Towards a Comprehensive Set of PII for Ensuring Privacy Protections

Tanusree Sharma, Illinois Informatics Institute, UIUC
Masooda Bashir, School of Information Sciences, UIUC

Abstract

Personal Identifiable Information (PII) refers to any information that can be used to trace or identify an individual. With increasing online communication and a remote workforce, sharing PII has become mainstream online. In turn, this allows adversaries to attack account users' systems, and impact users financially, economically, and affect their reputation. While the Internet, innovation and industrialization has become the important part of our social and economic structure as a natural component, each individual's development depends on reliable and resilient infrastructure. Since the Internet is an unavoidable resource in our everyday life, this has become necessary to ensure safe and secure communication among different parties to enhance technological capabilities of industrial sectors all over the world. Industries are liable to keep people in society safe in online environments, which makes this a good time to consider a sustainable development plan to ensure security and privacy when preserving online communication for individuals. There are different mechanisms that exist to provide users with a certain level of privacy and safety. With the overarching technological development, it has become complicated to measure and handle PII (directly or indirectly) considering the recent setting of piecewise protection for different data types. In our study, we detail how organizations provide protection for different data types among PII. In addition, we have conducted a short study that analyzes online social data privacy on Facebook and Reddit in regards to how they handle collected data. Finally, we offer several paths for future research that must be considered for a comprehensive privacy protection program for users' PII when developing resilient infrastructure, including regional and transborder.

1. Introduction

Information Communication Technology (ICT) is being continuously developed and is making significant contributions towards economic developments and achieving Millennium development goals [1]. ICT has also been continuously making our communication capabilities and exchange of information easier and more convenient than ever before. The developments in ICTs are paving the way for inhabitants from various nations to support a wide range of applications including health, finance, education, economy, social, and more. We can clearly observe the importance of information technology in recent years as it relates to an increase in remote and tele-workforce and healthcare concerns (i.e. Coronavirus). For example, the COVID-19 pandemic has impacted billions of people around the world in various ways. Advances in technology and ICT is allowing some people to work and learn remotely, and contain the spread of the virus through different means, such as digital contact tracing around the globe. While there are tremendous advantages to advanced technological resources, one important and critical aspect that remains neglected is the privacy risks arising from the digital age. Moreover, in times of crisis (e.g, COVID-19 pandemic), privacy protections tend to take a back seat or be ignored altogether.

Prior research shows that with the help of third parties, many governments around the world are keeping track of its citizen's online activities on some level in the interest of national security [3], [24]. A group of researchers has shown that individual privacy, civil liberty, democracy, and political identity is in crisis due to technological developments and infrastructures which often result in technological surveillance, adversarial attacks, and consumer data breaches [2], [4] [5], [6],[31]. This can result in more severe damages to society if motivation is deflated into surveillance-oriented population management [4] in the modern capitalist nation state (i, e. the United States). Eventually, it may form trends of a dictatorship-style government along the way. Some research is concerning including biometrics in their mobile SIM registration process [7] and disease surveillance through crowdsourcing [8]. Nowadays, utilization of online-based big data analytics with a variety of data driven models are paving the way to link anonymous datasets [9] to re identify individuals researched [32]. This continuous mapping of personal information is leading us to a privacy loophole which can be a potential threat to the overall sustainability of society and the economy. These types of information collection, processing, and analysis can cause cultural, social, and employment inequality. Privacy is a broad and often vague topic that is hard to define, and scholars from different fields have conceptualized privacy in a variety of ways which further illustrates its complexity. In this paper we will focus our work on the specific risks and privacy vulnerabilities that are associated with Personally Identifiable Information (PII). We believe this study is timely and essential for industries and nations around the world when considering the expansion of technology and tracking mechanisms. While PII has been addressed in many information privacy studies, to the best of our knowledge, it has not been researched in a comprehensive manner which suggests a need for an extension of the traditional PII and shows how critical privacy protections are as we move forward with advanced technological developments across the globe.

Sharing PII seems to be a daily activity for many online users. These data sharing practices increase exponentially through social media and online platforms. Many industries, and even government entities, purchase this type of data so they can infer more about certain individuals [6,8]. This data and any related analytics have become the lifeline of many industries across the globe. All recent data breaches indicate that PII is one of the most wanted types of data [10]. The typical data breaches include any incident where confidential or sensitive information has been accessed without permission by capturing or seizing online Ids, passwords, transaction information, and device identifiers. From the Statista report, the number of data breaches in the United States reported by industries amounted to 1,473, with over 164.7 million sensitive records exposed as of 2019. The total data breaches from 2005 to 2019 is 11239 [10]. In the course of normal operations, organizations across the globe collect a wide range of direct and linkable PII.

