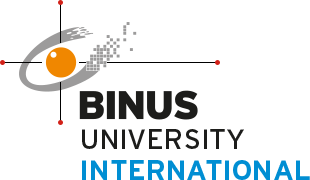
**Internet Privacy**



**Lecturer :**

Ir. Tri Asih Budiono, M.I.T.

**Created By :**

Edward Alvin 2501963141

Ferdinand Jacques 2501982600

Benedictus Filbert Federico 2502005263

Andrew Tjandra 2502069935

Github Repo Link: <https://github.com/fl-sll/PDM_InternetPrivacy>

**PROGRAM DESIGN METHOD**

**MAJOR OF COMPUTER SCIENCE**

**BINA NUSANTARA INTERNATIONAL UNIVERSITY**

**JAKARTA**

**2021**

### **Background**

A major ethical issue in the collection and management of consumer information is the privacy of that information (Bloom, Milne, and Adler 1994; Chonko 1995; Foxman and Kilcoyne 1993; Jones 1991). Internet Privacy also known as online privacy refers to the vast range of technologies, protocols and concepts related to giving individual users or other parties more privacy protections in their use of the global internet. Internet Privacy takes many forms, including mandatory privacy statements on websites, data sharing controls, data transparency initiatives and more. Internet Privacy and anonymity are paramount to users, especially as e-commerce continues to gain traction. Privacy violations and threat risks are standard considerations for any website under development.

One of the biggest things that people talk about when they discuss Internet privacy is the regulation of handling user data. A most commonly cited example is the General Data Protection Rule or GDPR, which is a European standard recently adopted to protect the data of European citizens. Apparently, the act governs data belonging to EU citizens, but the way that the regulation plays out affects many companies in other parts of the world. A multinational company utilizing the global internet (or just a company with international reach) may have any number of European users as members, subscribers or customers. This requires the company to keep GDPR compliance for the corresponding data set. In addition, other countries, states and provinces have come up with their own data privacy laws. Many of these are very much in the nature of trying to close barn doors already opened by a lack of universal internet regulation from the infancy of the World Wide Web itself.

Many kinds of internet privacy technologies and security implementations rely on biometrics as a key method of user authentication. The general idea is that if data is biometrically protected, only the individual with said biometric data has access to it. Early biometric designs included thumbprint and retina scan devices but many of these were not very feasible due to hardware requirements and integrations needed. Now, the promise of voice-based authentication adds a key functionality to internet privacy technology. Many types of data sets can be stored behind a voice-based authentication system, ensuring that only the individual with access will be able to view them.

The way that we use the internet related to our internet privacy is changing rapidly. Now, major technology companies have put in place stricter compliance protocols to increase individual user privacy. At the same time, many privacy advocates are calling for more transparency in how third-party data is used, whether that’s entirely demographic or involving data sets with personal identifiers. At the same time, others are also suggesting that individuals should own data and be paid to sell that data to third parties, which could also add needed transparency to the process. The use of blockchain has been explored as a means of building this new type of privacy compliance. In general, having data sets on a blockchain allows for a more diverse set of capabilities related to manipulating and evaluating that data or keeping track of who has access or where the data is stored. The conversation around internet privacy continues to evolve. New types of professionals and analysts are adopting new concepts and strategies for handling internet privacy as the internet matures and cloud services port ever more sophisticated data sets through global internet trajectories.

### **Problem**

Internet Privacy issue is an important topic on the internet. Much of the discussion is characterized by hype and preys on fear. This is obvious from looking at the wide range of “spyware protection” products available on the internet and the language used to promote these products. Without knowing the realities of how their surfing patterns are tracked and what they do with that information.

At the moment, technology is changing rapidly, so it is difficult for rules and procedures to be established and enforced as change is the only thing that is constant. Perhaps the greatest cause for concern is the unknown. Surfers do not know when and if they are being tracked, who collects that information, how it is done and for what purposes. Most internet users or surfers are least bothered about their online privacy and are unaware of the possible risks associated with it. Not only is their privacy endangered, but their safety too, especially when they are using the internet to carry out important and secretive tasks like online banking and sharing crucial business files.

