School of Computer Science and Mathematics

6100COMP Project

Final Report Submitted by

Jack Maloney

919070

Computer Security

Title

INFORMATION PRIVACY: AN ANALYSIS OF ORGANISATIONAL PRACTICES

Supervised by

Dr. Sorren Hanvey

Submitted on

5 May 2023

Contents

Abstract

This project explores the challenges organisations face in ensuring information privacy and compliance with global privacy laws. My research investigates the implementation of policies and procedures, the evolution of privacy practices over the last decade and the factors influencing individual attitudes and behaviours towards privacy. A mixed-method approach was employed, including a quantitative analysis of three large websites' privacy policies and the changes which they've undertaken in recent years and a survey, allowing for qualitative observations of user behaviour on these platforms.

The primary goal of this project is to address the lack of clarity surrounding information privacy on a global scale and I have created a comprehensive and user-friendly privacy compliance questionnaire that can be used by an organisation to assess and improve their privacy practices. The artefact is modular and adaptable to various industries and regions, addressing the global privacy landscape and the unique challenges which different organisations face.

The privacy compliance questionnaire is organised into four categories:

- Data Collection & Processing
- Data Storage & Security
- User Rights
- Third-Party Data Sharing

Including questions that cover the relevant areas of privacy laws on a global scale and provides a scoring system which allows an organisation to measure their compliance.

The results of the project indicate that the questionnaire has the potential to significantly improve organisations privacy practices, leading to better compliance with global privacy laws, increasing trust among users. By using the artifact, organisations can identify gaps in their privacy policies and procedures, reduce the risk of fines and legal issues, and enhance their overall privacy and security of user data.

This project has successfully created a valuable tool that addresses the challenges associated with information privacy and compliance on a global scale. The privacy compliance questionnaire provides a framework for organisations to assess and improve their privacy practices, contributing to the broader goal of protecting user privacy worldwide.

Future research in this field will include updating the artifact, as it will eventually be outdated. Consequently, future research could also focus on continuously updating the artifact to reflect the latest privacy-related developments and legal requirements. This may involve monitoring changes in legislation, incorporating new best practices and adapting the artifact to address emerging privacy risks and challenges.

Acknowledgements

I would like to express my sincere gratitude to those who have contributed to the successful completion of my project. Although this project is entirely my own work, I couldn't have done it without the emotional support and encouragement provided by my family, friends, and academic staff.

First, I would like to extend my appreciation to my family, who have been a constant source of emotional support and motivation. Their belief in my abilities and unwavering encouragement has been invaluable in helping me persevere through the challenges encountered during this project.

I am also very grateful to my supervisor, Dr. Sorren Hanvey whose continued guidance and insights have significantly contributed to the quality of this project. Sorren's expertise, constructive feedback, and ability to prod my brain has been essential in shaping my understanding of the subject matter and enhancing my research skills.

Additionally, I would like to thank my friends and fellow students for the stimulating discussions and camaraderie that have enriched my academic experience, these perspectives which I gained from my fellow students have contributed to my growth as a person and deepened my appreciation for the complexities of information privacy.

Finally, I would like to acknowledge the academic staff at Liverpool John Moore's University, who have provided a nurturing and intellectually stimulating environment in which to pursue my studies. This dedication to fostering academic excellence has left an indelible impression on me and has inspired me to continue learning and exploring the world of information privacy.

Introduction

The rapid growth of the internet and the increasing reliance on digital platforms for communication, commerce and information sharing have brought forth an array of challenges in the realm of privacy and data protection. Organisations worldwide have been grappling with the complexities of complying with privacy regulations while also trying to balance their business needs and the expectations of their users. This issue has been further complicated by the global nature of the internet and the varied privacy laws found across different jurisdictions.

The problem this project seeks to address is the lack of clarity and guidance for organisations in navigating the intricacies of privacy laws and data protection practices on the global scale. Many organisations, particularly those experiencing rapid growth and an expanding user base, may find themselves at risk of fines and penalties due to non-compliance with privacy regulations.

To tackle this challenge, this project aims to develop a privacy compliance questionnaire that organisations can use to assess their privacy policies, data handling practices, and overall compliance with relevant privacy regulations worldwide. By providing a practical tool for organisations to do this, my project hopes to minimise the risk of non-compliance, fostering a culture of data protection and transparency.

My report will outline the background and motivation for the project, followed by a comprehensive methodology that combines quantitative and qualitative research approaches. The results and findings of the project will be discussed, leading to the development of the proposed privacy assessment tool. Finally, the report will evaluate the project's effectiveness and suggest potential avenues for future research and improvements.

Literature Review

Introduction

Information privacy is a crucial aspect in modern society. Recently, individuals and organisations have been increasingly reliant on technology and the internet to store and transmit sensitive information. The rapid development of new technologies has led to increased concern regarding the protection of personal data, as well as the potential for breaches or any unauthorised access to sensitive information. In this literature review, I will explore the current state of research on information privacy, looking particularly at the practices which organisations have in place to ensure they're up to date with relevant privacy-related laws. This literature review will focus on key themes and trends in this field, examining the impact technology has had on information privacy, as well as the potential consequences which could arise from inadequate protection of Personally Identifiable information (PII).

This literature review is split into sections which I felt were relevant to the most critical aspects regarding information privacy.

Background

Information privacy has become an increasingly important concern in the age of digital technology and global connectivity. As organisations around the world handle vast amounts of personal data, ensuring the protection of this information isn't just a legal requirement but is also essential for maintaining user trust and confidence. The broad area of research leading up to this topic has focused on understanding the policies, procedures and practices organisations employ to safeguard information privacy.

Previous research in this field has explored various aspects of information privacy, such as data collection and processing, storage and security, user rights and third-party data sharing. While significant progress has been made in understanding the factors which shape organisational practices, gaps in knowledge remain, particularly in the context of rapidly evolving technologies and increasing public awareness of privacy concerns.

These gaps in knowledge need to be addressed to provide organisations with comprehensive guidance on how to navigate the complex landscape of information privacy regulations and best practices. As the consequences of non-compliance with privacy regulations can be severe, including substantial fines and reputational damage, it is crucial for organisations to have a clear understanding of their obligations and how to fulfil them.

Motivational

My project aims to address the gaps mentioned in the background section by conducting a thorough analysis of organisational practices pertaining to information privacy. By addressing these questions, my study will contribute to the existing body of knowledge on information privacy and can provide organisations with valuable insights into how they can enhance their privacy practices, navigate global privacy regulations, and ultimately foster a more secure and trustworthy digital environment.

The motivation behind this research stems in the increasing prevalence of data breaches, privacy violations and the widespread concern about personal data collection. In a digitally connected world in which vast amounts of personal information are collected, processed, and shared, organisations must take proactive steps to ensure the privacy and security of their users' data. The importance of this research is underscored by the consequences organisations face in the event of non-compliance

with privacy regulations or failure to protect user data adequately, which can include significant fines, reputational damage, and loss of user trust.

My project goes beyond the existing body of research by examining not only the policies and practices employed by organisations but also the evolution of these practices over the past decades and the factors that have influenced individual attitudes and behaviours towards privacy. By doing so, this seeks to provide a more comprehensive understanding of the current state of information privacy and the challenges faced by organisations when ensuring compliance with global privacy regulations and best practices.

Cross-cultural differences

Today, cultural values and norms are decisive to the way in which privacy is regarded. These cultural norms can be found to differ from two regions within one country, this is important as it tells us that there isn't going to be just one universal solution to privacy as different people have different concerns and needs. For example, it was found that 21% of white Americans wouldn't manage their privacy settings on social media sites, whereas 35% of Asian Americans, African Americans and Hispanic Americans had considered securing their privacy through methods like disguising their identities online. (Trepte) This paper's method involved a survey with a total of 1800 participants from classes in universities in Germany, the Netherlands, the United Kingdom, the United States and China, this is helpful for me as they already considered these differences in culture and accounted for it in their method by collecting survey data from all around the world. They found that the subjective importance of avoiding privacy risks showed a negative relationship toward one's willingness to have a public profile. In contrast to this, they found that the subjective importance of social gratifications was a positive predictor for the willingness to have an open profile. Individualism was also negatively related to the subjective importance of social gratification; this is because those from individualist cultures won't be as interested as social gratifications on social networking sites as those from a collectivist society or culture would.

These cultural norms are a factor which affects how people will manage their boundaries regarding privacy, people are socialised into norms for privacy in their culture, they may carry these norms with them to the internet, or at the very least these norms will play a part in how the idea of privacy is conceived to the user. This is interesting as it shows that there can be an innumerable number of factors which an organisation would need to consider regarding privacy for their users, especially for global organisations. For example, if someone is from a country which has lots of surveillance, they may be indifferent to not having privacy online – the same vice versa.

Another paper which I've seen mentions the relationship between the content of policies and that of privacy concern, the same goes for willingness to provide personal information and privacy concern, this paper outlines different determinants which can have an effect on an individual's privacy concern, these include things like geographical differences, cultural dimensions and different contextual or situational factors. This papers method involved using an online question to identify the relationships regarding the points I mentioned, this study was designed to test 7 research hypotheses and it was conducted online due to the low financial cost, implications, and response time. The survey respondents consisted of voluntary online users from Russia and Taiwan aged 18 and over, the questionnaire was translated to Chinese and Russian by a certified translation agency and posted to online forums, the respondents were split 250 from both countries. This paper was interesting as I have mentioned how cultural differences can impact a person's thoughts towards privacy, but I hadn't considered that there are different languages worldwide, and after seeing this paper say they used an online translation agency it makes sense to me. (Kuang-Wen Wua, 2012)

Polls regarding public opinion levels show that the level of concern and angst amongst Americans is rising surrounding privacy, people are becoming more perceptive to what's going on with their data and its leading to unrest. Since the 1990s, personal privacy has been one of the largest pressure points due to the rapid growth of technology, depersonalisation of the workplace, population growth and many other factors. This teaches us that there is a greater concern for privacy now more than ever and also that it is far from a new topic and is a debate spanning longer than my lifetime. The ultimate goal of this paper was to measure individual's concern about organisational informational privacy practices, this is useful to me as this paper is on a similar topic to mine, this paper's method featured a questionnaire, simply yes or no questions about privacy. This is important for me to consider as someone has already done a questionnaire regarding my topic. (Smith)

Many organisations gather, store, purchase or create information which links users' data to their identities, this data is known as personally identifiable information (PII). This information makes up the guts of many global firms, as these organisations gather PII, an individual's privacy is in the hands of these organisations and their privacy safeguards, despite these safeguards, breaches still occur. This paper is about categorising and assessing threats to Personally Identifiable Information in the USA, this paper's goal was to provide a classification system which provides some foundations for future research regarding PII breaches.

(Posey)

Steven Bellman and Eric J Johnson's study, "International Differences in Information Privacy Concerns: A Global Survey of Consumers," looks at regional variations in consumers' concerns about information privacy. The research involved asking consumers in eight different nations—the United States, Canada, France, Germany, Japan, Australia, South Korea, and Spain—about their attitudes around privacy invasion, their faith in organisations to secure that information, and their readiness to share it online. The methodology of the study includes online survey of consumers in 8 countries, the survey used a standardized questionnaire to collect data on privacy concerns, trust in organizations to protect personal information, and willingness to provide personal information online.