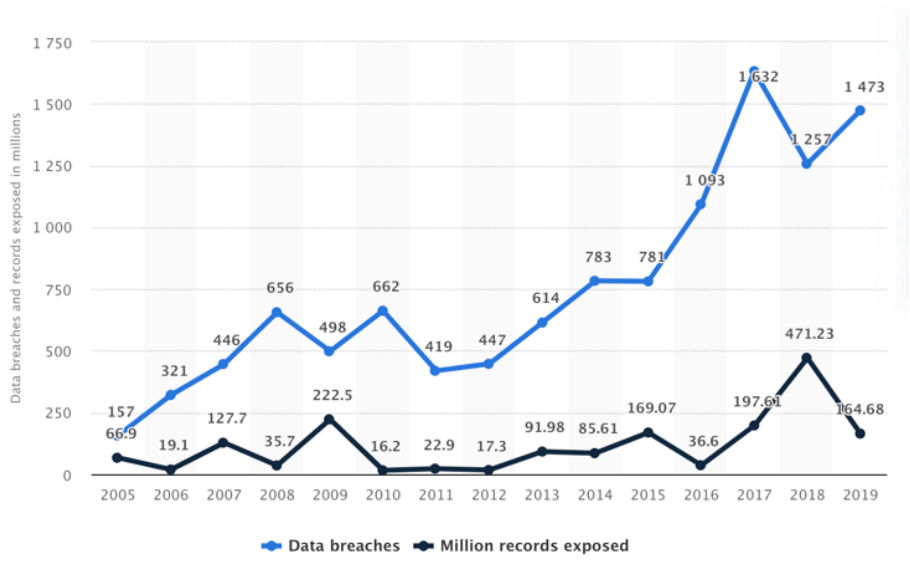

Figure 1: Data breach report from 2005-2019 [10].

While traditional data protections may include an individual's demographics, financial, and health information, there are many other data types that may reveal sensitive and private information to others. This becomes even more challenging due to advanced data tracking functionalities and analytic techniques. An individual's personal information can be easily inferrenced or linked to other identifying information in online environments. For example, our IP addresses and browsing patterns can now expose our behavior patterns and social and political beliefs by inferring through high-tech computational models by big data analytics [11]. In these cases, there is a lack of structured PII models to ensure protection. In developing countries, these issues are even more severe because they are trying to thrive and maintain their global presence through the use of technology without having the appropriate regulations and technological measures in place to protect every consumer's PII which contributes to disparity and privacy violations [19]. In order to move towards a comprehensive set of privacy protections, there needs to be a global and inclusive structure and categorization of PII that is consistent with the evolving capabilities of technology. Considering how PII may be categorized differently based on cultural, socioeconomic, and political differences around the globe are important factors to consider. Therefore, an examination of traditional PII, and an extension to include more categories and data types to formulate comprehensive privacy protections for citizens of the world, is an essential step forward.

2. Background

Scholars from different fields of study have conceptualized privacy from their specializations and world views. For example, Westin's privacy and freedom is one of the first initial efforts to provide an evaluation of the conflict between privacy and surveillance in modern society where he proposed to establish laws in society by developing public respect and concern (pgs. 2, 5) [13]. Whereas law scholar Louis Brandeis proposed privacy as a right that should be left alone which can be established on principles of private justice, moral fitness, and public convenience [14]. Another scholar described privacy as the right for people to withhold or conceal information about themselves that others may use to their disadvantages [15]. Contextual privacy has been proposed by Nissenbaum's [16], which considers the norms of information sharing to capture the nature of

challenges posed by information technologies. A taxonomy of privacy [17] described by Solve is one of the more comprehensive frameworks that has provided guidelines for privacy vulnerabilities at each stage of a data life cycle. For example, it addresses data collection, storage, processing, and sharing. While these conceptualizations may not fully capture the current technological challenges, modern views of privacy should consider digital media and online services, and third parties that collect personal information and utilize it for a variety of purposes.

Privacy protections for digital information have been discussed and debated for a long time. For example, the National Institute of Information and Technology (NIST), GDPR, CCPA (California Consumer Protection Act), and IAPP are some of the entities that have been developing strategies and proposing guidelines to protect individual privacy and safety in digital information [25], [26], [21]. One of the main mechanisms these guidelines illustrate is to defend against privacy violations in terms of consumer PII available online. However, maintaining these protection mechanisms at the same pace with our fast-paced technological development is challenging because today's big data environment involves a variety of consumer PII. Entities around the globe are managing data protection for PII pieces wisely, for example, the existing piecewise protection of the United States includes GLBA (Financial Services Modernization Act), for financial data. data, ECPA (Electronic Communications Privacy Act) for electronic communication, HIPPA for health data. These types of protection will not be sustainable with more integration and incorporation of different technologies. Therefore, we propose that the initial step towards developing comprehensive privacy protections is evaluating and expanding PII.

3. Method

In this section, we will describe in detail how we built our proposed comprehensive PII model and the steps we took to conduct our research study.

