Privacy & Security in a World that Collects Our Data: Financial Data

Esteban Lopez

School of Information, San Jose State University

INFM 203: Big Data Analytics & Management

Dr. Glen Mules

May 6, 2022

Abstract

In exploring the definition of personal data, this research looks at how to define that, especially in the context of big data. The first part looks at generic definitions of personal financial data. Then the federal organizations like General Accountability Office and National Institute of Standards and Technology are reviewed to see how they define personal data, which ultimately is not different from general personally identifiable information. From there laws and concepts from Fair Information Practices, Gramm-Leach-Bliley Act, and the General Data Protection Regulation are considered. Finally big data ethics from the responsibility of government and companies to the individual responsibilities are reviewed.

Keywords: Ethics, Big Data, Digital Citizenship, GLBA, GDPR, Fair Information Practices, PII, PIFI, Personal Financial Data

Privacy & Security in a World that Collects Our Data: Financial Data

A survey of exploring and defining personal financial data will show that there is not much difference between personally identifiable information (PII) and personal financial data. Looking at organizations and laws will help to clarify the differences and similarities. Finally, a look will be made at the ethics of big data and who is responsible. We will see that companies and governments are responsible, but they have a responsibility of educating the general public. While all financial data is basically the same as PII, there is the fact that PII is worth money. Google as Alphabet and Facebook as Meta are basically free to use but made 100's of billions of dollars off selling targeted ads (O'Sullivan, 2022). While it is difficult to pinpoint how much personal data is worth there are estimates that range widely between $26 and thousands of dollars per person (O'Sullivan, 2022). This is a subject worth exploring.

A Survey, or Challenge, of Defining Personal Financial Data

A challenge is to define and list what constitutes personal financial data. An infographic produced by Enterprivacy Consulting Group lists many categories of personal information; Under their personal financial information category, the four sub-categories are account, ownership, transactional, and credit (Cronk, 2017). Besides the financial category, the infographic lists historical, internal, external, social, and tracking as top-level categories and states that, "Categories are not exclusive. Information may transcend multiple categories" (Cronk, 2017). There is no real clear line between personal financial information and general personal information.

One important and widely used concept is that of personally identifiable information (PII). This can be used as a starting point for the attempt to pin down what personal financial data is exactly. One tactic can be to compare types of PII for some sort of distinction. Investopedia lays out 2 categories of PII and says it, "can be sensitive or non-sensitive"

(Frankenfield, 2022). Sensitive PII are information like full name, social security, medical records, driver's license and financial information, but non-sensitive PII are information that can be considered anonymized like zip code, race, and gender (Frankenfield, 2022). However non-sensitive PII, "when used with other personal linkable information, can reveal the identity of an individual" (Frankenfield, 2022).

Knowing that many types of PII can be pieced together to figure out who it belongs to along with the fact that many different categories of personal information exist and can implicitly be linked to personal financial information makes the task of defining which pieces of information or data make up personal financial information difficult. One interesting concept is called personally identifiable financial information (PIFI). PIFI is defined as "any information that a consumer provides to a financial institution that would not be available publicly" (Techopedia, n.d.). If PII and PIFI are essentially the same, why do these two terms and acronyms exist? They look like they exist in the legal world, so maybe defining personal data requires looking into legislation surrounding personal information.

Laws and Organizations About Personal Data

There are many organizations and laws that attempt to define personal data. The Government Accountability Office (2008) in a report to lawmakers defines PII as:

> Any information about an individual maintained by an agency, including (1) 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 (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (p. 1).

In the Unites States that is one definition provided to Federal lawmakers in congress. The Government Accountability Office (GAO) produces reports for congressional lawmakers. In contrast, the National Institute of Technology and Standards (NIST) advises federal agencies and develops standards "with which federal agencies must comply – federal agencies may not waive the use of the standards" (Lord, 2020). NIST uses the GAO's definition of PII in Special Publication 800-122 (McCallister et. al., 2010). It is a serious definition in use by the federal agencies. "The NIST 800 series is a technical standard set of publications that details U.S. government procedures, policies, and guidelines on information systems" (Lindberg, 2021). Not only must federal agencies comply, "contractor companies tied to federal agencies via obligatory contracts must comply with the standards laid out by references linked to the NIST 800" (Lindberg, 2021).