The study revealed that:

1. Customers' levels of concern about privacy invasion varied across nations, with German consumers having the highest levels of concern and Japanese consumers having the lowest levels.
2. Consumers in various nations expressed varying degrees of confidence in companies to safeguard their personal information, with Germans having the least and Canadians having the most.
3. Consumers in other nations varied in their readiness to divulge personal information online, with Americans being the most ready and Japanese consumers being the least.

The survey also discovered that consumer opinions toward privacy regulation varied between nations, with German consumers supporting privacy regulation the most and Americans supporting it the least. (Bellman)

Overall, this study provides some insight into how attitudes toward and concerns about privacy vary across cultural boundaries. It also suggests that a consumer's opinions and worries about privacy may be influenced by cultural and legal factors.

"How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?" This paper explores the attitudes and practices surrounding information privacy which

differ between young adults and the elderly. 683 people between the ages of 18 and 90 completed a survey which was used in the study. Participants' views toward information privacy and their knowledge of data protection policies were questioned in the study. The survey's findings revealed that the two age groups' views regarding information privacy and comprehension of data protection policies differed significantly from one another.

Younger adults are more likely to be concerned about the privacy of their personal data, whereas older adults are said to be less likely to be concerned, this paper proves that there is a need for more education and awareness regarding information privacy with older generations. (Hoofnagle et al., 2010)

Information Privacy law

Information privacy is one of the most central issues of modern times, there are hundreds of laws which pertain to privacy. For example, in America there are different statutes in each of the 50 states, from this we can learn how divisive this topic is, to better understand the laws surrounding information privacy, it is necessary to look to the origins and growth. Technology has played a large role in the story of the emergence of new laws regarding information privacy, this paper talks about new threats to privacy, including things like government census and records, for much of the nineteenth century, state governments didn't keep extensive records about citizens, this record-keeping rate began to rise. They go on to mention how the first census in America in 1790 asked only four questions, but this number grew to 142 questions by 1890, including questions about disease and such.

(Solove)

An extensive analysis of the current legal environment regarding to information privacy and its ramifications is presented in Daniel J. Solove's book Information Privacy Law. The concept of privacy is introduced at the start of the book, along with its importance in contemporary society. After this, it discusses about the many legislative frameworks placed in in order to protect people's privacy, including the Fourth Amendment, the Electronic Communications Privacy Act, and the General Data Protection Regulation of the European Union. The book goes onto explore the array of privacy rights which an individual is entitled to, including those in the workplace, online or those that arise when dealing with government organisation. The book closes by discussing the many court decisions which have had an impact on information privacy legislation.

This books methodology is based on an analysis of the historical progression of legislation regarding privacy, as well as a review of the pertinent legal documents, the books findings imply that the present legal environment around data privacy is complicated and constantly changing, which is crucial for people to be aware and stay aware of their rights and obligations when it comes to preserving their privacy. (Solove)

Law surrounding information privacy is an interrelated web of tort law. Information privacy is an issue of growing public concern and has been this way for a long time, information privacy is a priority in numerous state legislatures and the problems relating to information privacy can be frequently seen in the news, these laws are interesting as the issues can move as fast as the technology does which means the laws need to keep up.

"Consumer perspectives on information privacy following the implementation of the GDPR" by Wanda Presthus is a study that examines how consumers perceive and understand the impact of the General Data Protection Regulation (GDPR) on their information privacy. The GDPR is a regulation in the European Union (EU) that came into effect in May 2018, and it aims to strengthen and harmonize data protection for individuals within the EU.

The methodology of the study is a qualitative study that surveyed consumers in Norway, which is not an EU member but decided to implement GDPR on its own. The study used a standardized questionnaire to collect data on consumers' perceptions of the GDPR, their understanding of their rights under the regulation, and their attitudes towards the collection and use of their personal data by organizations.

The study found that:

1. The majority of consumers surveyed had a positive attitude towards the GDPR and felt that it protected their information privacy.
2. Consumers had a moderate understanding of their rights under the GDPR, but many were not aware of the specific provisions of the regulation.
3. Consumers reported that they felt more in control of their personal data after the implementation of the GDPR, but many still felt that organizations collect too much personal data and use it for purposes they did not understand.

The study also found that consumers were more likely to trust organizations that were transparent about their data processing practices and that provided clear explanations of how personal data would be used.

In conclusion, this study provides an insight into how consumers perceive and understand the impact of the GDPR on their information privacy, it highlights the importance of transparency and clear explanations in building consumer trust on how personal data is being used by organizations. (Presthus & Sørum)

Information Privacy in cyberspace transactions

Internet self-efficacy can have a role in influencing the frequency in which online transactions take place due to the complex nature of the internet technology, users need to understand how to search and find what they're looking for online and be able to follow through with the transaction, this feeling of comfort regarding navigating the internet is what's known as internet self-efficacy. Syed H. Akhter found that concerns for privacy are described as to have negative impacts on the frequency of online transactions, this makes sense as customers may be more hesitant to purchase something from a company who had a data breach in the past. Also, that the direct effect of internet-self efficacy and internet involvement on the frequency of online transactions is positive. This paper used a structural equation model to test the hypotheses. (Akhter)

Consumers need to have trust in their online transactions in order for e-commerce to progress, lots of factors can weigh into what makes someone trust an online vendor, things like the vendors reputation, the consumers perception of privacy or even where they're from can play a role in them deciding whether or not to make that online purchase, 'Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security' by Ramnath K. Chellappa covers this well, the point of this paper was to bring to light that the importance of studying online trust was being understated by many recent studies, and that there is overwhelming evidence that trust in the online environment is a crucial aspect of electronic commerce. This paper used a survey to test its hypotheses, Ramnath found that while perceived security of E-Commerce transactions, perceived privacy's affect on trust is mediated by perceived security. (Chellappa)

'An Extended Privacy Calculus Model for E-Commerce Transactions' The privacy calculus model (PCM), developed by Acquisti and Grossklags in 2005, serves as the basis for the Extended Privacy Calculus Model (EPCM) presented in this work. The EPCM aims to offer a more thorough knowledge of the elements that affect a user's choice to conduct online transactions. The approach is built on three primary elements: transaction advantages, privacy benefits, and privacy risk. The authors looked at how these elements affected a user's decision to do e-commerce transactions. The authors discovered that a user's perception of privacy risk, the advantages of privacy, and the rewards of the transaction all significantly influenced the user's choice through a study of more than 1,000 participants.

The authors also discovered that a user's perception of the privacy risks and benefits had a greater influence on a user's decision than the perceived transaction benefits, the authors concluded that the EPCM provides a more comprehensive understanding of the factors influencing a user's decision to engage in e-commerce transactions. (Dinev et al., 2006)

Organisational practices

H. Jeff Smith and Sandra J. Milberg's study, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," looks at people's worries about organisational practises including the gathering, using, and disclosing of personal information. According to the study's poll of American consumers, people's levels of worry about various organisational activities relating to privacy vary.

An American consumer survey was included in the methodology of this study. The author used a standardised questionnaire to gather information on people's worries about various organisational privacy practises, such as the gathering of personal information for targeted advertising and the sharing of personal information with third parties.

The study found that:

1. Different organisational privacy practises raised different levels of consumer concern, with the collection of personal information and its use for targeted advertising being the most alarming practises.
2. Consumers' levels of willingness to divulge personal information in exchange for hoped-for advantages, such as discounts or personalised services, varied widely, with the government and financial institutions receiving the most trust and Internet-based businesses receiving the least.

The study also discovered that factors like consumers' level of trust in businesses and their own personal traits, like age and education, affected their privacy concerns.

The study concludes by suggesting that individual characteristics and trust in organisations play a role in shaping consumers' privacy concerns. This study offers an insight into how individuals' concerns about organisational practises related to privacy vary. (Smith)

A study by Clay Posey categorises and evaluates threats to personally identifiable information (PII) in the USA. It is titled "Taking Stock of Organizations' Protection of Privacy: Categorizing and Assessing Threats to Personally Identifiable Information in the USA." The study focuses on the businesses that gather and use personally identifiable information (PII) and the various privacy threats that these businesses may present.

The study's methodology entails interviews with professionals in the fields of privacy and security as well as a review of academic literature and news articles. Data breaches, cyberattacks, and insider threats were among the threats to PII that were examined in the study, which also looked at how these threats affected people's privacy.

The study found that;

1. Inadequate security measures or human error are frequently to blame for data breaches, which are the most frequent threat to PII in the United States, according to the study.
2. Malware and other cyberattacks like phishing pose a serious risk to personally identifiable information.
3. Individuals' privacy may also be jeopardised by insider threats, such as staff members handling PII improperly.
4. While it is the responsibility of American businesses to safeguard personally identifiable information (PII) from threats of this nature, many do not do so adequately.

The study also discovered that although the US Government has implemented some regulations to safeguard people's personally identifiable information (PII), the regulatory environment is complicated and the enforcement is frequently insufficient, leaving PII vulnerable to threats. (Posey)

In conclusion, this study sheds light on the many threats to PII in the USA and how they arise. It also draws attention to the discrepancy between organisations' obligations to safeguard PII and the legislative and enforcement framework that exists today.

‘A scoping assessment of the literature on organisational privacy culture and climate is included in the publication "Organisational Privacy Culture and Climate: A Scoping Review." Using the databases PubMed, Web of Science, and PsycINFO, the authors carried out an organised search of the literature. Search results were restricted to English-language publications released after 2000. The authors found a total of 27 studies that addressed the climate and culture of organisations regarding privacy, and they categorised the studies based on their research methodologies. The research on organisational privacy culture and environment is scarce and dispersed, with the bulk of studies being qualitative in character, according to the authors.

The importance of top-down leadership, the value of trust and communication, the necessity of privacy rules and processes, and the necessity of staff education and training were some of the themes that the writers found in the literature. The authors concluded that further study on organisational privacy environment and culture is necessary. (L. H. Iwaya, 2022) I can benefit from this scoping review since it gives me a thorough overview of the literature and research on organisational privacy culture and climate. You may use it to comprehend the existing level of knowledge on the subject and spot gaps in the body of information that require filling. Additionally, it can serve as a foundation for the creation of plans and initiatives aimed at enhancing the privacy environment and culture inside an organisation.