Step 1: First, we studied the NIST and DHS guidelines for PII to form our initial understanding of how PII is defined by these organizations [18], [25], [21]. While these guidelines included several data types, it did not provide broader categories. The types of data, they include: basic demographics, personal preferences, contact information, community interaction, and financial information. NIST defines PII as "(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" (McCallister et al, 2010, p. 7). NIST's example of PII includes [25] name, personal identification number, address information, personal characteristics, and information about an individual that is either linked or linkable**.** Whereas **the** Department of Homeland Security (DHS) defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, person traveling to the U.S., or an employee or contractor to the Department (p.5) [21]. In the Department of Homeland Security handbook, PII is divided into two types: (i) Direct PII and (ii) Linkable Information.

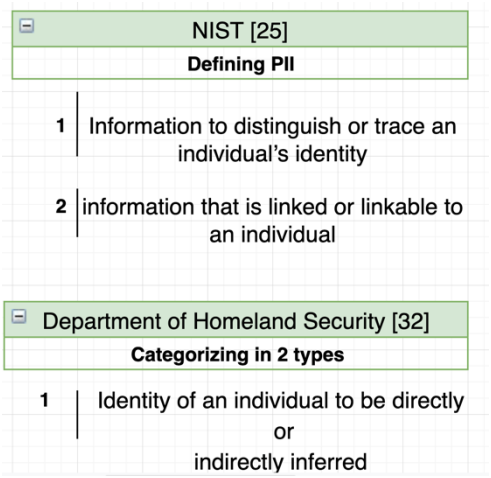

Figure 2: Step 1 of Method

Step 2: We researched existing PII frameworks to determine if there were any PII categorizations that we can use as our initial point. Through this search, we identified international associations of privacy professionals (IAPP) to have a broader framework for PII categorization that included six PII categorizations. IAPP considers PII categories of information about an individual which relates to their private, professional, or public life which includes 6 main categories [20]: Internal, external, social, financial, historical, and tracking.

Step 3: We used these six categories to build our first tier of the model of PII.

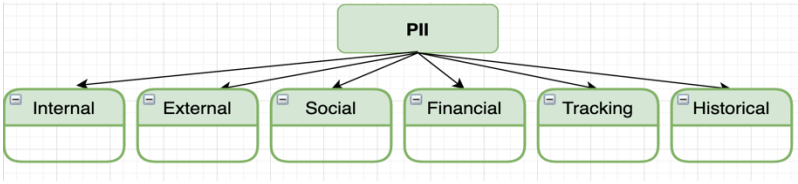

Figure 3: Step 2 of Method

Step 4: We populated each of the six categories in our first tier by including the data types that were described in the NIST and DHS guidelines. For example, basic demographics from NIST's PII example has been mapped to the internal category, contact information into tracking, community interaction into social, financial information into financial, and secure identifiers mapped into the external category.

Step 5: To assure that our PII model is comprehensive, we coded each of the data types included in the second tier as either Direct (DP) or Linked (LI) PII. We made this distinction based on NIST and DHS guidelines. We believe this classification would further enable and provide PII sensitivity that can be used to provide the appropriate privacy protections.

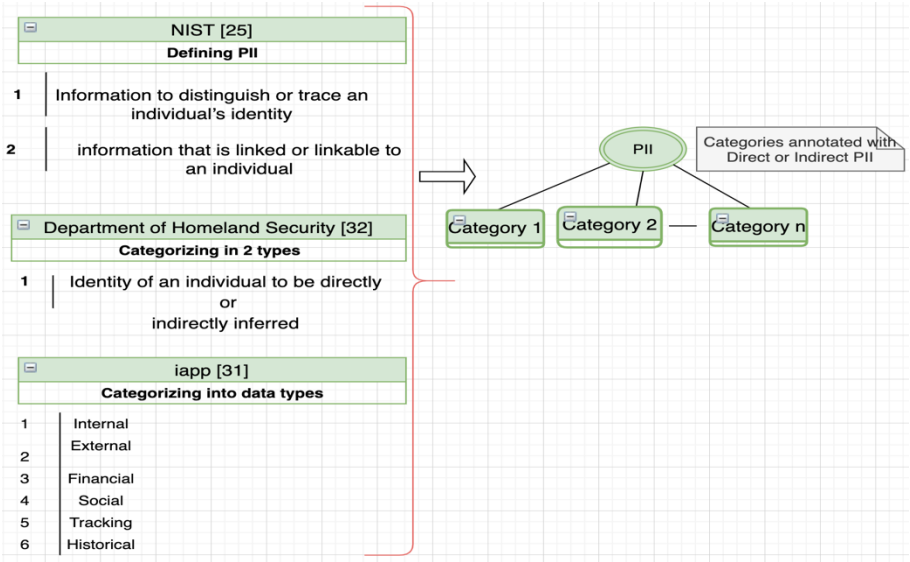

Figure 4: Skeleton of comprehensive PII categorization

Based on the skeleton model of our comprehensive PII categorization, Figure 5 shows our systematic approach in building a comprehensive model of PII below.

