The Current State of Data Privacy

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Christopher Nguyen

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Pedro A. P. Francisco, Department of Engineering and Society

Introduction

The evolution of telecommunication has had a profound impact on society, changing the way we use technology and interact with one another. However, the complexity of these systems has resulted in a knowledge gap regarding how these systems work and how user interactions are accessible to others, causing serious data privacy issues. The lack of transparency from service providers and imprecise government regulation has contributed to these issues. In this paper, we investigate: what are the reasons behind these issues using the actor network theory (ANT) and what are the steps taken to mitigate them?

The actor network theory is a framework that focuses on understanding complex systems by examining the interactions and relationships between actors within that system. In the context of telecommunication, the ANT can be used to explain the interactions and relationships between various actors involved in the functioning of the network, such as users, service providers, governments, and technologies.

One of the core concepts of the ANT is the notion of "black boxes," which refers to the parts of a system that are opaque and difficult to understand. In the case of telecommunication, the complexity of the network and the sheer number of actors involved can make it difficult to understand how data flows through the system, who has access to it, and how it is being used. This lack of transparency can lead to privacy breaches, as users may not be aware of the extent to which their data is being shared and used by various actors within the network.

The ANT also emphasizes the agency of non-human actors within a system, such as technologies or objects. In the case of telecommunication, these non-human actors play a crucial role in shaping the interactions between human actors. For example, the development of new

technologies can shape the way that users interact with the network, while changes in government regulations can shape the way that service providers operate.

Another key aspect of the ANT is the notion of "enrolment," which refers to the process by which actors are brought into a network and given specific roles and responsibilities. In the context of telecommunication, this could refer to the process by which users are enrolled in a service provider's network and given access to various technologies and services. The way that users are enrolled can shape their interactions with the network and their understanding of how their data is being used (Cressman, 2009).

Background

One of the main reasons for the lack of data privacy is poor user education; many users are not confident in or entirely unaware of the securities surrounding their data (Auxier, 2019). As technology evolves at a rapid pace, users struggle to keep up, resulting in service providers taking advantage of users and serious privacy breaches. The complexity of the network makes it a black box where the path of data is untraceable by any individual. Users lack the technical knowledge required to track data, making it impossible to hold those responsible for data accountable. The lack of transparency by service providers has contributed to this problem. Companies like Amazon, Meta, and Google offer financial services that require more sensitive information such as banking details and credit history, resulting in a detailed user profile (Boissay, 2021).

Another issue is the malpractice by providers who hide information in user agreements and go against privacy agreements without consent. Large corporations have violated privacy rights, requiring legislative and public action to mitigate issues. Meta and other data companies have given user data to third parties, such as Cambridge Analytica, leading to privacy breaches.

The unregulated amount of data sharing resulted in many users being unaware of the extent of information shared, and companies could not be held accountable (Isaak and Hanna, 2018).

To address these issues, government intervention has played a significant role in regulating data and reviewing security risks involved in telecommunications infrastructure. To prevent such privacy breaches and ensure accountability, the government has put in place stringent regulations that require companies to obtain explicit consent from users before collecting or sharing their data.

Moreover, it is crucial to improve user education about data privacy. One of the reasons behind data breaches is the lack of knowledge about data privacy among users. The incorporation of data privacy education in the curriculum of schools and universities is necessary to make users aware of the risks and consequences of data breaches. Service providers should also take responsibility for educating their users about data privacy and informing them about the collection and usage of their personal data. They must provide transparency in their practices and ensure that their users have control over their data.

In order to make improvements to the regulations and in turn improve overall data privacy, we must determine if there are any changes to the regulations that can be made to remove loopholes and cover all edge cases. Currently, improvements are only made once a data privacy violation occurs, but we must be proactively adapting the regulations as technology continues to evolve. The complexity of the network and the increasing amount of data being shared online make it challenging to regulate data privacy effectively. However, with the right regulatory framework, we can protect users' data privacy while still allowing for innovation and growth.