“Examining the intended and unintended consequences of organisational privacy safeguards” This study analyses how organisational privacy protections affect both intended and unforeseen results. A qualitative examination of case studies from several organisations in various industries served as the technique. The results showed that businesses with strict privacy protections suffered from both intentional and unforeseen impacts. Increased client confidence, better data security, and a lower chance of data breaches were all intended outcomes. Unintended repercussions included higher prices, more complicated data administration, and trouble tracking client preferences. Overall, the results indicate that businesses should carefully examine the effects of putting in place privacy measures. (Parks, 2017)

Information Privacy and Cyber Crime

“Handbook of Research on Cyber Crime and Information Privacy" is a book by Maria Manuela Cruz-Cunha which provides us an overview of the latest research regarding cyber-crime and information privacy. The book covers an array of topics, including the types of cybercrime, the motivations behind cybercrime, and the methods used to prevent it. The book’s methodology is primarily based on a review of existing literature and research in the field. The book finds that cybercrime is a rapidly growing problem which has a need for more research and collaboration between law enforcement, businesses, and academia to combat it. This book could be useful for researchers, policymakers, and practitioners in the field of cybercrime and information privacy, as it provides a comprehensive overview of the current state of research in this area. (Cruz-Cunha)

In the article "Cyber risks to health information systems: A systematic evaluation," the most significant dangers are identified after a review of the relevant literature on the subject. This paper employed a methodology based on a systematic literature search and the selection of articles according to predetermined standards. The review's conclusions highlight the enormous risk that cyber-attacks pose to health institutions, with numerous cases of data loss and theft as well as unauthorised access and manipulation. In order to lower the danger of cyber threats, the authors also listed a number of potential security concerns and precautions that health information systems should take. This article is helpful since it sheds light on the possibility of health-related cyberthreats. (Luna et al., 2016) This review is useful for understanding the scope and types of cyber threats to health information systems, so that appropriate countermeasures can be put in place to protect them.

Conclusion

In conclusion, this dissertation's literature study offers a thorough analysis of the numerous aspects of information privacy in organisational practises. Organizations must have strong security measures in place to guard against malicious assaults and data breaches, as highlighted in the section on cybercrime. To secure the security of personal information, the section on organisational practises highlights the significance of putting in place efficient privacy policies and procedures inside a business. The section on cultural variations in privacy emphasises the significance of taking cultural norms and values into account when putting privacy practises and policies in place. To guarantee the protection of personal information, businesses must abide by all applicable rules and regulations, as shown in the section on information privacy law, then, the section on information privacy in cyberspace transactions highlights the need for organizations to implement secure and transparent data handling practices in the digital age. Overall, the literature reviewed emphasizes the importance of organizations being proactive in their approach to information privacy by implementing effective policies and practices, staying informed of the latest developments in the field, and considering cultural and legal considerations.

Aims and objectives.

The overall aim of my project is to assess the measures which organisations are taking to safeguard user privacy, I will examine the evolution of these practices and find out how exactly they've changed over the last decade. This project additionally seeks to investigate how a user's attitudes towards privacy have evolved over the past decade. I believe that examining both the user and organisational side of information privacy over the past decade will provide a holistic view of privacy in the current context of the ever-changing cyber-security landscape.

Research Questions

These questions set the scope for my project, and clearly define what my research is seeking to achieve:

1. "How do organizations around the world implement policies and procedures for ensuring information privacy and what factors influence their effectiveness?"
2. "How have organisations' policies and practices for ensuring information privacy evolved over the past decade, and what factors have driven these changes?"
3. "How have individual attitudes and behaviours regarding information privacy changed over the past decade, and what factors have influenced these shifts?"

In order for me to answer these questions, I believe there are some other questions which I need to answer which will help me with my project, these include:

- What impact do data privacy regulations have on organisational practice regarding user personal information?
- How clearly does an organisation communicate their privacy policies to their employees, stakeholders, or users?
- To what extent are organizations aware of and prepared for information privacy breaches?
- What is the role of privacy-enhancing technologies in terms of ensuring information privacy within an organisation?

Objectives

My objectives will help me achieve the aims of this project and will be vital when it comes to my research, these questions include:

- Review the privacy policies from three organisations, examine the changes these have went under during the last decade.
- Make my own or find a relevant questionnaire pertaining to privacy, allowing me to evaluate how a user's decisions might have changed over the years.
- Analyse data collected from the privacy policies and users, determining the changes.

Research problem

The computing problem which I seek to address with this project is the prevalent lack of clarity surrounding global privacy regulations. As organisations grow and their user base expands, they can become vulnerable to legal repercussions, such as fines, due to non-compliance with privacy laws. An example of this would be Discord facing an $830,000 fine for GDPR violations, and Apple faced similar issues for not adhering to EU legislation concerning USB-C cables.

To tackle this issue, I will develop a comprehensive set of questions which organisations can use to self-assess their privacy policies and data management practices. By engaging with these questions, organisations can identify potential areas of non-compliance and take necessary actions to avoid fines and enhance the security of their user data. The goal of this project being to empower organisations with a practical tool which helps them navigate the complex landscape of privacy regulations on a global scale and foster a more secure and privacy-conscious digital environment.

Methodology

This project aims to address the issue of clarity for organisations when handling user data and complying with regulatory requirements, various factors need to be considered in this context, and I think a mixed-methods approach would be beneficial here, to help me gain a comprehensive understanding of the subject.

In the quantitative aspect of the research, an objective and systematic assessment of privacy practices will be conducted by analysing the policies of three prominent websites that handle a significant amount of user data, this analysis will offer valuable insights into organisational approaches to privacy and data management, and how they've changed in the past decade.

For the qualitative component of this project, observations will be made as to how individuals protect their privacy when using these websites. This approach will provide a deeper understanding of the balance between user preferences for privacy protection and the extent to which companies collect and store their information.

By combining both quantitative and qualitative research methods, this project will yield a well-rounding understanding of privacy-related practices and challenges faced by organisations and users alike. This comprehensive perspective will inform the development of a practical tool which can be used to help organisations navigate complex privacy regulations and improve their data management practices.

Quantitative Research: Privacy Policy Analysis

In my Quantitative research I will be evaluating the privacy policies of Facebook, Discord and TikTok, to look at how they've changed over the years.

My research will be based around GDPR as this provides me with a comprehensive set of guidelines for data protection and privacy practices, it's based around the UK's Data Protection Act in the form of the structure of the research, for each organization I will split up the privacy policy into sections covered by GDPR and see how they've changed over the years.

The structure is as follows, I will start with

- Data Collection and processing
- Data storage and security
- User rights
- Third-party data sharing

Looking at how these have changed for these organisations over the years will give me a comprehensive understanding of privacy practices and their evolution. After completing the sections above, I will also include a section in which I can discuss any other relevant regulations which have had an impact on the organization and/or their privacy policy.

Qualitative research: Privacy survey

For my qualitative research I will conduct a short survey created on google forms, I will then send this survey around to get some responses, my survey is regarding information privacy from a consumer standpoint, each of these questions are useful to my research and provide me with insights into a consumer view towards privacy. I have explained my choices for the questions below.

1. “Have you become more concerned about protecting your privacy online in the past few years?”

This question is related to my third research question about the changes in individual attitudes and behaviours regarding information privacy. By understanding if people have become more concerned about protecting their personal information online, I can gauge the general trend in privacy attitudes and identify potential factors that might have contributed to these changes.

2. "Do you read privacy policies or terms of service agreements before using a new website or app?"

This question examines the level of user engagement with privacy policies and terms of service, which is an important aspect of the relationship between organizations and individuals in the context of privacy. Responses to this question can help me understand how much users care about their privacy and the extent to which they trust organizations with their personal information.

3. "Do you adjust your privacy settings on social media platforms or other online services to limit the amount of data they collect about you?"

This question helps explore the proactive measures individuals take to protect their privacy. It can provide insights into the extent of user awareness and how willing they are to take action to safeguard their information, which can be compared to organizational practices.

4. "Have you ever deleted a social media account or other online service due to concerns about privacy or data collection?"

This question assesses the impact of privacy concerns on user behaviour. Responses can reveal the severity of privacy concerns and their influence on individuals' decisions to discontinue the use of certain services, providing an indication of the significance of information privacy in user choices.

5. "Have you ever used a virtual private network (VPN) or other tools to protect your privacy online?"

This question explores the use of privacy-enhancing technologies by individuals. It helps identify the extent to which users employ additional tools to protect their privacy, which can reflect their concerns and awareness of privacy issues.

6. "Have you ever experienced a privacy or data breach which impacted your personal information?"

This question is related to the prevalence of privacy breaches and their impact on individuals. Understanding the extent to which respondents have experienced data breaches can shed light on the effectiveness of organizational practices and the consequences of privacy violations.

7. "Have you ever filed a complaint or taken legal action related to a privacy or data protection issue?"

This question assesses the extent to which individuals are willing to act against organizations for privacy or data protection issues. It provides insights into the level of public awareness and concern about privacy rights and can also serve as an indicator of the effectiveness of existing privacy regulations and enforcement mechanisms.

Privacy Policy Analysis:

Facebook

Before delving into the privacy policy analysis of Facebook, it's essential to provide a brief overview of what this section entails. The objective of this analysis is to examine Facebook's privacy policy, a significant player in the digital space, to better understand its data handling practices, compliance with various privacy regulations and how these have evolved.

In this section I will split Facebook's privacy policy into the critical components of privacy seen through this project, these include data collection and processing, data storage and security, user rights and third-party data sharing. By analysing these elements, I aim to gain insights into the company's privacy practices and see how these have changed over the years.

Introduction

Information Privacy is one of the most frontal issues of the twenty-first century, for both individuals and organisations alike. In today's society, where vast amounts of personally identifiable information is being collected and processed. Facebook, as one of the largest social media platforms in the world and having spent so long at the peak of relevance, has a massive role when it comes to shaping the online landscape, this is because any changes which Facebook make to their policies are going to impact billions of users.

The purpose of this research is to analyse Facebooks approach when it comes to information privacy, and to evaluate the effectiveness of its policies and practices ensuring user privacy.

To view Facebook's older privacy policies, I will make use of the Wayback machine internet archive. I have split the privacy policy into sections which are what makes up the policy and will discuss the changes that've occurred over the years.

(*Internet Archive*)

Data Collection and Processing

In the early years of Facebook, the company collected relatively limited information about its users, but there was still a range of user data collected for varying purposes, including personalising the user experience and serving targeted ads. This data was collected without the consent of the user, and the user would often unknowingly share sensitive information. As time went on, Facebook expanded the amount of data that it collects, including information about user's offline activities.

There were big changes made to Facebook's data collection practices in 2014, in light of the Cambridge Analytica scandal, Facebook introduced new policies limiting the amount of data which third-party apps could collect, and they made it easier for the user to understand what data specifically was being shared with these apps.

Another noteworthy change would be the one that came with the increased regulatory scrutiny in 2018 when the General Data Protection Regulation (GDPR) was introduced in Europe, this gave users more control over their data and required explicit consent for certain types of data to be collected and processed. Facebook had to change their privacy policy because of this, leading to further limits being placed on the data collected from users and increased transparency about what data was being collected.

(*Facebook GDPR*)

Facebook's data collection policy has changed significantly in the past decade, this is both a result of increased concern towards privacy and increased regulation, these changes reduce the amount of data which Facebook collects, and provides the user with more control over the data they share with the company, but Facebook's data collection practices have only grown more expansive and sophisticated, due to the introduction of tracking technologies and Facebooks acquisitions of companies like WhatsApp and Instagram, which allowed them to expand the type of data they're collecting.