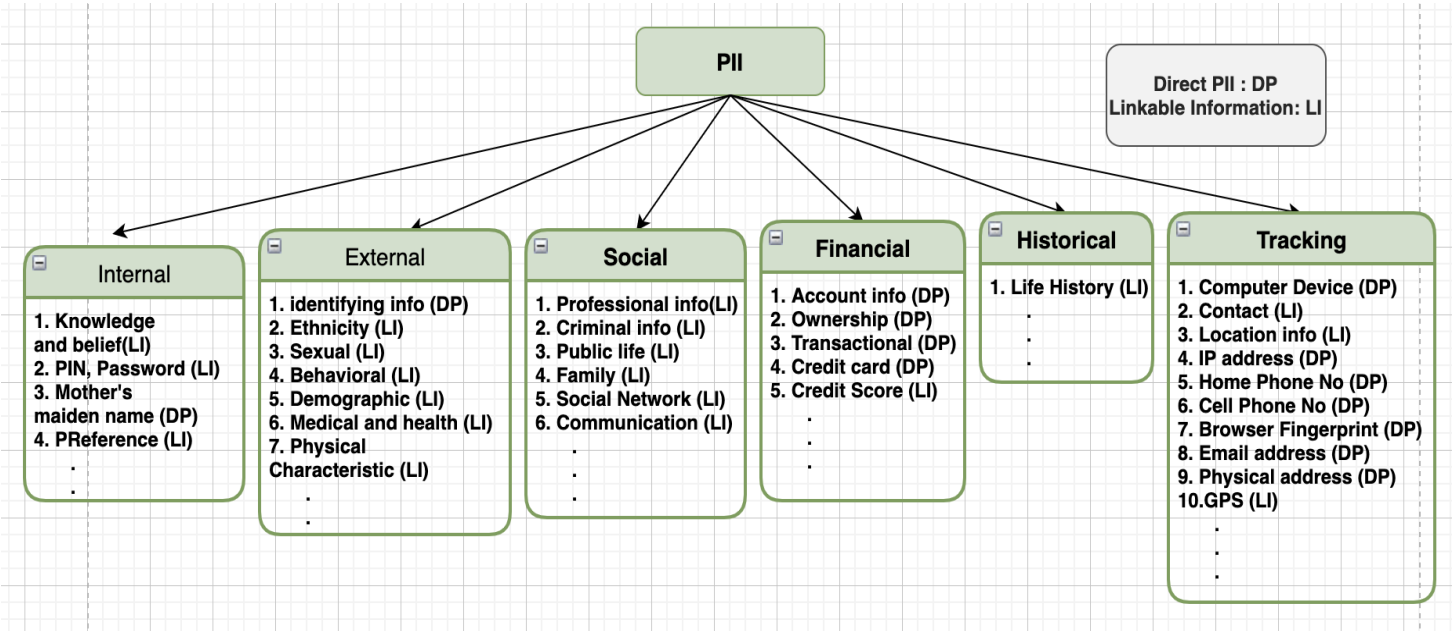

Figure 5: PII data categorization model, motivated by NIST, iApp, and Department of Homeland Security [25], [20], [21]

Step 6: In the final step of building our PII model, we included protection mechanisms that are currently available for the PII categories and data types present in them. These protections include legal and technological protections such as encryption, data aggregation, and anonymization.

Data Types	Example	Laws	Technology
Internal		✓	✓
Knowledge and Belief	Religious beliefs, philosophical beliefs, thoughts	Federal Law NCSL US Constitution, NIST ECPA Communications Decency Act	
Authentication	Passwords, PIN, mother's maiden name		
Preference	Opinions, intentions, interests		
External		✓	✓
Identifying	Name, user-name, unique identifier, government issued identification, picture, biometric data	Data Protection Law digital inequality NIST Federal Identity Management U.S. Department of Education CCPA Health Insurance Portability and Accountability Act (HIPPA)	
Ethnicity	Race, national or ethnic origin, languages spoken, dialects, accents		
Sexual	Gender identity, preferences, proclivities, fetishes, history		
Behavioral	Browsing behavior, call logs, links clicked, demeanor, attitude		
Demographic	Age ranges, physical traits, income brackets, geographic		
Medical and Health	Physical and mental health, drug test results, disabilities, family or individual health history, health records, blood type, DNA code, and prescriptions		
Physical	Height, weight, age, hair color, skin tone, tattoos, gender, piercings		
Historical		✗	✗
Life History	Information about an individual's personal history		
Financial		✓	✓
Account Infornation	Credit card number, bank account	Data Protection Law FTC guideline Financial Services Modernization Act (GLBA) [1999]	
Ownership	Cars, houses, apartments, personal possession		
Transactional	Purchases, sales, credit, income, loan records, transactions, taxes, purchases and spending habits		
Credit	Credit records, credit worthiness, credit standing, credit capacity		
Social		✗	✓
Professional	Job titles, salary, work history, school attended, employee files, employment history, evaluations, references, interviews, certifications, disciplinary actions	FTC guideline , NIST	
Criminal	Convictions, charges, pardons		

