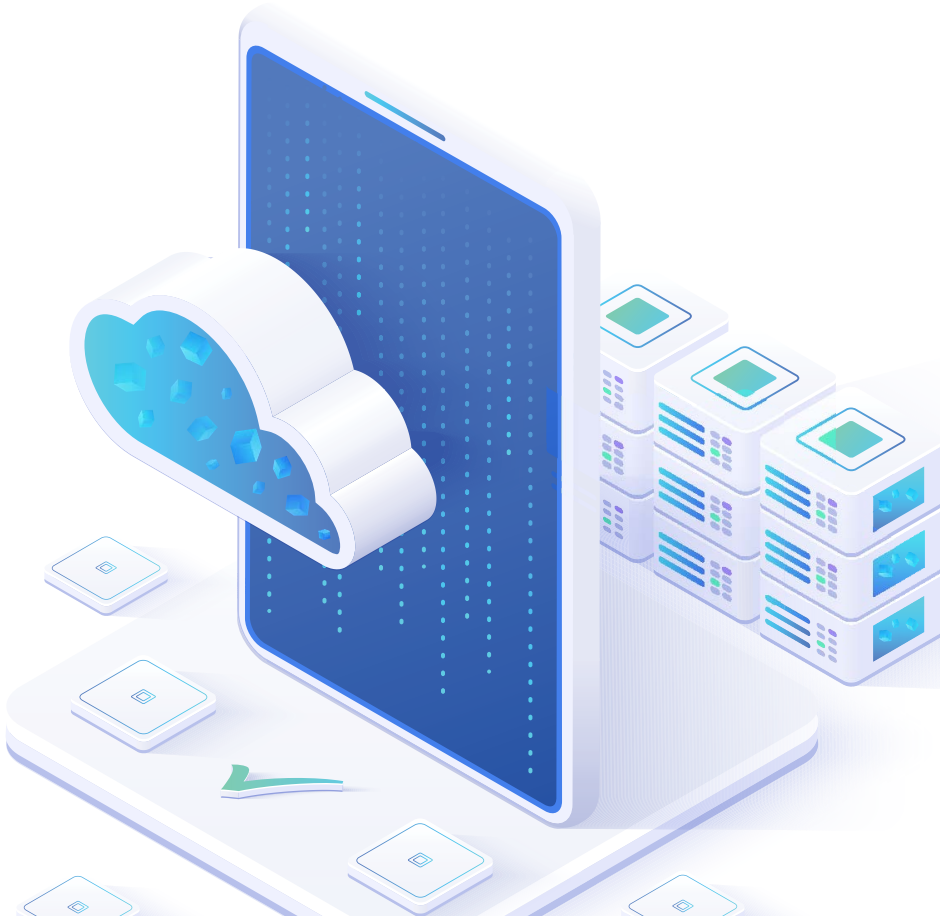
continued

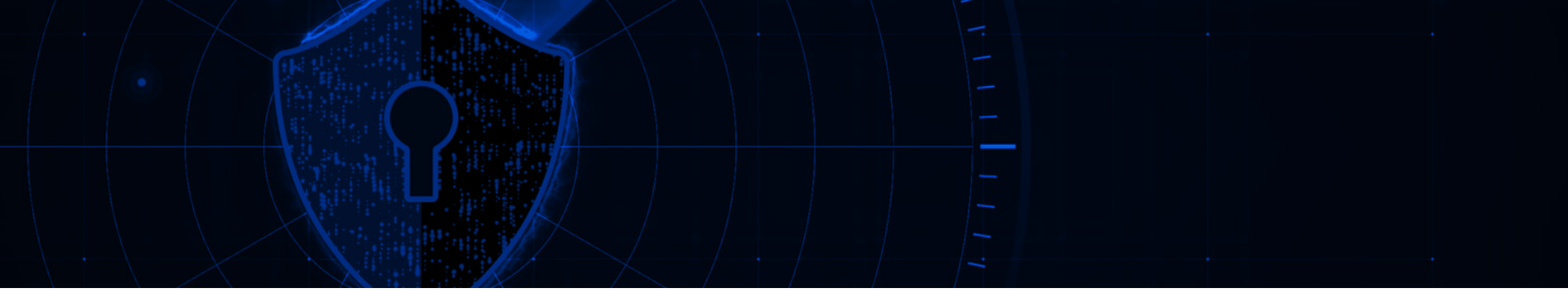
- Medical information
- Health insurance information
- Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual PII in GDPR

You can learn more about CCPA compliance here.