Data storage and Security

Facebook launched in 2004, at this time they were storing all user data on servers which were in the United States. As the platform grew, Facebook's server infrastructure also grew to accommodate the increasing user base and ensure fast and reliable services. In 2010, Facebook opened its first international data center in Prineville, Oregon

(*Facebook double size of Data Center* 2010)

Facebook has also continued to expand its server infrastructure. In 2020, Facebook announced it had opened a new data center in Singapore, bringing the total number of data centers to 15.

(Clay, 2021)

When it comes to data security, Facebook has made numerous changes over the years to improve the protection of user data. In 2011, Facebook implemented HTTPS encryption for all pages to help prevent unauthorized access to user accounts.

In 2018, Facebook experienced a major data breach, resulting in millions of users' personal data being exposed. In response, Facebook implemented new security measures, including restricting data access for third-party apps and implementing a "Security Checkup" feature to help users review, update and improve the security of their account.

(*An update on the security issue*, 2019)

When GDPR came into effect in 2018, Facebook updated its privacy policy and terms of service to comply with the new regulations. Facebook stated that they were committed to protecting user data and that it had implemented technical and organizational measures to ensure data security and protect against unauthorized access.

Overall, there have been a lot of changes made by Facebook over the years to improve data security and storage, including implementing HTTPS encryption, improving security measures following the 2018 data breach, and expanding its server infrastructure. The company has also taken steps to comply with GDPR and other data protection regulations and has demonstrated a commitment to protecting user data.

User rights

Facebook didn't always offer the same amount of user control toward their own privacy, and as such have increased the control that users have over their personal data, now offering a range of privacy settings.

This side of the policy also saw changes in 2012 and 2014, giving users greater control over their personal data, and introducing tools to help users understand what data was being shared with third-party apps, giving users the ability to revoke access.

(Welch, 2014)

Changes after the GDPR: In 2018, the European Union's General Data Protection Regulation (GDPR) came into effect, which introduced new requirements for data protection and privacy. In response, Facebook made additional changes to its privacy controls and settings to give users even greater control over their personal data. These changes included the right to access, delete, and transfer their data, and the right to object to the processing of their data for certain purposes.

(*Facebook GDPR*)

Third-party data sharing

In the past, Facebook had a more open approach in terms of sharing data with third-party companies, allowing third-party developers access to user data, in recent years however Facebook have tightened their policies and reduced the amount of data that they share with third parties.

In 2012, Facebook made significant changes to their data sharing policies in response to the growing concern surrounding privacy, this saw the introduction of new controls which could be used to limit the amount of data which third-party developers can access, also introducing new review processes put in place to ensure that apps which access user data comply with Facebooks policies.

Facebook made further changes in 2014 as a response to the Cambridge Analytica scandal, reducing the amount of data available through Facebook's API, and implementing more controls to further limit the amount of user-data which third-party developers can access including things like allowing users to log in to third-party apps anonymously.

(Welch, 2014)

In 2018, the European Union's General Data Protection Regulation (GDPR) came into effect, which introduced new requirements for data protection and privacy. In response, Facebook made additional changes to its data sharing policies to ensure that it was following GDPR, including limiting the amount of data that it shares with third-party companies and organizations.

Regulations

Facebook was fined $5 billion by the US Federal Trade Commission for privacy violations related to the Cambridge Analytica scandal. This scandal led to Facebook being more heavily regulated, including GDPR in Europe and the California Consumer Privacy Act (CCPA) in the United States. As a result of this, Facebook has made changes to its privacy policies and practices. For example, improving transparency around data usage and providing users with more control over their personal data. This means that the Cambridge Analytica scandal had a significant impact on Facebook's privacy practices.

Heatmap of Facebook's privacy policy

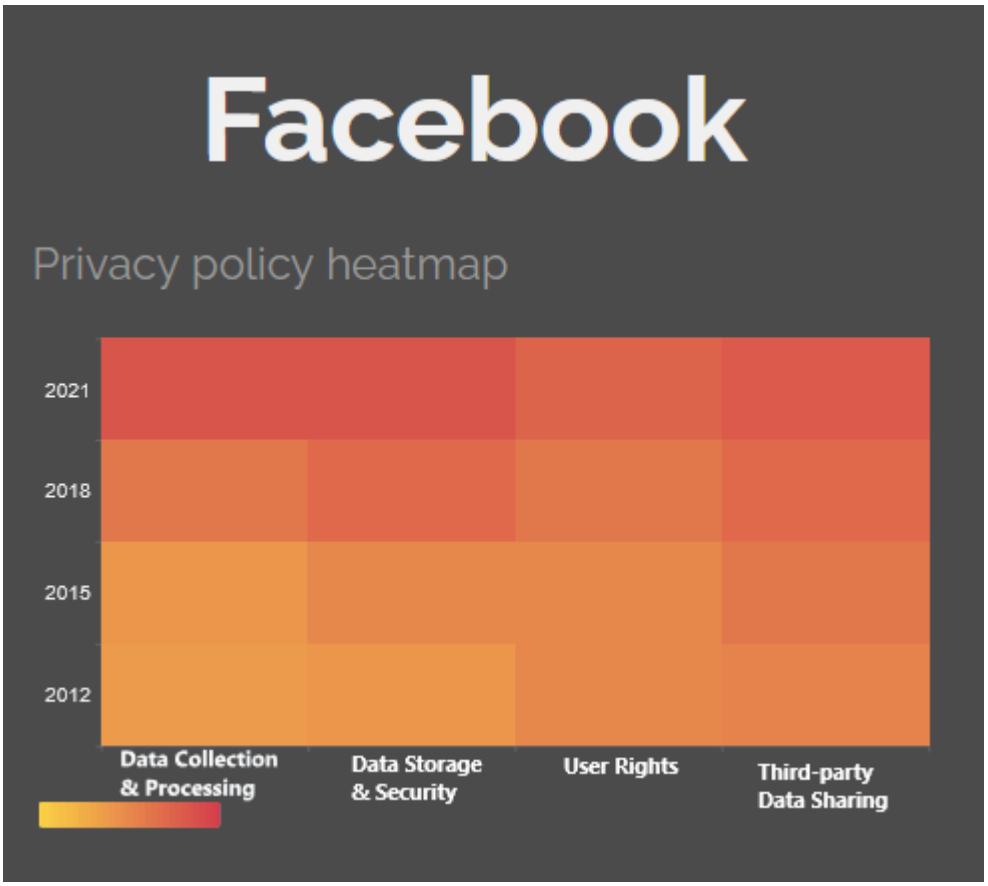


Figure 1

Facebook's data collection and processing practices have been a point of concern for many years, this is reflected in the heatmap. In the earlier years (2011-2014) Facebook's data collection and processing practices were relatively unregulated, with little restrictions as to how the company could collect and use user data. (Vedova & Technology, 2022)

However, as more public awareness of Facebook's practices grew, the company began to face more scrutiny from regulators and lawmakers, this is reflected in the increase in the score from 2015 onwards. Facebook has made some changes to its data collection practices over the years, such as giving users more control over what data they share and how it's used, but these changes have been incremental rather than transformative. (Shore & Steinman, 2015)

Facebook has faced several high-profile data breaches over the years, this is also reflected in the heatmap. The score for this category is relatively low in the early years (2011-2014), reflecting the fact that Facebook's data storage and security practices weren't yet under much scrutiny. However, as data breaches became more common and Facebook faced more regulatory pressure to improve its security practices, the score for this category began to increase. In recent years, Facebook has made some changes to its data storage and security practices, such as implementing stronger encryption and increasing its investment in cyber security, but it remains to be seen whether these changes will be sufficient to protect user data from future breaches. (Mazaji, 2016)

Facebook has faced criticism for its handling of user data and privacy over the years, this is reflected in the heatmap. In earlier years, Facebook's user rights score was relatively low, reflecting the fact

that users had few options for controlling how their data was used and limited recourse if their privacy was violated. However, as public awareness of these issues grew and Facebook faced more pressure from regulators and advocacy groups, the company began to make changes to improve user rights. For example, Facebook introduced more granular privacy controls and created a dedicated privacy policy to explain its data practices to users. However, some critics argue that these changes don't go far enough, and that Facebook still has a long way to go to protect user rights. (Esteve, 2017)

Facebook has been criticized for its data-sharing practices over the years, and this is reflected in the heatmap. In the earlier years. Facebook's score for this category was relatively low, reflecting the fact that the company had few restrictions on how it could share user data with third parties. However, as concerns about data privacy grew and regulators began to investigate Facebook's data-sharing practices, this score began to increase around 2015, with the Cambridge Analytica scandal being the catalyst. Facebook has made changes to its data-sharing practices over the years, such ass limiting the amount of user data that app developers can access and requiring more transparency about how user data is shared, but some critics argue that these changes don't go far enough to protect user privacy.

Discord

Comparative & Chronological

Introduction

Discord is a chat and voice communication platform that has gained popularity in recent years, among gamers and communities for content creators, Discord is relatively new, having only been in existence for a few years, despite the relative youth of the platform, Discord quickly established itself as a major player in the online communication space, and has had to navigate several privacy challenges and regulatory requirements. In this section of my research, I will examine the evolution of Discord's privacy policy and practices, seeing how much has changed since the birth of the company, and examining the factors which influence these changes. I think it is worthwhile to include Discord as, compared to Facebook which has been around for much longer, Discord was launched in 2015 and I think it will prove useful to see how a newer social media giant has had to adapt their practices and policies.

Data collection and processing

In the beginning, Discord's collection of user information was focused on providing the chat and voice communication services, meaning that Discord primarily collected data like usernames, email addresses and IP addresses.

Big changes occurred in 2018 because of GDPR coming into effect, bringing new requirements for data protection and privacy, in response Discord needed to update their privacy policy to ensure it was in compliance with GDPR, though it seems the company struggled with this, as they received a fine of €800,000 euros for failing to comply with several of the obligations of GDPR.

(*Privacy policy update and GDPR FAQ – discord*)

Discord has continued to change their practices surrounding data collection in response to the changing concerns around privacy, regulations and even fines. The company has implemented more robust security measures to protect users' data, giving the users greater control over their privacy settings and the information they share with the company.

Discords practices surrounding data collection of user information has undergone significant changes since the launch of the company, these changes help reduce the amount of data that discord is collecting and gives users greater control over the information they share with the company.

(*Privacy policy*)

Data storage and security

Discord was only launched in 2015, at this time they were storing all user data on servers which were in the United States, as the platform grew, Discord expanded its server infrastructure to accommodate the increased user base and to ensure fast and reliable service.

In 2016, Discord began using Cloudflare, a content delivery network and security service, this helped improve server stability and protect against Denial-of-Service attacks.

(*Case study: Discord*)

In terms of data security, Discord has made numerous changes over the years to improve the protection of user data. 2017 saw Discord implement two-factor authentication to help prevent

unauthorized access to user accounts. In 2018, Discord introduced an optional feature for server admins called “Audit logs” which would act as a log of actions taken by server administrator, to improve accountability and security.