Public Life	Character, general reputation, social status, marital status, religion, political affiliations, interactions, communications meta-data		
Family	Family structure, siblings, offspring, marriages, divorces, relationships		
Social Network	Friends, connections, acquaintances, associations, group membership		
Communication	Telephone recordings, voice mail, email		
Tracking		✗	✓
Computer Device	IP address, Mac address, browser fingerprint.	FTC guideline , NIST	
Contact	Email address, physical address, telephone number		
Location Information	Country, GPS coordinates, room number		

Table 1: Existing Protection Mechanisms for PII Data categories and Data types from the United States' Perspective (Public Sector)

4. Case Study

To test our newly developed Comprehensive PII model, we decided to conduct a case study to examine PII availability in an online environment and how that type of information is protected. To carry out this test, we selected one PII category (social) from the model and chose to analyze social network data types from Facebook and Reddit. We elected these two social networks because they present different privacy protection mechanisms. We also studied these two social networks' data lengths to have understanding of available PII and PII handling and sharing.

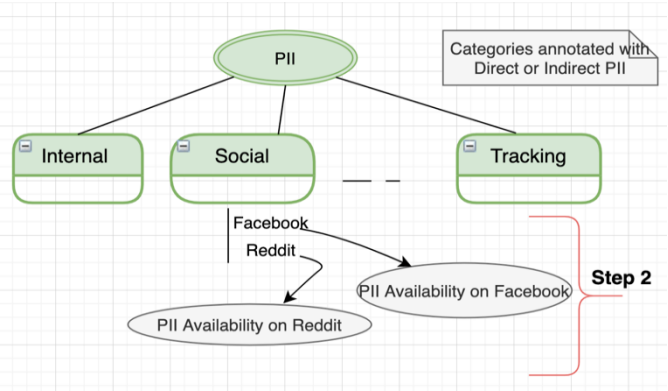

Figure 6: Case Study of one data category (social) from our model

In cases of information sharing on social media, researchers have found evidence of users intending to publish different pieces of information on different social networks which demonstrates privacy risks by linking personal information [28]. Facebook states that, on average, more than 600 million users provide more than 90 pieces of content per month [29]. Whereas, Reddit – a web traffic powerhouse known for anonymous usage of communication – recorded almost 1.6 billion visits as of April 2019, making it one of the most-visited websites [10]. We can see that these two online media are quite rich in terms of users' personal information.

DataReportal-Global Digital Insights mentioned that during the sign-up process on Facebook, users tend to share contact information (e.g., name, address, telephone number, email address) [23]. Frequent sharing of personal information from users' is increasing Facebook PII data spread [30]. In our study, we initially recorded different types of information on Facebook deals with (either from users input or collected by Facebook via different ways). Most information is linkable across different social networks.