Online users are incredibly vulnerable to security threats and there is a long list of issues associated with their safety. When we are online, we are spied on by a number of trackers for various purposes. Trackers keep a record of our search history and track all of our online activities through various means. This provides them with a clear picture of who we are and our interests, which is a breach of internet privacy policy and makes us a public property. Most of the time, this tracking is for advertisement purposes only and it allows advertisers to show ads according to our tastes and interests. But sometimes, this information is used by cybercriminals to carry out unauthorized and illegal activities risking our online existence.

There are various sites on the internet that need our personal information to get access to their services. These sites often store cookies and save your personal information and later use it for various purposes. Most of the time, this information is not encrypted and can be accessed by anyone. This mishandling of personal information may lead to serious consequences. The modern trend of e-banking portals have multiplied the risks associated with our internet privacy. By sharing our bank details and crucial files on the internet, we are paving ways for cyber burglars and making ourselves vulnerable to cybercriminals.

Most internet users proudly upload their social media posts highlighting their current location along with tagging friends and family members. It’s fun and exciting to share your life events with friends and family, but this data does not remain restricted to our expected audience only. This same data is stored on the social media site we are using and stays there forever, often without us knowing (though we might have been given our consent through a terms and services agreement). Along with social media apps, Google Maps and other apps also ask for our location and by turning on our location, we are providing first-hand information to the world about where exactly we are and what our next move is which is certainly risky and insecure.

With the internet being around for quite some time already, identity theft is nothing new. New and better technology has allowed hackers and online criminals to find new ways to commit these crimes. Online identity theft is when someone steals your identity by gaining access to your personally identifiable information to commit fraud. These malicious hackers could steal personal information such as your Social Security number, bank account number or your passwords. When we share personal info online, that information might risk falling onto the wrong hands. These perpetrators use different methods to commit identity theft. Such methods are: phishing, pharming, malicious software and unsecured websites. Phishing occurs when cybercriminals send emails purporting to be from a financial institution or other trusted organization, trying to trick you into opening attachments or clicking on links and providing your PII. Ignore unsolicited emails and online requests for information. If you want to visit, say, your bank’s website to provide information, type in the URL rather than clicking on an emailed link. Pharming occurs when your browser, compromised by a virus, is hijacked without your knowledge. You type a legitimate website URL into the address bar, but you’re redirected to a fake site that looks legitimate. There, cybercriminals are able to collect any PII you may type into the website. Malicious software is when a hacker tricks you into downloading a malware that does damage to your computer once downloaded. Once attacked, the malware reveals and sends your private information to the hacker. Some websites online are not secured. When a person accesses one of these unsecured websites, they are at risk of getting their information stolen. To know if a website is unsecured or not, Make sure you use only official, secure websites. Websites with the “https:” prefix are safe while other prefixes are unsecured.

### 

### **Findings And Discussions**

A study was conducted including 77 surveys and 21 in-depth interviews. The results suggest that, in addition to using the default privacy settings, students have developed a number of strategies to address their privacy needs. These strategies are used primarily to guard against social privacy threats and consist of excluding contact information, using fixed profile selection, untaging any information attached onto and removing tagged photos. These strategies are used primarily against social privacy threats and consist of cutting out any contact information. It concludes as there is a tilt toward social privacy concerns. Little concern was raised about institutional privacy and no strategies were in place to protect against threats from the use of personal data by institutions. This is relevant for policy discussions, because it suggests that the collection, aggregation, and utilization of personal data for targeted advertisement have become an accepted social norm.

Another study was done on the internet users of the United States. With more and more people using the internet everyday, rates of internet penetration have risen exponentially. In this data-driven era, some people depend on the internet to store their information. The study shows that the number of data breaches that occurred in 2019 rose by 216 than the number of breaches that occurred during 2018. While some see the loss of privacy as a necessary evil, almost 50 percent of U.S. internet users were more concerned about online privacy in 2019 than they were in 2018. With the rise of concern for the breach of internet privacy, new methods to prevent data breaches have been implemented. These new measures have reduced the number of breaches recently. Data breaches have been reduced by 400 from 2019 to 2020.

