Digital Information Privacy and the Art of P.I.I

[redacted]

[redacted]

[redacted] Laws & Ethics of Computer Security

[redacted]

31 March 2024

Digital Information Privacy and the Art of P.I.I

Digital information privacy is extremely relevant to today's society as we live in a world and a country where technology is used heavily to complete day-to-day tasks in home, small businesses, and large corporations. Legal frameworks including data protection and computer crime laws oversee the digital information collection and storage as well as sharing. Ethical considerations are put in place to guide responsible practices such as equal privacy rights digitally for all. There are also security measures that are very important and probably the most important part such as encryption and access control, meaning who gets access to what, and it is also to protect digital assets from access that is not allowed and digital threats.

What is P.I.I?

Personal identifiable information (for short, P.I.I) is information about a person or business that is stored somewhere for financial or security purposes. Such items include name, address, date of birth, Social Security number, phone number, e-mail, physical address, mailing address, anything that can be physically tied to your name in your information. There are certain laws put into place that prevent this information from being leaked or exposed online, which is unfortunately not something that most people are aware of but as our growing planet is starting to revolve around technology, we need to be more involved with this information. Most people are unaware of why compliance is so important, risks of exposure and mitigation techniques, and the 4th amendment see sure and search and how it connects to it, and most of all the importance.

Compliance with P.I.I

Compliance with personal identifiable information is extremely important today because it houses people's personal information that can tie back to them financially or physically. If in the wrong hands, then it can lead to disastrous effects such as identity theft, credit card fraud, check fraud, and millions of dollars in lawsuits from one person to a multi-million-dollar company. For example, many industry-based data privacy standards in the United States include PCI (Payment Card Industry), or DSS (Diplomatic Security Service) for payment information, and HIPAA (Health Insurance Portability and Accountability Act of 1996) for health information and medical records. The health insurance portability and accountability act is a federal law that requires the creation of standards to protect sensitive patient information from being released without the patient's consent. *(CDC, Unknown)*. There are also other privacy mandates across the world, for example in the European Union, GDPR, or the General Data Protection Regulation mandates specific purpose for personal information use, and it grants data subjects rights to access and correct personal information comma and restricts data transfer outside the European union. (European Council, unknown). Many people don't know this but the term cookies was born from this GDPR, because it tells you that your information is stored and may be used for other purposes, which is why you can either allow all of them, deny all of them, or manage what is given away. That's why when someone goes on a certain website, they must either accept or decline cookies. Implementing policies to stay compliant involves complex processes, including data assessment, security assessments, and ongoing monitoring. Automated tools can streamline these tasks, helping businesses and people personally efficiently manage compliance requirements and mitigate data breaches, which will be explained more in detail in the next section.

Exposures & Risk Mitigation of P.I.I

Believe it or not, exposures and data breaches are more common than most people would think. Even with some of the tightest security known to man, anything is possible. Major corporations or small ones face challenges in protecting your PII due to complications introduced by cloud storage and remote work arrangements. Ever since the coronavirus pandemic in 2020, a shocking 29% have reported a significant increase in identity theft risk. 43% expect an increase even bigger over the next year or two *(Petrosyan, 2020*). Security policies are very important when mitigating risk of exposure, beginning with creating a comprehensive security strategy and policy covering every aspect of cybersecurity and of data information. Identifying and assessing security threats across the globe determine their impact should it target your information. Creating what are called “honeypots” or “sandboxes” to attract these viruses and exposures for a better understanding of how they work and what they could take. Employee awareness is one of the other most important aspects of this, because as a cyber specialist, they may know what the risks are but the naked eye and employee or regular Joe Schmuck would not know these risks. Educate employees about security risks, and how to protect their information at work and at home. Explain potential risks and show demonstrations of what could be stolen or put on the Internet and explain the consequences of what could happen so that employees could be more vigilant when it comes to securing information. Lastly, granting access to authorized people or persons is just as equally important as the other two. People would say that it is the most important one because it can make a difference between who can be trusted and who cannot be. A lot of companies like to use DLP, or data loss prevention software to track and control access to PII. And who logs in at a certain time and takes exactly what. *(Cocoara, 2020**)***

4th Amendment of the US Constitution and its relation.