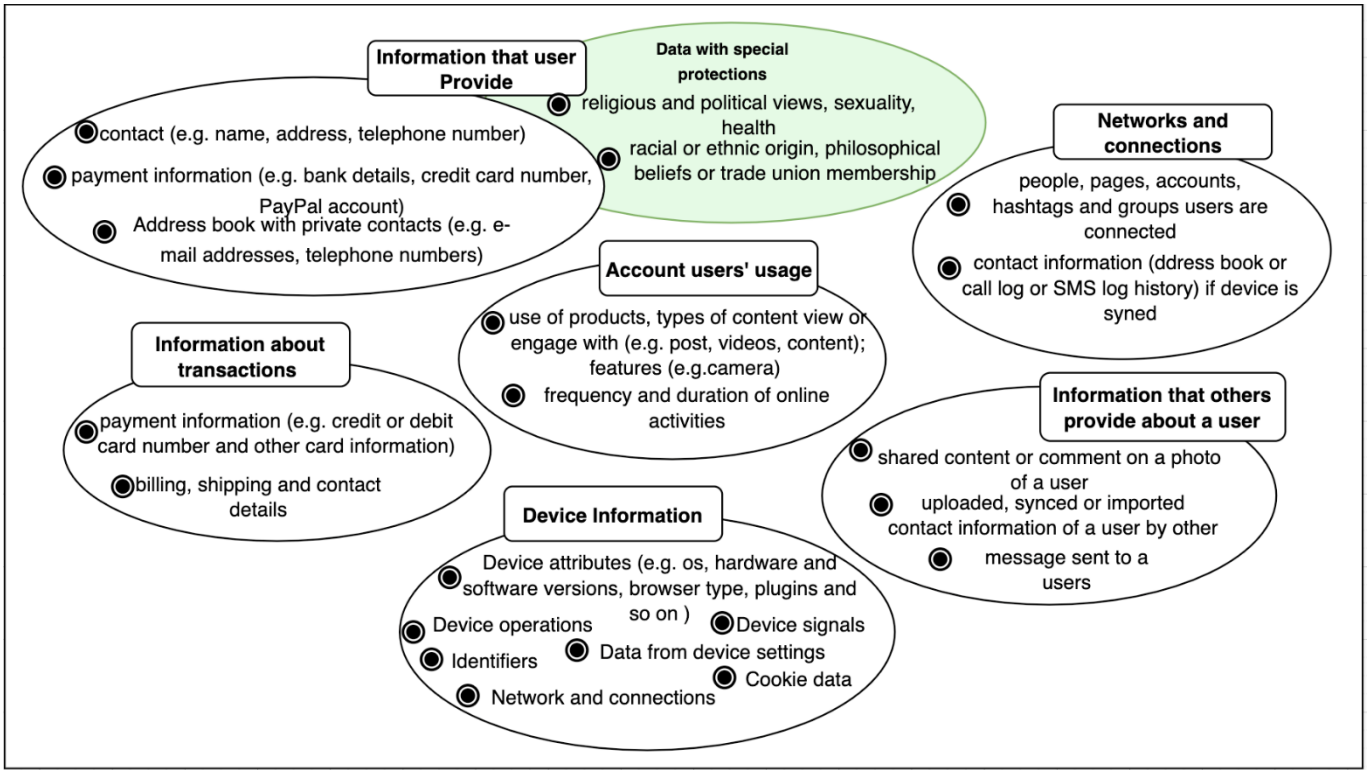

Figure 7: Personal information available on Facebook

Facebook has direct PII and linkable information from different sources and settings: directly from users; transaction by users on Facebook for donation or any online shopping; Facebook network connection by different pages, hashtags, and accounts; users' preference of content (e.g., posts, videos), product, services, and feature (e.g. camera) usage; time spent on Facebook; information shared by others via post, comments, and photos; and device information. Our accumulated result for users' personal information on Facebook online platforms are organized in **Figure 7.** We have found that Facebook mentions certain PII to be considered for special protection which includes religious and political views, sexuality, health, racial and ethnic origin, philosophical beliefs, or trade union communication. We aim to conduct a more detailed analysis in our future study about other linkable information that is available on Facebook such as shared posts, comments, online activities, and how those are protected online.

Unlike Facebook, Reddit is quite different in terms of its anonymous online communication. Therefore, we also tried to find out how and what types of individual information Reddit deals with. PII collection by Reddit includes: account information, posts, comments, messages and

communication, transaction information, and some automatically collected information (e.g., log and usage data, location data) [22]. Reddit has not specified any special protection for any particular data categories compared to Facebook. However, it provides anonymous communication where a user's name is not required to be a real name, which provides a certain level of confidentiality, and users are not required to provide email during sign up.