Fair Information Practices

The NIST links PII with Fair Information Practices in Special Publication 800-122: "The Privacy Act, as well as other U.S. privacy laws, is based on the widely-recognized Fair Information Practices, also called Privacy Principles" (McCallister et. al., 2010, Sec. 2.3). The reason Fair Information Practices are important as a foundation is that "Fair Information Practices, also known as Privacy Principles, are the framework for most modern privacy laws around the world" (McCallister et. al., 2010, Sec. D-1). There are different laws that pertain to different types of PII, or different sectors.

Sector and Jurisdiction Based Laws

Because different sorts of businesses need different guidance based on their field it can get quite complicated. The NIST gives examples that "the Health Insurance Portability and Accountability Act of 1996 (HIPAA) applies to the health care sector, and the Gramm-Leach-

Bliley Act of 1999 (GLBA) applies to the financial services sector" (McCallister et. al., 2010, Sec. B-2). Companies also must consider not only federal laws, but also state laws and international laws. Basically companies "are responsible for determining which laws apply to them based on sector and jurisdiction" (McCallister et. al., 2010, Sec. B-2).

Gramm-Leach-Bliley Act (GLBA)

In looking laws that focus on financial data, the GLBA is singled out by the NIST. The GBLA has 2 requirements, "It imposes these obligations under two 'Rules': (i) the Privacy Rule, and (ii) the Safeguards Rule" (Oberheiden, 2022). "Nonpublic Personal Information, or NPI, is a type of sensitive information created and defined by the Gramm-Leach Bliley Act (GBLA)" (Steele, 2021). NPI sensitive information has much of the same information protected by PII in general and protected health information (PHI) regulated by HIPAA. The information is that is in all these categories are name, address, social security number, etc. Even though there are categories for financial information, the protected information greatly overlaps.

Sometimes it takes court cases to clarify definitions. Financial information is legally broad. The Federal Trade Commission (2002) reported that:

> The Court concluded that the Commission has the authority to define PIFI under its "broad rulemaking authority." The Court rejected Trans Union's argument that credit header information, such as name, address, telephone and social security numbers, is not "financial" information and does not fall within the definition of "personally identifiable financial information," because any information requested by a financial institution in order to provide a financial service "can be fairly characterized" as financial information.

In terms of defining personal financial data, really that is enmeshed with PII in general. So, it really might be worth looking at different laws. There are many specific financial laws, those

should not be ignored. As demonstrated so far, an exact line differentiating personal financial data, from personal health data to general personal data doesn't really exist.

General Data Protection Regulation (GDPR)

Data laws are being developed by many states, countries, and regions like the European Union (EU). "[T]he General Data Protection Regulation (GDPR) is considered the gold standard when it comes to data protection laws" (Baig, 2022). This law basically crosses many borders, and not just in Europe. There are even agreements amongst different regions and nations. For example, Japan has an agreement with the EU for both the GDPR and Japan's Act on Protection of Personal Information where "organizations based in the EU and subject to the GDPR can face legal action in the EU and Japan if the privacy violation occurs in Japan while being based in the EU – and vice versa" (Baig, 2022). This highlights that it is important to consider all PII regardless of sector or jurisdiction.

The Ethics of Working with Big Data

People don't like breaches or sneaky things done with their personal data. While it is probably not the case for everyone some people do enjoy the results of algorithms tailored to them. "Many people are even delighted by the idea that proper data analytics can uncover hidden desires and motivations" (Ofori-Boateng, 2020). That is certainly not a universal sentiment, but if the population understands what is going on there might not be a huge backlash. One ethical framework for big data provided by Forbes (Ofori-Boateng, 2020) is as follows:

Six Methods That Incorporate Data Ethics In Your Business

1. Inform and consent . . .
2. Privacy and protection . . .
3. Two-way transparency . . .

4. Respect the rules . . .
5. Privacy by design . . .
6. Algorithm evaluation and auditing

That is a business perspective. Businesses need to recognize the ethics of big data not only for legal compliance but also for goodwill of their customers.

In terms of financial ethics and big data, the Institute of International Finance released the *IFF Data Ethics Charter* (Bailey et. al., 2021). The document (Bailey et. al., 2021) lists a few areas to focus on: "Responsible data management cycle; data control; challenges around algorithmic decision-making systems; partnerships and third parties; and skills, awareness, and knowledge sharing" (p. 4). They both highlight a few of the same things, but the most interesting aspect is the idea of consumers providing consent with transparency and knowing how to understand and control their own data.