In contrast, GDPR defines personal data as any information relating to an identified or identifiable person. Under GDPR, an identifiable person is someone who can be identified, directly or indirectly, particularly by reference to personal data such as:[12]

- Names
- Identification numbers
- Location data
- Online identifiers
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person





6 An Overview of PII Scanning Tools

PII scanning tools are types of software that help organizations identify where PII is located and what it contains. These tools can also help to simplify compliance. Understanding where your organization's PII data resides is a critical component of maintaining compliance and avoiding breaches or data loss.

Ground Labs' Enterprise Recon simplifies the PII scanning process. Whether it's stored on your server, cloud, or your employees' devices, organizations can find and remediate personal data across a broad range of structured and unstructured data. Enterprise Recon makes it possible to locate and secure PII – credit cards, driver's licenses, passports, addresses, national IDs, and more – while complying with GDPR, CCPA, HIPAA, and other data security standards.

"Woodforest National Bank is committed to earning and maintaining customer loyalty and trust. A cornerstone of earning loyalty and trust is protecting customer personal data. Utilizing our partnership with Ground Labs enables us to go beyond our PCI DSS obligations and categorize all PII data across our organization. This ensures we know where personal and sensitive data resides across our infrastructure ecosystem, so we can maintain our commitments to our customers and meet our regulatory obligations." — **Marc Crudgington, MBA - CISO, SVP Information Security at Woodforest National Bank**

The benefits of Ground Labs' data discovery tools:

- **Personal and Sensitive Data Discovery:** All organizations should have an awareness of the personal and sensitive data they have stored in their enterprise. Customers trust organizations with a vast amount of data and it's important for businesses to maintain customers' trust and loyalty through confirmation that their personal information is being kept safely and securely.

- **Find Unencrypted PII:** Encryption is an important part of preventing criminals or unauthorized individuals from viewing personal and sensitive information on an organization's servers. With a PII discovery tool, organizations can quickly identify unencrypted data such as social security numbers, credit card information, health data, and more.

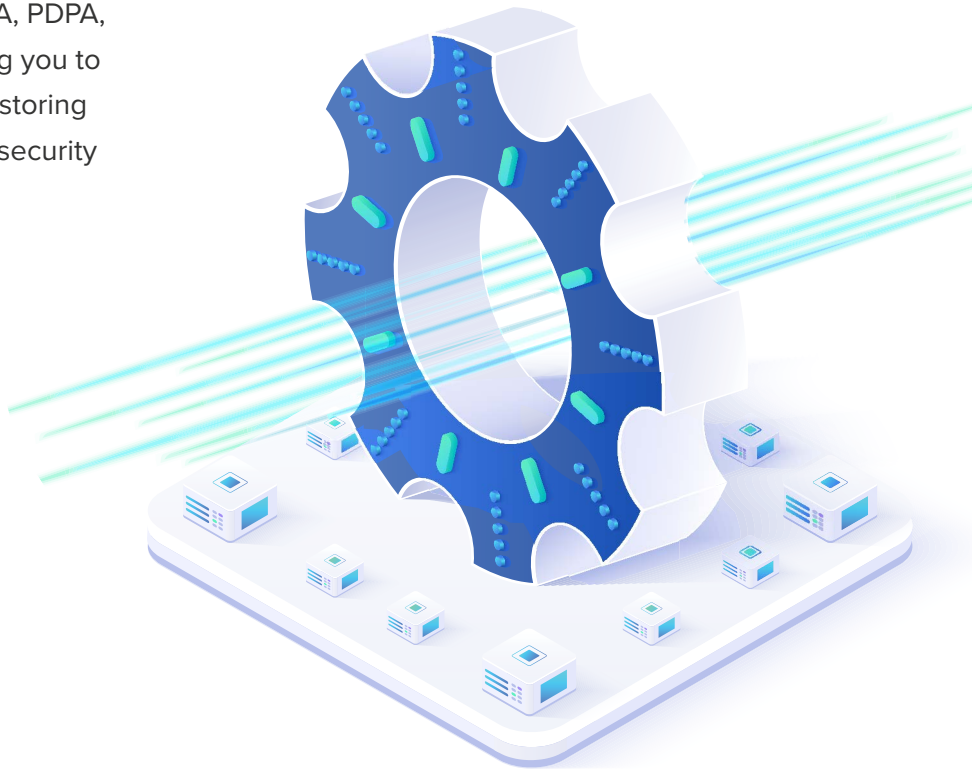
- **Maintain Compliance:** Scanning the enterprise for PII is the first step towards simplifying data discovery and working towards compliance for HIPAA, GPDR, and PCI requirements. Global and regional requirements are ever-changing, and a PII discovery tool ensures organizations avoid liability and risk. Global and regional requirements are constantly changing, and an effective PII discovery tool that supports automated scans will ensure organizations avoid liability and risk.