(*API docs for bots and developers*)

When it comes to data storage, discord continued to expand their server infrastructure to accommodate the growing user base. In 2020, Discord announced that it had opened its first data center in Europe, located in Frankfurt, Germany. This move was aimed at improving service performance and reducing latency for users situated in Europe, whilst also complying with the local legislation regarding data protection.

Overall, Discord has made numerous changes over the years to improve data security and storage, including implementing 2FA, introducing Audit Logs, and expanding its server infrastructure. The company has also taken steps to comply with GDPR and other data protection regulations and has demonstrated a commitment to protecting user data.

User rights

In 2015, when Discord was launched, users had limited control over their privacy settings, users could set their online status to online, idle or offline but there weren’t many options for controlling the data which was being shared with the company.

When GDPR was introduced in 2018, Discord needed to update their privacy policy to give users more control over their data, this came to shape in the form of the ability to view, modify, or delete the data that Discord has collected on them.

(*Privacy policy update and GDPR FAQ – discord*)

In more recent years, Discord has continued refining the user control aspect of their privacy policy to provide users with even greater control over their data. An example of this could be the features that were implemented to allow a user to control who can send them friend requests and messages.

Overall, Discord has made significant efforts to increase the user’s control over their privacy and the data which they share with the company. These changes were driven by both user demand and regulatory requirements. These changes helped establish Discord as a company that prioritises user privacy and data protection.

Third-Party Data Sharing

Towards the beginning of Discord, the company’s sole focus was to provide a chat and voice communication program for its users, and because of this the company wasn’t engaging in significant third-party data sharing practices.

In more recent years, since GDPR was introduced in 2018, Discord had to update its privacy policy to give users greater control over how their data was shared with third parties, the company also clarified that it wouldn’t sell users’ personal information, and only shared user data with third-party services when necessary.

(*Privacy policy update and GDPR FAQ – discord*)

Discord has continued to refine its policies regarding third-party data sharing, the company has implemented more stringent security measures to protect users' data due to regulatory pressure and significant user growth since the launch of the platform.

Overall, Discords policies surrounding third-party data sharing have evolved over the past few years to prioritise privacy and to comply with regulatory requirements. The company has also made it clear that it is committed to protecting its users' personal information and limiting the sharing of this information with third parties.

Regulations

One regulation which has had an impact on Discord's privacy practices is the Children's online privacy Protection Act (COPPA) in the United States. This is a federal law which regulates the collection and use of personal information from children under the age of 13. Discord has implemented measures to ensure they comply with COPPA, such as requiring users to confirm that they're over the age of 13 when signing up for an account. Discord has also implemented additional measures to protect children's privacy, such as limiting the amount of personal information that can be shared in public chat channels.

Another regulation which has had an impact on Discord's privacy practices is the European Union's ePrivacy Directive, which regulates the use of cookies and other tracking technologies. Discord updated their privacy policy and practices to comply with the ePrivacy Directive, such as providing users with more control over cookie settings and requiring consent for the use of cookies.

Heatmap of Discord's privacy policy

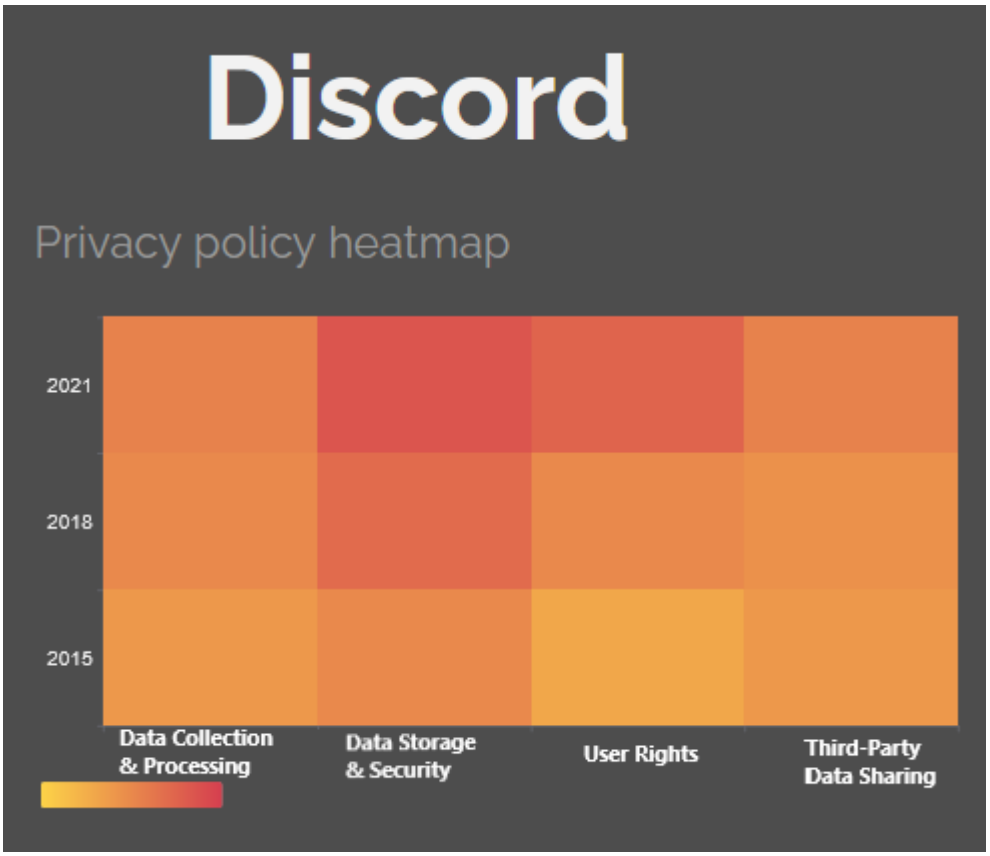


Figure 2

Discord's heatmap begins in 2015 as this was when the company was launched.

Discord began as a gaming-focused chat app, and in the early years there was very limited data collected beyond basic account information. However, as Discord expanded to other communities and features (i.e. voice chat), more data began to be collected and processed. The increase in data collection and processing in the later years follows this trend. (Discord, *Privacy policy*)

Discord has always had a focus on security, and in fact was originally created as a more secure alternative to existing chat app. As discord has grown, they have continued to prioritise data security, and storage, adding features like two factor authentication and end-to-end encryption. This is reflected in the increasing scores in this category over time.

Discord has had a somewhat mixed track record when it comes to user rights. In the early years, there was little focus on privacy or user control over their data. Though in more recent years Discord has made efforts to give users more control over their data and privacy settings, resulting in a higher score for the later years. (Discord, 2023)

Discord has generally been very cautious about third-party data sharing; this is also reflected in the consistently low scores in this category over time. In more recent years however, its worth mentioning that Discord has begun exploring more integrations with other services, which results in increased third-party data sharing in the future, which explains the slight increase in score for the last column.

TikTok

Comparative & Chronological

Introduction

TikTok is also a relatively new social media platform, TikTok was launched in 2016, meaning that it hasn't been around for a decade just yet. In 2017, TikTok's parent company ByteDance acquired Musical.ly, another social media platform which was popular amongst teenagers. This acquisition helped to increase TikTok's user base and expand its reach.

Data collection and processing

Much like its peers, TikTok collects a significant amount of user data. In the earlier days of TikTok, its data collection practices were relatively basic and were limited to things like users' names, email addresses and phone numbers. As the platform grew, TikTok's data collection has become more sophisticated. Today, TikTok gathers a wide range of data on its users, including their location, device information and even things like browsing history and even facial recognition data.

TikTok uses the data which it collects to improve its app and provide personalized content to users. The platform's algorithms analyse user data to identify emerging trends and suggest content that it likely to be of interest to the individual users, TikTok also uses user data to serve targeted advertising.

TikTok uses sophisticated algorithms to analyze the data it collects from users and make recommendations for content based on their interests and behavior. This includes making use of machine learning to analyze user behavior and preferences. In response to growing concerns about data privacy, TikTok has made efforts to increase transparency around its data collection practices and give users more control over their data, an example of this is how the app now allows users to download a copy of their data and provides a clear explanation of its data processing practices in the privacy policy.

TikTok has faced regulatory scrutiny in numerous countries over its data collection and processing practices. In the United States, the company was fined by the Federal Trade Commission for breaching COPPA. TikTok has also faced scrutiny from lawmakers over its ties to China and concerns about data security.

Data storage and Security

Although TikTok is a relatively new platform, there are still some notable changes in TikTok's data storage and security in the years since its launch.

TikTok's parent company, ByteDance was initially storing user data on servers located in China, though this raised concerns among users and lawmakers, due to China's reputation for strict online censorship and surveillance, in response to these concerns, TikTok announced in 2019 that it would store user data in the United States and Singapore and establish a new data center in India to serve their users.

(TikTok, 2019)

In addition to changing the locations of their data storage, TikTok took additional steps to improve data security measures. In 2019, the company announced that it had hired a team of security experts to help expose and address vulnerabilities in the systems. TikTok also implemented multi-factor authentication and other security measures to help protect user accounts from unauthorized access.

In 2020, TikTok announced the opening of a "Transparency Center" in the United States. The center is designed to provide more information about TikTok's data collection and security practices and to allow outside experts to review these practices and provide feedback.

(*Transparency center homepage meta* 2021)

Overall, TikTok has made significant changes to their data storage and security practices in the seemingly short time since the platform's launch. There are still ongoing concerns regarding how user data is collected, used, and protected, it is of utmost importance that TikTok continue to be transparent about its practices and are ready to take steps to mitigate any issues which might arise.

User Rights

TikTok's privacy policy was introduced in 2019, this policy outlines how the company collects, uses and protects user data. TikTok's privacy policy includes several provisions which are aimed at protecting user privacy. For example, the company states that it will only collect and use user data for specific purposes, such as providing and improving its services, and that it will obtain a user's consent before sharing their data with third parties.

(TikTok, 2019)

TikTok now also allows for users to control certain aspects of their privacy settings, such as who can view their profile and videos, and whether their account is public or private, TikTok has also implemented various features to help users protect their privacy, such as the ability to filter comments and restrict direct messages from other users.

Although TikTok is still a new platform when compared to a giant of yesteryear such as Facebook, though there have still been positive developments when it comes to protecting user privacy and giving users more control over their personal information. It is important for TikTok to remain transparent about its practices and to stay up to date with evolving privacy regulations and best practices.

Third-party data sharing

TikTok's approach to sharing user data with third parties has undergone significant changes in the past few years, one key development came with the introduction of TikTok's privacy policy in 2019, which clarified how the company handles user data and sharing with third parties.

TikTok has faced scrutiny over their data sharing practices. In 2020, the company was facing a potential ban in the United States due to rising concerns over its ties to the Chinese government and their pervasive data collection practices. As a result, TikTok announced plans to form a new company, TikTok Global, which would be based in the US and be majority-owned by American investors.

Under the current policy, TikTok states that they may share user data with third-party service providers which help the company operate and improve its services, such as data storage and processing companies, and with partners who work with TikTok to provide joint services, promotions, or research activities.