In any case, stolen personal information is always considered as loss, however sometimes consumers can benefit from revealing personal information, there are many situations in which they would rather remain anonymous. Several tools are available to help people browse the Web anonymously. Perhaps the best-known Web anonymity tool is the Anonymizer (http://www.anonymizer.com), a service that submits requests to Web sites on behalf of its users. Because the request is submitted by the Anonymizer rather than the user, information about that person is not revealed to the Web site. The Anonymizer is easy to use and provides both free and paid-subscription services. Users must trust the Anonymizer to protect their privacy, however, and this tool does not prevent users' Internet service providers from logging their Web activities. Other anonymity tools do not require users to trust a third party to maintain anonymity. Most of these tools, however, are still research prototypes. Crowds is an anonymity system developed by my colleagues at AT&T Labs-Research. With the slogan "Anonymity loves company," Crowds is based on the idea that people can be anonymous when they blend into a crowd. Large numbers of geographically distributed Web surfers can join a group called a crowd and forward all of their HTTP requests through the crowd. Each request is randomly forwarded to another member of the crowd, who can either submit it directly to the end server or forward it to another randomly selected member of the crowd. Neither the end Web server nor any of the crowd members can determine where the request originated. Users participate in a crowd by running a proxy server on their local computers and configuring their browsers to use the local computer as a proxy. Another anonymity tool developed at Lucent's Bell Labs is useful for people who want persistent but anonymous relationships with Web sites. The Lucent Personalized Web Assistant (LPWA) inserts pseudonyms into Web forms that request a user's name. LPWA is designed to consistently use the same pseudonyms every time a particular user returns to the same site, but use a different pseudonym at each Web site. This tool works in conjunction with an anonymizing proxy server; it could also be used with a system like Crowds. LPWA users allow Web sites to accumulate a profile of their preferences over time that may be useful for tailoring content and advertisements to their interests. However, LPWA prevents profile information from being linked to a user's name or combined with information revealed to other sites. P3P also contains a feature that allows for pseudonymous relationships and can be used in place of cookies. Users may choose to send the same unique identifier each time they return to a Web site with which they have reached an agreement. A P3P-compliant browser keeps track of the identifiers and sends a different one to each site. The goal is that once P3P implementations are readily available, Web sites will use this feature when they wish to develop persistent relationships with consumers but do not need personally identifiable information to provide their services. A P3P-compliant browser should also give users complete control over when to take advantage of this feature.

### 

### **Conclusions And Recommendation**

To sum up everything that has been stated so far, Internet privacy is one of the most important things that we need to pay attention to while we are surfing the internet. Because without our concern, our sensitive information that we have inputted on the internet might be tracked by anybody out there. More often than not, the majority of the people are unaware of the risks it might cause. In addition to our privacy being at risk, our safety might also be threatened. Therefore, In order to protect our privacy from being violated in the future, we suggest you to surf the internet anonymously.

Anonymizer (http:// www.anonymizer.com) is one of the well-known websites that we can use to surf the internet anonymously. Moreover, it is easy to use and provides us both free and paid-subscription services. However, this tool doesn’t prevent users’ Internet service providers from logging their web activities. Besides Anonymizer, there are also developed anonymity tools, which most of them are still research prototypes. Crowds, LPWA (Lucent Personalized Web Assistant), and P3P are few of the anonymity systems developed. Crowds is used to forward our HTTP requests randomly to another member of the crowd which can either choose to submit it directly to the end of the server or forward it to a randomly selected member of the crowd. While LPWA inserts pseudonyms into a web form that requests a user’s name and it uses the same pseudonyms for each website the user has visited. P3P also allows pseudonymous relationships and can be used in place of cookies. Everytime users return to a website, they are required to enter a specific identifier/recognizer.

### **References**

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook: The Internet privacy paradox revisited. *Information, Communication & Society*, *16*(4), 479-500.

Miyazaki, A. D., & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing*, *19*(1), 54-61.

Cranor, L. Internet privacy: A public concern. netWorker 2, 3 (June/July 1998), 13–18.

#### 3 Major Internet Privacy Issues and How to Avoid Them -- Security Today. (2019). Retrieved 26 November 2021, from <https://securitytoday.com/Articles/2019/09/03/3-Major-Internet-Privacy-Issues-and-How-to-Avoid-Them.aspx?Page=2>

#### 

#### Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. (2019). Retrieved 26 November 2021, from <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>

#### The History of Internet Privacy - DreamHost. (2019). Retrieved 26 November 2021, from <https://www.dreamhost.com/blog/history-of-internet-privacy/>

https://www.statista.com/topics/2476/online-privacy/#topicHeader\_\_wrapper

<https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>