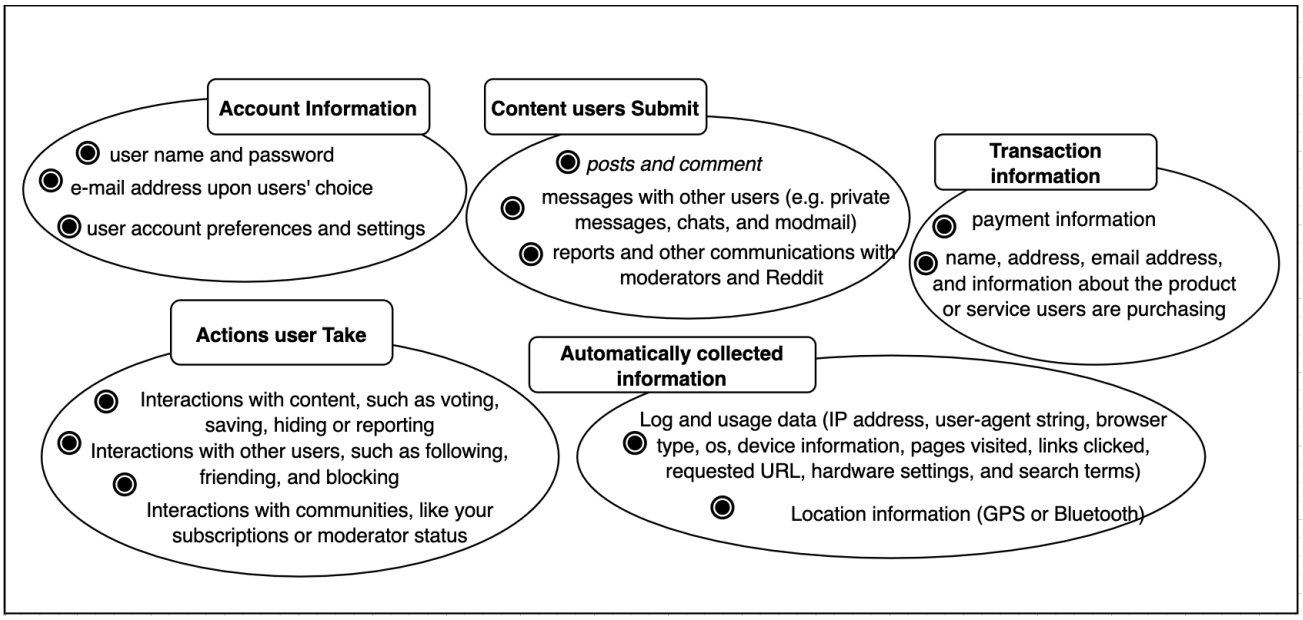

Figure 8: Personal information available on Reddit

5. Discussion

PII is a big part of preserving users' privacy, and while building reliable and resilient infrastructure of technological innovation, industries need to prioritize protecting their consumers' privacy. In doing so, industries need a comprehensive PII model to ensure quality protection. Our purpose during this study was to contribute to the industrial development of PII identification and categorization. In order to do that, we have initiated PII categorization, mapped existing protection mechanism availability for PII, and conducted a case study of PII availability online.

PII-breach is one of the most frequent threats to information privacy. Online media allows users to publish personally identifiable information and people are using this opportunity extensively. Though users expect their data to be visible in their respective platform, their data is linked with other data sets on different social media platforms which increases risk of data breach and other privacy violations. A person can be associated with their online identifier (e.g., device Id, IP address, cookie identifiers) which may be traced back to the user [12]. According to the PII definition, these are not direct PII because they are anonymous. However, this information is linkable and distinguishes one individual from another, therefore, it may pose privacy risks. Hence, there needs to have privacy protections for this linkable information. In our model, we distinguished between direct and linkable PII because this would ensure further protection of sensitive information online.

NIST has specified that organizations should categorize their PII by the PII confidentiality impact level [26] based on factors (identifiability, quantity of PII, data field sensitivity, context of use, obligations to protect confidentiality, and access to and location of PII). For example, some federal agencies, such as the Census Bureau and the IRS are subject to specific legal obligations to protect certain types of PII [27]. While collecting and processing PII is becoming a commonplace and a great deal of cross border information sharing, all sectors of business and online social media platforms should have a comprehensive PII categorization to ensure data protection. We believe our study provides two important contributions towards online privacy protections. Our first contribution includes a hierarchical tree of different PII categorizations based on established standards and regulations. In addition, our model includes annotated data types as direct PII and linkable PII. Our second contribution is a case study that reveals an overall picture of PII (social category) on current social networks (Facebook, Reddit). This gives us a clear idea about available PII online and some of the special data protection practices for particular types (e.g., religious affiliations, political beliefs, sexuality, health).

Our study also mapped mechanisms available for our categorized PII. It reveals a piecewise privacy protection. For health data, there is HIPPA, for financial data, there is the Financial Service Modernization Act (GLBA), for children's data, there is COPPA, for computer-related activities involving the unauthorized access of a computer to obtain certain information, there is Computer Fraud & Abuse Act (CFAA) [1986], and for electronic communications, there is Electronic Communications Privacy Act (ECPA) [1986]. With the fast advancement of technologies, it will become more difficult for government entities and organizations to compartmentalize privacy protection to the ever-increasing amount of PII data types online where our comprehensive PII model would be designed to ensure protection beyond different data types.

While we have the PII categorization and the landscape of existing laws and technology of different PII, our next stop will be measuring the value of PII mathematically. The measure of different information types of PII will give concrete decision-making properties for any entities on how much importance they should provide on each type. For example, if we want to measure how much threats can happen if a particular Data type (SSN) gets leaked or lacks protection, we can think of this Privacy Threat (PT) as a function of Data Types (D). PT = f(D). This can present "**How much an individuals' record, D can change the output of Privacy Threat PT in online?"** In our future work, we will be exploring different mathematical models to explain this relationship.

6. Conclusion

This paper summarizes some of the existing challenges of PII data protection within realms of big data, when personal information of individuals can be found, and cross examined and aggregated from many different data sources. We have summarized the early attempts of solutions that are developed for different data types while highlighting the issues of disarrayed protection associated with those, which needs detailed comprehensive study that can give protection beyond different data types available online. For ensuring continuous technological advancement with sustainability and reliability among industries and consumers, this study on PII categorization

online could be a critical step forward. In future study, we will be conducting an analysis of collective privacy impact for different PII categorization in our model and the level of sensitivity for finding appropriate measures of comprehensive privacy design.

Reference

[1] Gaevart, R. (2012). A Sustainable Model for {ICT} Capacity Building in Developing Countries. In *Presented as part of the 26th Large Installation System Administration Conference ({LISA} 12)* (pp. 123-134).

[2] Santa Maria Shithil, T. K. S., & Sharma, T. A Dynamic Data Placement Policy for Heterogeneous Hadoop Cluster.

[3] Sharma, T., & Bashir, M. (2020). Are PETs (Privacy Enhancing Technologies) Giving Protection for Smartphones?--A Case Study. *arXiv preprint arXiv:2007.04444*.

[4] Ogura, T. (2006). Electronic government and surveillance-oriented society. *Theorizing surveillance: The panopticon and beyond*, 270-295.