TikTok also states that it may share user data in response to legal requests or to protect its own rights or the rights of others. Additionally, TikTok may share data with third parties in connection with a merger, acquisition, or sale of assets, subject to the appropriate confidentiality measures.

Regulations

In 2019, TikTok came under scrutiny over their data collection practices, though the backlash was particularly relating to TikTok's practices for handling data from minors. In response, TikTok made several changes to their policies, including disabling direct messaging for users under the age of 16 and making user accounts for minors private by default.

Another regulation which has had an impact on TikTok is the Children's Online Privacy Protection Act (COPPA), this is a federal law in the United States which regulates the collection of personal information from children under 13. In 2019, TikTok was fined $5.7 million by the US Federal Trade Commission (FTC) for illegally collecting personal information from children under 13 without parental consent. This resulted in TikTok implementing changes to its policies and features to comply with COPPA regulations, such as limiting the data collected from users under 13 and providing parental controls.

Heatmap of TikTok's privacy policy

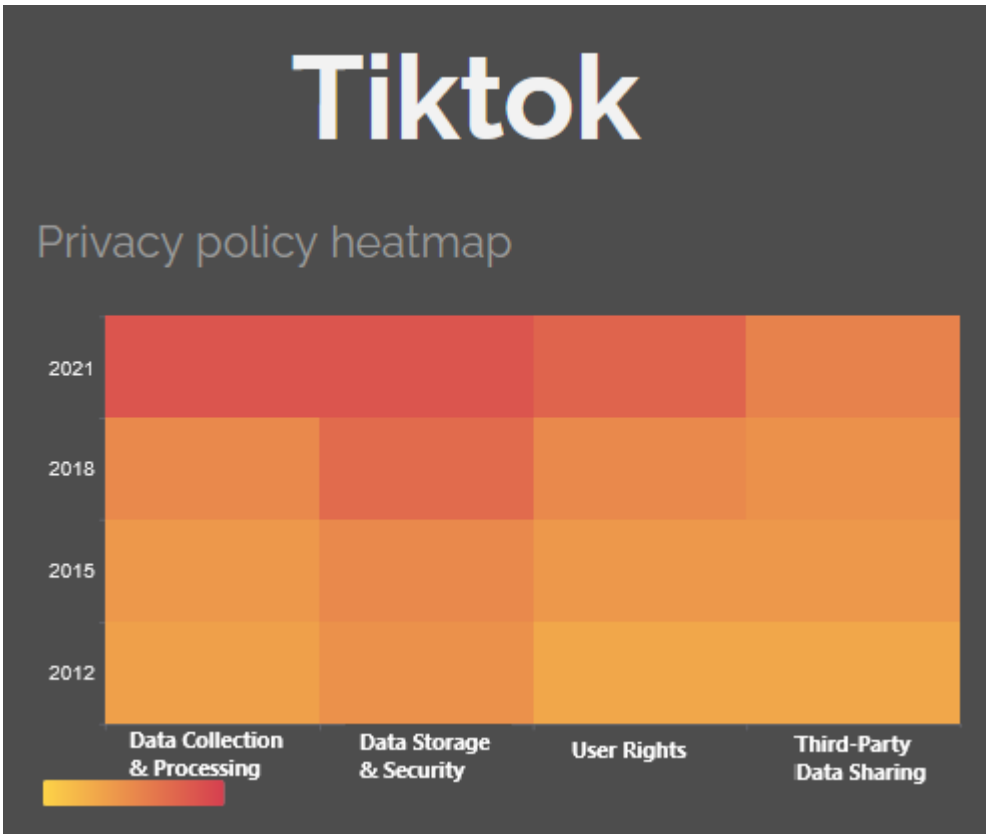


Figure 3

TikTok began with a lower score for data collection and processing practices for 2012 and 2015, but in 2018 and 2021, its score would be high and very high respectively due to the platform's increasing use of artificial intelligence and machine learning algorithms to personalize content for users. TikTok has been known to track user behavior, such as the type of content a user likes or comments on, to provide more targeted content in the future, this is why TikTok scored so highly for this in the more recent years.

TikTok's data storage and security score also started off low between 2012 and 2015, but these improved over time. By 2021, the platform's score would be high due to the implementation of stronger security measures, such as encryption and multi-factor authentication, to protect user data.

In terms of user rights, TikTok again started with a low score in 2012 and 2015, but this improved to be around medium by 2018 and 2021, this is due to the platform implementing features which allow users to control their privacy settings, such as the ability to make an account private, restrict comments and limit notifications. (*Why TikTok is the latest security threat* 2020)

TikTok's score for third-party data sharing followed the same trend as the others, starting off low and creeping up as the years go by. This is due to the platform sharing user data with third-party vendors to personalize ads and content for users. However, the platform has faced criticism for its data-sharing practices and has since implemented features which allow users to control their data sharing preferences. (*Tiktok: It's hip, it's fun and it's a security risk* 2023)

Discussion/Analysis

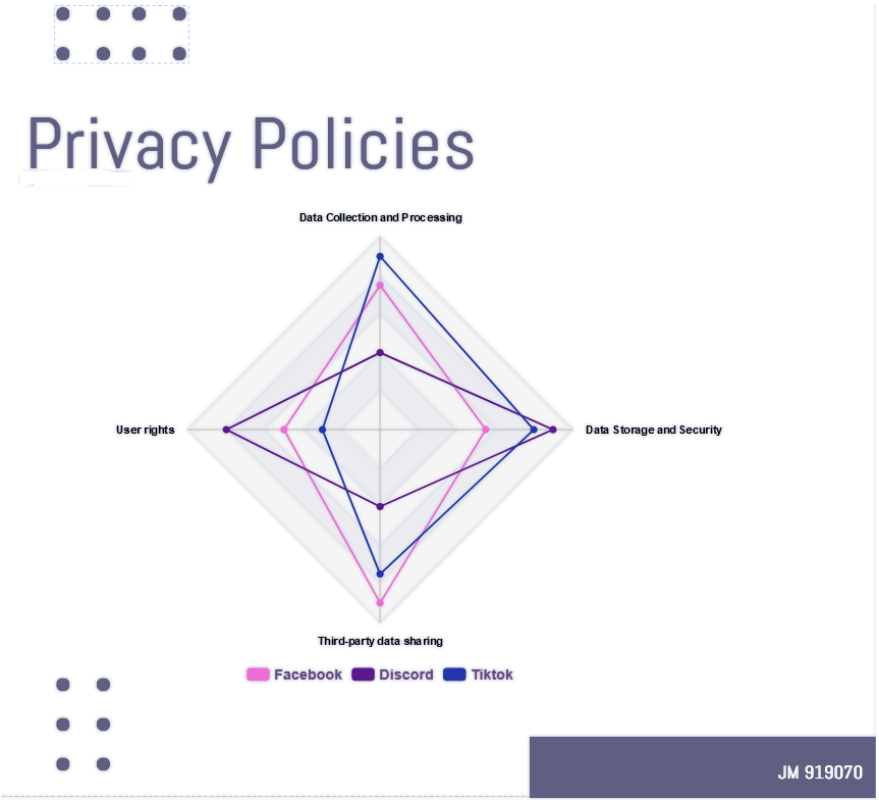


Figure 4

Figure 4 presents a radar chart in which I plot the different categories within a privacy policy on the axes and scored the companies appropriately.

Data Collection and Processing

1. TikTok received the highest score in this category due to the platform's extensive data collection practices and use of algorithms for targeted advertising and content recommendations.
2. Facebook's score was also high in this section due to the platform's long history of collecting user data and involvement in high-profile privacy scandals.
3. Discord had a moderately low score due to the platform having limited data collection practices when compared to other social media platforms.

Data Storage and Security

1. I scored TikTok moderately high in this section as the platform has made efforts to improve its data storage and security measures in response to concerns raised by governments and users.

2. Facebook's score here was moderately low due to the platform's past breaches and the Cambridge Analytica scandal, which revealed that the data of millions of Facebook users was obtained without their consent.
3. I plotted Discord quite high here due to the platform implementing several security features, such as two-factor authentication and end-to-end encryption for certain features.

User rights

1. TikTok's score here was moderately low due to the platform's past controversies regarding censorship and privacy violations, such as collecting user data from clipboard without consent.
2. Facebook also received a moderately low score here due to the platform's past scandals as mentioned earlier and other ongoing controversies related to misinformation and election interference.
3. Discord received the best score here through the platform's policies which are in place to protect user privacy and limit the collection and sharing of user data.

Third-party data sharing

1. TikTok received a moderately high score in this section due to the platform's extensive use of user data for targeted advertising and partnerships with third-party vendors.
2. Facebook had the highest score here as the platform has a long history of sharing user data with third-party vendors and has been involved in several data privacy scandals.
3. Discord's score here was moderately low due to the app having limited third-party integrations.

Qualitative Research

Introduction

With the rapid increase in the amount of personal data being collected, processed, and shared by companies, concerns over information privacy have become more significant than ever. In recent years, major social media platforms like Facebook, TikTok and Discord have faced scrutiny due to their privacy policies and practices. I aim to conduct a survey to help me better understand how attitudes toward privacy have evolved on the consumer side, over the last few years.

My survey will focus on various aspects of information privacy, including users' concerns, awareness of privacy risks, use of privacy settings and trust in companies' handling of personal data. By comparing the results of this survey with existing research on privacy attitudes and behaviours, I aim to gain a better understanding of how privacy concerns have shifted over the years, as well as what factors might've influenced these changes.

Through this research, I hope to obtain a deeper understanding of the evolving landscape surrounding information privacy and help shed light on the factors which are driving changes in user privacy attitudes and behaviours. This information can help organisations better understand how to adapt their privacy policies and practices to meet consumer expectations and maintain trust in their brand.

Survey

- Google forms
- Anonymous
- Each question related to research.
- Not about quality of survey, follow proper procedures etc.

Questions:

1. Have you become more concerned about protecting your personal information online in the past few years?
2. Do you read privacy policies or terms of service agreements before using a new website or app?
3. Do you adjust your privacy settings on social media platforms or other online services to limit the amount of data they collect about you?
4. Have you ever deleted a social media account or other online service due to concerns about privacy or data collection?
5. Have you ever used a virtual private network (VPN) or other tools to protect your privacy online?
6. Have you ever experienced a privacy or data breach which impacted your personal information?
7. Have you ever filed a complaint or taken legal action related to a privacy or data protection issue?

The design of my survey is essential for obtaining valuable insights into individual attitudes and behaviours regarding information privacy. The survey is divided into sections that address key aspects of information privacy, such as awareness, attitudes, behaviours, and expectations.

The survey questions are crafted to cover a wide range of the privacy spectrum, the survey's questions are open-ended, encouraging participants to share their experiences. This approach allows for a nuanced exploration of individual attitudes and behaviours related to information privacy.

The survey is designed to be visually appealing and easy to navigate, with clear instructions and concise questions, avoiding jargon. The user-friendly interface of google forms ensures that participants are able to complete the survey with minimal effort and confusion.