Methods

The research methods of this paper involve collecting secondary sources such as legal rulings and policy documents to identify where regulations have failed to protect user data and where organizations have circumvented the regulations. This research will use case comparisons and historical analysis to identify the faults in policies and draw conclusions about how to improve them in the future. The theoretical framework chosen is the actor network theory (black boxes) due to the complexity of the internet and telecommunication systems.

The use of secondary sources such as legal rulings and policy documents is a common method of research in the social sciences. Secondary sources are valuable because they provide a wealth of information that has already been analyzed and interpreted by other researchers. By examining these sources, we can gain insight into the history of regulation and identify gaps in existing policies. The use of legal rulings is particularly useful because they provide a record of how regulations have been interpreted and applied in practice.

I will also use case comparisons and historical analysis to identify faults in policies. This method involves comparing different cases and analyzing their similarities and differences to draw conclusions about the underlying issues. Historical analysis is another valuable method of research because it helps understand how policies have evolved over time and identify patterns that may be relevant to current issues.

The use of the actor network theory (black boxes) as a theoretical framework is a novel approach to understanding the complexity of the internet and telecommunication systems. The actor network theory posits that there are many actors involved in any system, each with their own interests and motivations. By understanding the relationships between these actors, we can gain insight into how the system operates and identify potential areas of weakness. The use of

black boxes refers to the idea that some actors in the system may be unknown or hidden, making it difficult to fully understand the system.

Overall, the research methods used in this paper are well-suited to the research question and theoretical framework. By using secondary sources, case comparisons, and historical analysis, we can gain a comprehensive understanding of the issues surrounding data protection regulations. The use of the actor network theory (black boxes) is particularly valuable because it explores the complexities of the internet and telecommunication systems in a nuanced and detailed way. By employing these research methods, we can draw meaningful conclusions about how to improve data protection regulations and ensure that user data is properly protected in the future.

Results

Before every aspect of life was interconnected with technology, the primary type of data collected from users were identity related, such as name, address, and phone number, as well as browsing history within applications. Today, technology has connected all systems, with companies collecting information on users, creating one very detailed profile for each user, expanding beyond identity. One example is companies such as Amazon, Facebook, and Google, entering the financial sector. They have built on top of their digital platforms in social media and e-commerce their own financial service, including “payments, money management, insurance, and lending.” These services require more sensitive information such as banking information, social security numbers, and credit history, which can be shared among other companies and added to a user’s global profile (Boissay, 2021). The sharing of this information must be consensual, which is impossible if the companies cannot be held accountable for their actions.

Evidence has shown that many users are either unaware of or feel a lack of control over how their personal information is being used. In a survey conducted by Pew Research Center, 81% of respondents stated they do not have control over their data and 59% said they do not understand how their data is collected or used (Auxier, 2020). Another survey by Cisco from 2021 studied consumer's perception of privacy practices and laws. The study found that over half of respondents do not feel they have the ability to protect their own data. A majority of them care about their privacy and are willing to act but only half have actively made choices to protect their data. When asked what entities should be responsible for protecting data, the results were spread out between the government, private companies, and individuals (Building Consumer Confidence Through Transparency and Control, 2021). The gap in understanding is both due to reluctance of users in understanding the complexities of telecommunications, and malpractice by providers through hiding information in user agreements and going against privacy agreements without consent.

There are multiple instances of privacy violations by large corporations, and it has taken legislative and collective public action to expose and mitigate these issues. One company in particular, Meta, has had multiple violations in the past that have led to massive lawsuits. Meta, along with many other large data companies, give access to user data to third parties such as Cambridge Analytica. In one case, it was discovered that Metagave Cambridge Analytica access to "personally identifiable information of more than 87 million users." Meta had violated a consent decree created in 2011, but Cambridge Analytica leveraged an "alliance" with Metathat circumvented regulations (Jim, 2018). Because the amount of data is relatively unregulated, most users were unaware of what data was shared and Meta could not be held responsible.