[5] Verplanke, J., Martinez, J., Miscione, G., Georgiadou, Y., Coleman, D., & Hassan, A. A. (2010). Citizen Surveillance of the State: A mirror for eGovernment?. In *What kind of information society? Governance, virtuality, surveillance, sustainability, resilience* (pp. 185-201). Springer, Berlin, Heidelberg.

[6] Wang, S. S., & Hong, J. (2010). Discourse behind the forbidden realm: Internet surveillance and its implications on China's blogosphere. *Telematics and Informatics*, *27*(1), 67-78.

[7] Sharma, T., & Bashir, M. (2020, July). Privacy apps for smartphones: An assessment of users' preferences and limitations. In *International Conference on Human-Computer Interaction* (pp. 533-546). Springer, Cham.

[8] Haddawy, P., Frommberger, L., Kauppinen, T., De Felice, G., Charkratpahu, P., Saengpao, S., & Kanchanakitsakul, P. (2015, May). Situation awareness in crowdsensing for disease surveillance in crisis situations. In *Proceedings of the Seventh International Conference on Information and Communication Technologies and Development* (pp. 1-5).

[9] Ardagna, C. A., Bellandi, V., Bezzi, M., Ceravolo, P., Damiani, E., & Hebert, C. (2018). Model-based big data analytics-as-a-service: take big data to the next level. *IEEE Transactions on Services Computing*.

[10] Annual number of data breaches and exposed records in the United States from 2005 to 2019. Statista. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/. Retrieved on March 23, 2020.

[11] Panzarasa, P., Opsahl, T., & Carley, K. M. (2009). Patterns and dynamics of users' behavior and interaction: Network analysis of an online community. *Journal of the American Society for Information Science and Technology*, *60*(5), 911-932.

[12] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1374-1-1. Official Journal of the European Union

[13] Westin, A. F. (1967). Privacy and freedom Atheneum. *New York*, *7*, 431-453.

[14] Brandeis, L., & Warren, S. (1890). The right to privacy. *Harvard law review*, *4*(5), 193-220.

[15] Posner, R. A. (1977). The right of privacy. *Ga. L. Rev.*, *12*, 393

[16] Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.*, *79*, 119.

[17] Solove, D. J. (2005). A taxonomy of privacy. *U. Pa. L. Rev.*, *154*, 477.

[18] Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. In *European data protection: coming of age* (pp. 3-32). Springer, Dordrecht.

[19] Vestoso, M. (2018). The GDPR beyond Privacy: Data-Driven Challenges for Social Scientists, Legislators and Policy-Makers. *Future Internet*, *10*(7), 62.

[20]CATEGORIES OF PERSONAL INFORMATION. iapp. https://iapp.org/media/pdf/resource_center/Categories-of-personal-information.pdf. Retrieved March 21, 2020.
[21] Handbook for Safeguarding Sensitive PII, Department of Homeland Security. https://www.dhs.gov/sites/default/files/publicationsdhs%20policy%20directive%20047-01-007%20handbook%20for%20safeguarding%20sensitive%20PII%2012-4-2017.pdf . Retrieved March 21, 2020.
[22] Reddit Privacy Policy. https://www.redditinc.com/policies/privacy-policy-january-10-2020. Retrieved March 23, 2020.
[23] DataReportal-Global Digital Insights. https://datareportal.com/. Retrieved on March 23, 2020.
[24] Sharma, T., & Bashir, M. (2020). Use of apps in the COVID-19 response and the loss of privacy protection. *Nature Medicine*, 1-2.
[25] MCCALLISTER E, GRANCE T and SCARFONE K (2010) Guide to protecting the confidentiality of personally identifiable information (PII). NIST Special
Publication. [WWW document] http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=904990 (accessed 19 March 2020).
[26] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems,* http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.
[27] Whisner, M. (2009). The United States Code, Prima Facie Evidence, and Positive Law. *Law Libr. J.*, *101*, 545.
[28] Labitzke, S., Taranu, I., & Hartenstein, H. (2011, August). What your friends tell others about you: Low cost linkability of social network profiles. In *Proc. 5th International ACM Workshop on Social Network Mining and Analysis, San Diego, CA, USA* (pp. 1065-1070).
[29] Statista report. https://www.facebook.com/press/info.php?statistics
[30] Data Policy, Facebook, https://www.facebook.com/about/privacy/. Retrieved on March 21st , 2020
[31] Rahman, S., Sharma, T., Reza, S. M., Rahman, M. M., & Kaiser, M. S. (2016, December). PSO-NF based vertical handoff decision for ubiquitous heterogeneous wireless network (UHWN). In *2016 International Workshop on Computational Intelligence (IWCI)* (pp. 153-158). IEEE.
[32] T. Sharma, J. C. Bambenek, and M. Bashir. (2020). Preserving Privacy in Cyber-Physical-Social Systems: An Anonymity and Access Control Approach. [Online]. Available: https://www.ideals.illinois.edu/handle/2142/106049