The qualitative data collected from the survey responses is analysed using thematic analysis, identifying common patterns and themes that emerge from the participants' answers. This approach allows for an in-depth exploration of the data, revealing insights into the complex factors that shape individual attitudes and behaviours related to information privacy.

(Jefferson Seide Molléri Blekinge Institute of Technology et al., 2016)

Findings

Question 1:

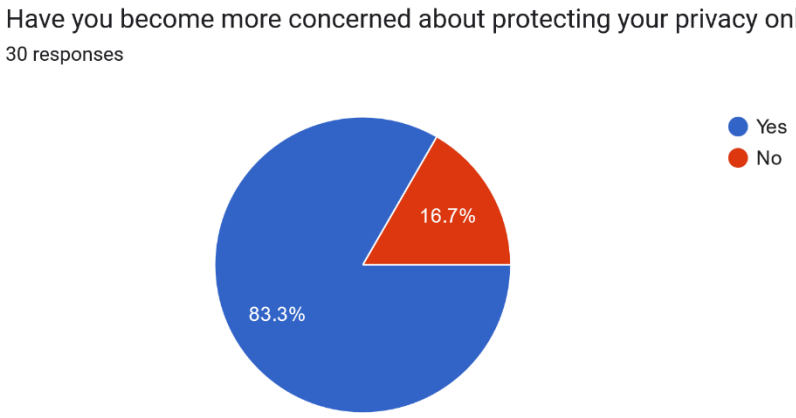


Figure 5

Based on the survey results for the first question, it appears that a significant majority (83.3%) of respondent's attitudes towards privacy has changed in recent years. This is a significant finding for my research as it suggests that people are becoming increasingly aware of the importance of online privacy and are taking steps to protect themselves. This could be due to numerous factors, such as high-profile data breaches and more press coverage relating to privacy.

This finding highlights the need for companies and regulators to take online privacy seriously and ensure that individuals have control over their personal data.

Though the sample size is relatively small and may not be representative of the broader population, I believe there wouldn't be a massive difference when it comes to a question like this for reasons stated prior. Therefore, whilst the results of this question are interesting, they need to be interpreted with caution and in the context of other research findings.

Question 2:

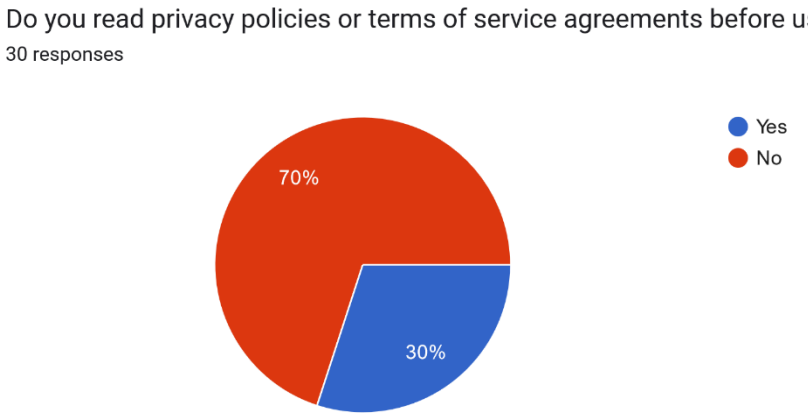


Figure 6

Based on the results of question 2 with 70% answering no and 30% answering yes, this indicates that a majority of the respondents to my survey don't read privacy policies or terms of service agreements before using a new website or app. I think that the findings from this question highlight an important issue in the current landscape of privacy, even though the majority of respondents in question 1 showed a concern for their privacy, they aren't concerned enough to read and understand the privacy policies of the websites and apps they use.

This suggests that users may be agreeing to terms and conditions without fully understanding what they are agreeing to and may be unaware of the ways in which their data is being collected, stored and shared. This lack of understanding puts users' personal information at risk, as they may be inadvertently providing access to their data to third-party companies or other entities.

As a result, it is important for websites and apps to improve their privacy policies transparency and readability, in an effort to make it easier for users to understand what is happening with their data. It may also be necessary for users to take a more proactive approach to protecting their privacy, such as taking the time to read privacy policies or doing research about the websites or apps they're considering signing up for.

Question 3:

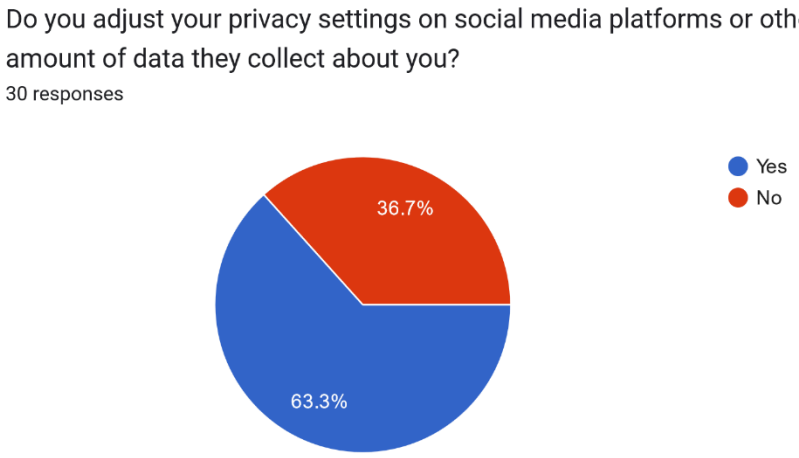


Figure 7

From the results of question 3, it is apparent that a majority (63.3%) of respondents do adjust their privacy settings on social media platforms or other online services in order to limit the amount of data being collected on them. This suggests that consumers could be becoming more aware of the importance of their privacy and taking the necessary steps to protect it though this could suggest that users who adjust their privacy settings may be doing so based on their general concerns for privacy, rather than being informed by the specific privacy policies of the platforms they use. This is again indicative of a need for greater transparency and accessibility of privacy policies and for platforms to make it easier for users to understand and adjust their privacy settings, as 36.7% of respondents voted no.

The fact that 36.7% of respondents do not adjust their privacy settings may also indicate that there is still a large portion of the population that isn't aware of the risks associated with sharing personal data or that they don't see the value in taking steps to protect their privacy.

Overall, these results suggest that while users may be becoming more concerned about their privacy, they still mightn't be informed about the specific privacy policies of the platforms they're using. Although some users are taking proactive steps to protect their privacy by adjusting their privacy settings, there is an opportunity for platforms to provide better transparency and guidance to help users make informed decisions about their privacy.

Question 4:

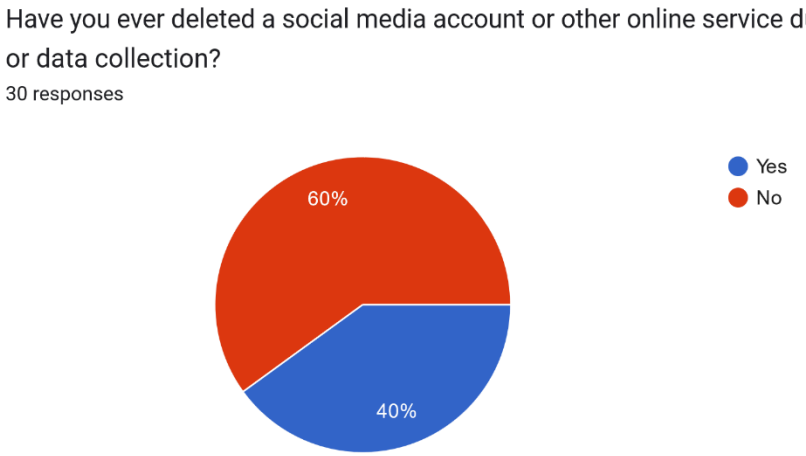


Figure 8

The results of question 4 show me that it is a minority of respondents who have deleted a social media account or other online service due to concerns about privacy or data collection. This suggests that privacy concerns have a tangible impact on user behaviour and may be a factor which companies need to account for when developing their privacy policies and practices. It's also worth noting that the majority of respondents (60%) haven't taken this step, this suggests that other factors (i.e. convenience, social pressure) may also play a role in user decision-making.

I think that if I were to repeat this survey soon, the results for this question would be different, due to the increasing number of breaches and cyber-attacks, I would advise the 60% of users who voted no to make themselves aware of services like Incogni which can help protect their privacy by ensuring that data brokers delete their data.

Overall, this result highlights the importance of understanding user attitudes and behaviours when it comes to privacy and suggests that there may be opportunities for companies to differentiate themselves by offering more robust privacy protections, as the users are prepared to delete their account if needs be.

Question 5:

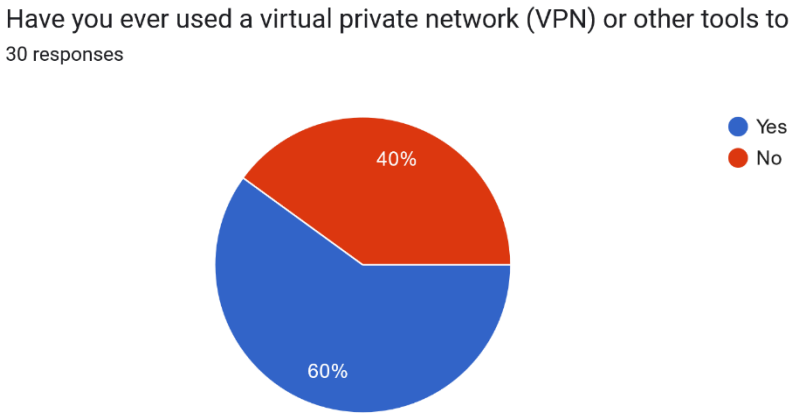


Figure 9

The results of question 5 show that a significant portion of respondents (60%) have used a virtual private network (VPN) or other tools to protect their privacy online. This suggests that privacy concerns are a top priority for a significant portion of users, and that they are taking active steps to protect their personal data. This informs my research as it shows me how exactly users are proactively safeguarding their privacy in the face of increased data collection and processing by online services.

Although most respondents have used a VPN and are being proactive in that regard, the 40% that have not used a VPN or other tools to protect their privacy online suggests that there is still a significant portion of the population that may be unaware of the risks associated with sharing personal information online or mightn't be taking proactive measures to protect their privacy. This highlights the need for increased awareness and education about online privacy and the tools available to safeguard personal data.

It is also worth noting that while 60% of respondents have used a VPN, some of these may have just been used as a workaround for things like region-locked content and mightn't always have been used in the name of safeguarding privacy.