In another case, Instagram, whose parent company is also Meta, was found guilty of violating the General Data Protection Regulation (GDPR), which was put into place in 2018. In May 2021, the Data Protection Commission (DPC) in Ireland fined Instagram €225 million for violating the GDPR. This was the largest fine ever imposed under the GDPR and highlights the increasing role of government regulation in protecting individuals' data privacy. The DPC's investigation found that Instagram had failed to provide adequate transparency to users about how their data was being collected and processed. The social media platform was found to have failed to provide clear information about how it used users' data for advertising purposes, and had also failed to obtain valid consent from users for targeted advertising. The investigation also found that Instagram had processed the personal data of children without obtaining parental consent, which is a serious violation of GDPR. Instagram had also failed to implement adequate measures to protect users' data from unauthorized access, as required by GDPR (Data Protection Commission announces conclusion of two inquiries into Meta Ireland, 2023).

Meta was once again found guilty of violating data privacy after these instances. On November 25, 2022, the Data Protection Commission (DPC) in Ireland announced that it had concluded its inquiry into Meta Platforms Ireland Limited (MPIL), the data controller of Facebook, and imposed a fine of €265 million, as well as corrective measures. The inquiry was initiated on April 14, 2021, following media reports of a collated dataset of Facebook personal data that had been made available on the internet. The inquiry focused on an examination and assessment of Facebook Search, Facebook Messenger Contact Importer, and Instagram Contact Importer tools and their processing during the period between May 25, 2018, and September 2019. The DPC's investigation centered on whether MPIL was compliant with the General Data Protection Regulation's (GDPR) obligation for Data Protection by Design and Default, which

requires companies to implement technical and organizational measures to ensure the protection of user data. The inquiry process was comprehensive, including cooperation with all other data protection supervisory authorities within the EU, who agreed with the DPC's decision (Data Protection Commission announces decision in Facebook "Data Scraping" inquiry, 2022).

As more companies continue to adopt 5G, there are several existing infrastructure that do not meet the requirements of objectivity and transparency. An article the research primary security risks of telecommunication supplies found the following are related to reduced data privacy: a strong link between supplier and government of a third country, a third country's legislation, characteristics of the telecommunications supplier's ownership, and the ability of a third country to exercise pressure (Rogalski, 2021).

Government intervention has taken a big part in regulating data; one example is a review done by the government of Australia on security risks involved in the telecommunications infrastructure. These reviews were decided to be held because of the rise in cybersecurity incidents, including officers of other countries colluding with the Australian government. In addition, the shift to new 5G in all government processes has increased the need for higher security measures. With the adoption of 5G technology, the current infrastructure lacks objectivity and transparency, leading to reduced data privacy. As a result, the government must take steps to improve transparency in the telecommunications sector and regulate the flow of data (Botton 2018).

Telecommunication continues to innovate, creating new protocols and standards; 5G is anticipated to be replaced with 6G by 2028. In addition to the technological changes, there are several societal changes that have to be made. First is which groups will govern what aspects of the new technology. This includes the source code and user data. Second is how will the new

technology be distributed between governments, including trade barriers and where the hardware is held. Lastly is how society will use 6G, such as how will the carbon footprint change and how will the public perceive 6G (Moussaoui, 2022).

While it is important to ensure user data is used ethically and securely for the existing systems, it is important to also prepare for changes in technology. The lack of preemptive planning when creating legislation has led to the existing gaps in data privacy, so preparing for future changes now will prevent the same issues repeating themselves.

Discussion

This research studied three aspects of the current state of data privacy, user confidence, past regulation violations, and current actions being taken to improve regulations. The use of personal data has become increasingly widespread in recent years, with companies collecting vast amounts of information about users' habits, preferences, and behaviors. While this data can be used to improve products and services, it also raises significant concerns about privacy and the potential for misuse.