While the big data responsibilities are asymmetric with companies and governments having the larger share of responsibility, it is important for individuals to understand their part in the system. The concept of digital citizenship is important not only for consumers but also for companies and their employees. During the COVID-19 pandemic and resulting shutdowns almost everyone was dependent on the internet (if they were fortunate enough to have it). Elementary schools and some jobs were conducted via Zoom. Even though digital citizenship is geared towards K-12 school students it or some variation should be taught at almost any job. So two of the many concepts of digital citizenship are "Understanding user data" and "Securing Digital Devices" (Zook, 2019). There is an ethical obligation by everyone to have a baseline understanding of personal data and privacy, not only of their own information but of others. Digital citizenship should be taught as a basic subject in schools and work.

Conclusion

In trying to categorize personal financial data there is no authoritative or colloquial definition by any organization that is the signpost. The main issue is that personal financial data cannot really be extricated from PII or PHI or any other personal identifiers. Regulations and laws are aimed at sectors and jurisdictions, but many laws cross borders and sectors. There are legal obligations companies and individuals must follow, but there are also ethical reasons for businesses and individuals to understand big data and personal data.

References

Baig, A. (2022, April 29). *10 Strictest Data Privacy Laws By Country in 2022.* Techopedia. Retrieved on May 5, 2022, from https://www.techopedia.com/10-data-privacy-laws-every-business-should-know/2/34759.

Bailey, N., Ferenzy, D. & Carr, B. (2021, June). *IIF Data Ethics Charter.* [pdf]. Institute of International Finance. Retrieved on May 6, 2022, from https://www.iif.com/Portals/0/Files/content/Innovation/06_07_2021_iif_data_ethics_charter.pdf.

Cronk, R. J. (2017, March 1). *Categories of Personal Information.* Enterprivacy Consulting Group. https://enterprivacy.com/2017/03/01/categories-of-personal-information/.

Federal Trade Commission. (2002, July 29). *Appeals Court Upholds Financial Privacy Regulations: Trans Union May Not Sell Consumers' Personally Identifiable Information without their Consent.* Retrieved on May 6, 2022, from https://www.ftc.gov/news-events/news/press-releases/2002/07/appeals-court-upholds-financial-privacy-regulations.

Frankenfield, J. (2022, February 25). *Personally Identifiable Information (PII).* Investopedia. Retrieved on May 5, 2022, from https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp.

Government Accountability Office. (2008, May). *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information.* (Publication No. GAO-08-536) [PDF]. Report to Congressional Requesters. United States Government Accountability Office. Retrieved on May 6, 2022, from https://www.gao.gov/assets/gao-08-536.pdf.

Lindberg, R. (2021, January 27). *NIST Special Publication (SP) 800 Series.* Rivial Data Security. Retrieved on May 6, 2022, from https://www.rivialsecurity.com/blog/nist-800.

Lord, N. (2020, December 1). *What is NIST Compliance?* Digital Guardian. Retrieved on May 6, 2022, from https://digitalguardian.com/blog/what-nist-compliance.

McCallister, E., Grance, T. & Scarfone, K. (2010, April). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). (Special Publication No. 800-122) [PDF]. National Institute of Standards and Technology, Computer Security Division. Retrieved on May 6, 2022, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

Oberheiden, N. (2022, May 6). *Gramm Leach Bliley Act: 2 requirements & 7 Ways to Achieve Compliance.* The National Law Review. Retrieved on May 6, 2022, from https://www.natlawreview.com/article/gramm-leach-bliley-act-2-requirements-7-ways-to-achieve-compliance.

Ofori-Boateng, C. (2020, June 8). *Your Big Data Responsibility: The Rise in Data Ethics.* Forbes. Retrieved on May 6, 2022, https://www.forbes.com/sites/forbestechcouncil/2020/06/08/your-big-data-responsibility-the-rise-in-data-ethics/.

O'Sullivan, F. (2022, April 25). *How Much Is Your Data Worth to Advertisers?* How To Geek. Retrieved on May 6, 2022, from https://www.howtogeek.com/792013/how-much-is-your-data-worth/.

Steele, K. (2021, November 3). *A Guide to Types of Sensitive Information.* BigID. Retrieved on May 6, 2022, from https://bigid.com/blog/sensitive-information-guide/.

Techopedia. (n.d.). *Personally Identifiable Financial Information (PIFI).* Retrieved on May 5, 2022, from https://www.techopedia.com/definition/14222/personally-identifiable-financial-information-pifi.

Zook, C. (2019, December 10). *What is Digital Citizenship & How Do You Teach It?* Applied Educational Systems. Retrieved on May 6, 2022, from https://www.aeseducation.com/blog/what-is-digital-citizenship.