The 4th amendment of the United states constitution, which is also the first ten amendments also known as the Bill of Rights, states “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrant shall issue, but upon probable cause, supported by oath or affirmation comma and particularly describing the place to be searched” *(US Courts)*. The 4th Amendment is Not for Sale Act, or FAINSA, sponsored by Senator Ron Wyden, aims to close legal wormholes allowing government agencies to obtain personal and consumer data from brokers and sellers without oversight from a court of some kind. Agencies like the FBI, DoD, ICE, IRS, and DHS in recent years have been obtaining personal information such as location data, search history, and phone and message communications from data brokers without proper warrants, as shown in the leak from NSA committed by Edward Snowden *(Macaskill & Dance, 2013)*. Before the amendment was intentionally designed originally to protect against physical surges and seizures, but since it's birth in 1787, it is evolved to include a broader right to privacy, as well as adapting to advancements in technology. The stored Communications Act, or SCA limits the government's ability to force or manipulate Internet service providers to disclose customer data, but unfortunately it does not extend to data brokers and sellers. Another great case that highlights the importance of data privacy is the Crispin v. Christian Audigier, Inc. Case, in which a dispute over the disclosure of private data on Facebook was involved. Christian Audigier wanted access to a Facebook users personal information, and private messages, comments, and timeline postings for litigation reasons. In Crispin, the court ruled in favor of protecting the user's privacy under the stored Communications Act, and the court held that the subpoena issued a Facebook for the users personal information did not meet these standards set forth in the SCA. The ruling itself, along with the other cases and the Fourth Amendment to the US Constitution emphasized the importance of statutory

privacy protections in safeguarding and protecting individuals' electronic communications from unreasonable and unlawful search seizure from the Government.

Conclusion

The true significance and importance of digital information privacy and the art of personal identifiable information, or PII, cannot be overstated in our technology driven society. Legal frameworks and ethical considerations help guide responsible practices, such as proper training, and employee awareness, and laws and regulations such as GDPR, and HIPAA dictate strict rules and regulations for the collection comma storage comma and distribution of PII. Compliance with these standards is vital for preventing disastrous lawsuits and shutdowns of major corporations because of simple identity theft and fraud. Despite security measures, data breaches and exposures are inevitable, especially with the rise of remote working and cloud-based storage from the COVID-19 pandemic, mitigation risks involve comprehensive security, employee education, and controlled access. The 4th amendment to the US constitution which is also on the Bill of Rights guarantees protection against unreasonable search and seizure, which in recent years has also been extended to digital privacy rights. Recent efforts like the faints act aimed to address wormholes allowing government agencies to access personal information without proper court oversight or a warrant.

The AI document attached to this report not only lacks depth and real-life context compared to this document, it briefly covers digital privacy and PII but doesn't dive into specific cases or ethical applications. The original report provides complex examples of how privacy breaches impact individuals and small businesses, and how the government in the past has used technology illegally to obtain personal information. Overall, the longer an original document offer a more comprehensive understanding of Digital Information Privacy and the Art of P.I.I

References

Cooper, Stephen. What is PII Compliance. Comparitech. https://www.comparitech.com/net-admin/what-is-pii-compliance/

Centers for Disease Control and Prevention. Health Insurance Portability and Accountability Act of 1996. https://www.cdc.gov/phlp/publications/topic/hipaa.html

European Council. The General Data Protection Regulation. https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/

Petrosyan, Ani (2020). Global increase in identity theft risk since the coronavirus outbreak as of August 2020. Statista. https://www.statista.com/statistics/1175657/increase-identity-theft-coronavirus-outbreak/

Cocoara, Zoran. 5 Best Practices for Minimizing the Risk of PII Breaches in any organization. Endpoint Protector Blog https://www.endpointprotector.com/blog/5-best-practices-for-minimizing-the-risk-of-pii-breaches-in-any-organization/

Administrative Office of the U.S. Courts. What does the Fourth Amendment Mean? Retrieved from https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0

Macaskill, Ewan., & Dance, Gabriel. (1 November 2013). NSA Files: Decoded - What the revelations mean for you. The Guardian. Retrieved from https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Gu, Katie. (29 September 2022). The Fourth Amendment and the Post-Roe Future of Privacy. Petrie-Flom Center Blog. Retrieved from https://blog.petrieflom.law.harvard.edu/2022/09/29/the-fourth-amendment-and-the-post-roe-future-of-privacy/