One critical aspect of data privacy is user confidence. When users entrust their data to companies, they expect it to be used responsibly and kept secure. However, high-profile data breaches and scandals, such as the Cambridge Analytica scandal, have eroded trust in companies' ability to protect users' data. This lack of confidence can have significant implications for companies, as users may be less likely to share their data or use their products or services.

Another significant concern is the past regulation violations. In recent years, many companies have been found to violate data privacy regulations, resulting in significant fines and reputational damage. For example Meta has been found guilty and fined on multiple occasions

for mishandling user data. These violations highlight the need for stronger regulations and enforcement to protect user data.

Fortunately, steps are being taken to improve regulations and protect user privacy. In the United States, there have been calls for a federal data privacy law to establish a clear set of rules for companies to follow.

These three aspects directly relate to the actor network theory. Specifically, the complexity of telecommunications, the black box, has left users unaware or skeptical of how their data is handled, and it requires multiple actors, such as private corporations or government, to step in and create regulations that prevent exploitation and allow for more transparency for users.

Conclusion

This research paper analyzes the current state of data privacy through three key aspects: user confidence, past privacy violations, and steps being taken to improve regulations. The study reveals that data privacy is still a significant concern for users, companies, and policymakers, but progress is being made to address the issue. User confidence in data privacy is low due to high-profile data breaches and scandals, which can negatively impact companies as users may be less likely to share their data or use their products or services. However, companies are taking measures to improve data privacy, such as investing in better security measures, implementing privacy-by-design principles, and being transparent about their data collection practices.

Past privacy violations have highlighted the need for stronger regulations and enforcement to protect user data, and governments have been proactive in addressing the issue. Overall, while the state of data privacy is still imperfect, companies that prioritize data privacy can build trust with users and ensure the long-term sustainability of their businesses by

implementing stronger regulations, better security measures, and transparency in their data collection practices.

References

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center: Internet, Science & Tech. Retrieved October 27, 2022, from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Boissay, F., Ehlers, T., Gambacorta, L., & Shin, H. S. (2021). Big Techs in Finance: On the new Nexus Between Data Privacy and Competition. *The Palgrave Handbook of Technological Finance*, 855–875. https://doi.org/10.1007/978-3-030-65117-6_31

Botton, N., & Lee-Makiyama, H. (2018). *5G and national security after Australia's telecom sector security review*. Retrieved from European Centre for International Political Economy (ECIPE) website: http://hdl.handle.net/10419/202509

Building Consumer Confidence Through Transparency and Control. (2021). *Cisco Secure*. retrieved from https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf

Cressman, D. (2009). A Brief Overview of Actor-Network Theory: Punctualization, Heterogeneous Engineering & Translation.

Data Protection Commission announces conclusion of two inquiries into Meta Ireland. Data Protection Commission. (2023, January 4). Retrieved March 16, 2023, from https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-con

clusion-two-inquiries-meta-ireland#:~:text=Final%20decisions%20have%20now%20been,relation%20to%20its%20Instagram%20service).

Data Protection Commission announces decision in Facebook "Data Scraping" inquiry. Data Protection Commission. (2022, November 28). Retrieved March 16, 2023, from https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry

Isaak, J., & Hanna., M. (2018). *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection*. in *Computer*, *51* (8), 56-59, https://doi.org/10.1109/MC.2018.3191268

Moussaoui, M., Bertin, E., & Crespi, N. (2022). Telecom Business Models for Beyond 5G and 6G \ networks: Towards Disaggregation?. *2022 1st International Conference on 6G Networking (6GNet)*, 1-8, https://doi.org/10.1109/6GNet54646.2022.9830514

Rogalski, M. (2021). Security assessment of suppliers of telecommunications infrastructure for the provision of services in 5G Technology. *Computer Law & Security Review*, *41*, 105556. https://doi.org/10.1016/j.clsr.2021.105556