"Organizations today need to be aware of what data they handle, where they store it and what controls they have to protect it. Ground Labs develops products that fit this requirement. The tools are easy to use yet provide incredibly valuable information that can be acted on for further analysis or remedial efforts. The applications support most popular operating systems, databases and also a number of online applications." — **Murray Goldschmidt - COO at Sense of Security**

7 Conclusion

Any organization that handles personal or sensitive information should implement data scanning software to comply with GDPR, CCPA, HIPAA, PDPA, Australian Privacy, PIPEDA, and other data security standards requiring you to locate and secure PII. Knowing what kind of data your organization is storing and where it resides will help you comply with local and international security regulations and maintain trust with customers.

You can learn more about Enterprise Recon here.



End Notes

1. “Rules and Policies - Protecting PII - Privacy Act,” U.S. General Services Administration, January 12, 2020, https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act.

2. “Guide to Identifying Personally Identifiable Information (PII),” University of Pittsburg, https://www.technology.pitt.edu/help-desk/how-to-documents/guide-identifying-personally-identifiable-information-pii.

3. “Personally Identifiable Information: What Companies Need to Know,” Reger, Rizzo, Darnall LLP, Attorneys at Law, March 29, 2017, https://www.regerlaw.com/personally-identifiable-information-what-companies-need-to-know.html.

4. “Identity theft resource center®’s annual end-of-year data breach report reveals 17 percent increase in breaches over 2018,” Identity Theft Resource Center, January 28, 2020, https://www.idtheftcenter.org/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/.

5. Steve Zurier, “8 Ways Hackers Monetize Stolen Data,” Dark Reading, April 17, 2018, https://www.darkreading.com/attacks-breaches/8-ways-hackers-monetize-stolen-data----------/d/d-id/1331560?image_number=1.

6. Jeff John Roberts, “Wawa breach: A hacker is selling 30 million stolen credit cards on the dark web, cyber experts say,” Fortune, January 28, 2020, https://fortune.com/2020/01/28/wawa-data-breach-credit-card/.

7. James Rundle and Catherine Stupp, “Capital One Breach Highlights Dangers of Insider Threats,” The Wall Street Journal, July 31, 2019, https://www.wsj.com/articles/capital-one-breach-highlights-dangers-of-insider-threats-11564565402.

8. “Personally Identifiable Information (PII),” Imperva, https://www.imperva.com/learn/data-security/personally-identifiable-information-pii/.

9. Malia Thuret-Benoist, “What is the difference between personally identifiable information (PII) and personal data?,” Tech GDPR, June 27, 2019, https://techgdpr.com/blog/difference-between-pii-and-personal-data/.

10. Joseph J. Lazzarotti, “Personal Information, Private Information, Personally Identifiable Information...What’s the Difference?,” December 30, 2019, https://www.natlawreview.com/article/personal-information-private-information-personally-identifiable-information-what-s.

11. “Civil Code: Obligations Arising from Particular Transactions,” California Legislative Information, 2019, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.81.5.

12. “Regulation of the European Parliament and the Council...General Data Protection Regulation,” Official Journal of the European Union, April 27, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1374-1-1.