Question 6:

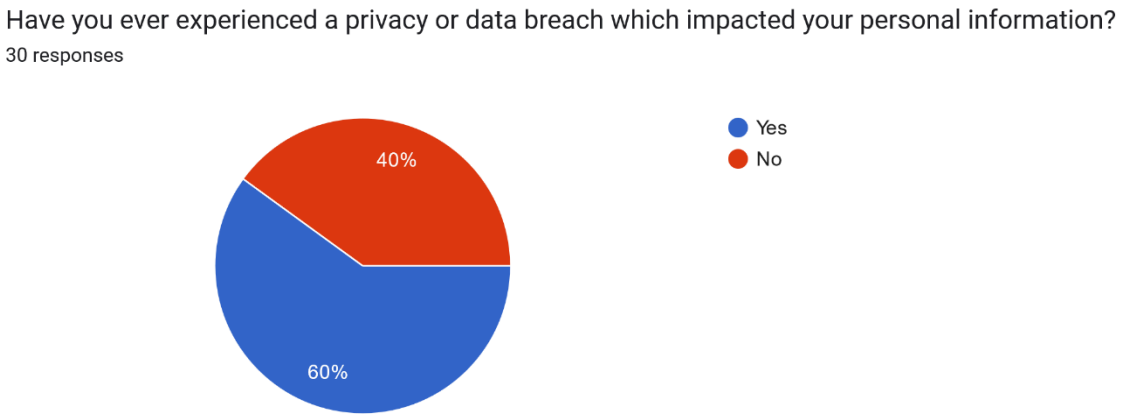


Figure 10

A 60% response rate of yes to this question indicates that a significant portion of the surveyed population has had their personal information compromised at some point. This finding underscores the importance of user privacy and highlights the risks associated with sharing personal information online. The high percentage of respondents who have experienced a data breach also suggests that companies need to do more to protect their users' personal information. This includes implementing robust security measures, being transparent about data collection and processing practices, and promptly notifying users in the event of a data breach.

This finding underscores the importance of companies taking the necessary steps to protect user data and privacy, as these breaches will have an impact on not only an individual but also their trust for the company or service in question. It's also important for users to take the necessary steps to protect their personal information, such as monitoring their accounts and updating their privacy settings.

For future research, it could be useful to explore the specific types of data breaches which respondents have experienced and then their impact on individuals' personal and professional lives can be better measured. Understanding the consequences of data breaches can provide invaluable insight into the real-world effects of inadequate privacy and security measures.

Question 7:

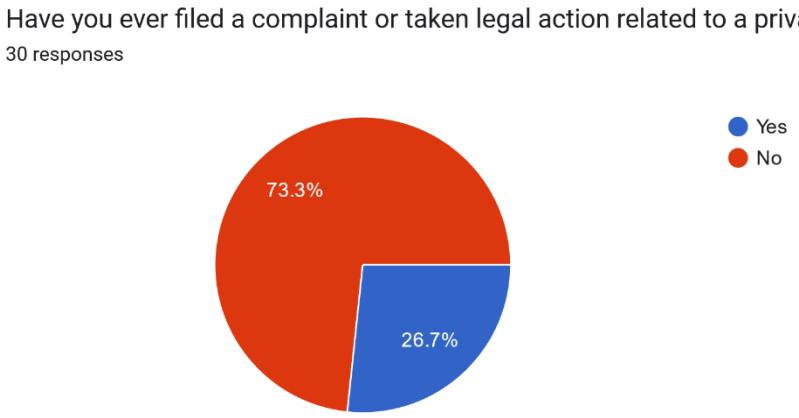


Figure 11

Question 7 was the final question of my survey and was regarding users acting against incidents such as data breaches, the low percentage of respondents who reported filing a complaint or taking legal action related to a privacy issue suggests that there may be a lack of awareness or understanding of privacy laws and how to enforce them.

From this question we can tell that most respondents haven't taken legal action or filed a complaint related to a privacy or data protection issue. This could indicate that people mightn't be fully aware of their rights when it comes to privacy or data protection issues, or they may not believe that their complaints will be addressed appropriately. Additionally, some respondents might not have the resources or time to file a complaint or take legal action, this could be due to the (typically) younger age of my respondents.

Overall, these results provide insights into consumer behaviour and preferences regarding privacy and can also potentially inform future research or policymaking in this area, this information may be useful in understanding the level of awareness and understanding of privacy rights among the general population and can help guide efforts to improve privacy policies and legal protections.

Discussion

From my survey, I can now tell that a significant majority of respondents do not read privacy policies or terms of service agreements before using a new website or app, whilst a smaller percentage do, this suggests that there is a need for improved user education and awareness around privacy policies and terms of service agreements.

Additionally, the fact that most respondents do adjust their privacy settings on social media platforms or other online services to limit the amount of data collected about them is promising, indicating that users are taking active steps to protect their privacy online.

The fact that a sizeable percentage of respondents have deleted a social media account or other online service due to privacy concerns, used tools like VPNs and been impacted by data breaches which impact their personal information, these questions highlight the importance of privacy and data protection for consumers.

Finally, the relatively low percentage of respondents who have filed a complaint or taken legal action related to a privacy issue suggests a need for more accessible and user-friendly avenues for users to address privacy concerns. Overall, the results of my survey provide valuable insights into consumer privacy attitudes and behaviours, which can inform future research and development of privacy policies and tools.

Based on the results of my survey, it seems that most of the respondents are concerned about their privacy and take steps to protect it, such as adjusting their privacy settings and using tools like VPNs. However, a significant portion of respondents also reported experiencing a privacy or data breach, indicating that there is still room for improvement in terms of data protection.

Design of artefact

I will create a comprehensive set of questions that cover all relevant areas of privacy laws, so that an organisation could present themselves with this set of questions to find out if they're fully compliant with all the relevant privacy laws.

It is important that the questions being asked cover all the relevant areas of privacy law globally. For this, I need to do some research and include laws such as GDPR, CCPA, PIPEDA etc. Once I have my comprehensive list of the laws surrounding privacy, I will be able to identify the common themes across them and use this as the basis for my set of questions.

The set of questions can be divided into the four categories which make up a privacy policy, this is also consistent with how I split up my research, these categories include: data collection and processing, data storage and security, user rights and third-party data sharing, each category should contain a set of questions which are relevant to the category, but also cover the relevant areas of the privacy laws including region-specific laws like HIPAA for healthcare data in the United States and the Australian Privacy Act for Australian organizations.

It's also important to ensure that the questions are structured in a way which makes it easy for organisations to understand and answer them, this may take the form of the questions simply being made up of clear and concise language, providing examples where necessary and avoiding technical jargon.

Overall, the design of my artefact is focused on providing a comprehensive set of questions that cover all relevant areas of privacy laws, whilst also being easy to understand and answer by organisations. It should also adhere to good design practices such as modularity, separation of concerns and the use of design patterns to ensure maintainability and extensibility.

I will include a scoring system within my artifact, ensuring that the scale is relevant and appropriate to each question, this is done so the organisations are able to take their score and assess their compliance, identifying areas in which they need to improve their practices.

To use my artifact, an organisation will need to carefully review each question and provide a score based on their current practices. The scores range from 0 to 3, with 0 indicating non-compliance or insufficient practices and 3 indicating comprehensive and effective practices. The explanations of scores provided in the table are there as a guideline and can be used to help organisations determine the appropriate score for each question, I also included some industry-specific questions, which won't apply to every organisation.

After completing the questionnaire, the organisation will be able to tally their scores for each category and calculate the total score. I have made the following guidelines for interpreting the results.

- High scores (close to the maximum possible score for each category): Your organization demonstrates strong privacy practices and is likely compliant with relevant privacy laws and regulations. However, there may still be areas for improvement or opportunities to further enhance your privacy program.
- Moderate scores (middle range for each category): Your organization has implemented some privacy practices, but there may be significant areas for improvement or potential compliance gaps. Review the questions with lower scores and consider implementing changes to strengthen your privacy program.

- Low scores (close to the minimum possible score for each category): Your organization may be at risk of non-compliance with privacy laws and regulations. It is important to review your practices and make significant improvements to protect user data and ensure compliance.

By regularly assessing your organisations privacy practices using this questionnaire, you can work towards continuous improvement and ensure that you remain compliant with the ever-evolving privacy regulations.

Plan of Design

Section	Question	Relevant Law	Region	Score	Score explained
Data collection & Processing					
	1	COPPA			
	2	GDPR			
	3				
Data Storage & Security					
	1				
	2				

Development and implementation of Artifact

Category	Question	Relevant Law(s)	Region(s)	Score (0-3)	Explanation of scores
Data Collection & Processing	1. What types of personal data does your organisation collect from users?	GDPR, CCPA, LGPD, PIPEDA	EU, USA, (California), Brazil, Canada		0: No personal data collected 1: Minimal personal data collected 2: Moderate personal data collected 3: Extensive personal data collected
	2. How does your organisation obtain user consent for data collection and processing?	GDPR, CCPA, LGPD, PIPEDA	EU, USA, (California), Brazil, Canada		0: No consent obtained 1: Consent obtained for some data 2: Consent obtained for most data 3: Consent obtained for all data.
	3. What purposes specifically does your organisation use the collected data for?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No data usage 1: Limited purposes (e.g., basic services) 2: Moderate purposes (e.g., marketing) 3: Multiple purposes (e.g., marketing, analytics)
	4. Does your organisation collect data from third-party sources? If so, how is it used	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No third-party data collected 1: Limited third-party data collected and used for specific purposes 2: Moderate third-party data collected and used for multiple purposes 3: Extensive third-party data collected and used for various purposes
	5. Does your organisation have a clear and concise privacy policy that informs users about data collection principals?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, Australia, US (Healthcare)		0: No privacy notice 1: Limited clarity in privacy notice 2: Privacy notice mostly clear and concise 3: Clear and concise privacy notice
	6. How does your organisation handle sensitive personal data (e.g., financial	GDPR, CCPA, LGPD, PIPEDA	EU, US (California), Brazil, Canada		0: No sensitive data handled 1: Limited handling measures for sensitive data 2: Moderate handling measures

	information, health records)?				3: Comprehensive handling measures
	7. Do users have the option to opt-out of non-essential data collection and processing?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, Australia, US (Healthcare)		0: No opt-out option 1: Opt-out option for limited non-essential data 2: Opt-out option for most non-essential data 3: Opt-out option for all non-essential data
	8. Does your organisation retain personal data only for as long as necessary to fulfil the purposes for which it was collected?	GDPR, CCPA, LGPD, PIPEDA	EU, US (California), Brazil, Canada		0: Indefinite data retention 1: Retention beyond necessary duration 2: Retention mostly aligned with purpose 3: Retention strictly aligned with purpose
	9. How does your organisation ensure data accuracy and up-to-date information?	GDPR, CCPA, LGPD, PIPEDA	EU, US (California), Brazil, Canada		0: No measures for data accuracy 1: Basic measures for data accuracy 2: Intermediate measures 3: Comprehensive measures
	10. Does your organisation have a process in place for conducting a Data Protection Impact Assessments (DPIAs) when required?	GDPR, CCPA, LGPD, PIPEDA	EU, US (California), Brazil, Canada		0: No DPIA process 1: Limited DPIA process 2: DPIA process mostly in place 3: Comprehensive DPIA process in place
Healthcare	11. Does your organisation have a process for obtaining informed consent from patients before collecting	GDPR, HIPAA	EU, US (Healthcare)		0: No process 1: Limited process 2: Process mostly in place 3: Comprehensive process

	and processing their health data?				
Healthcare	12. How does your organisation handle sensitive health data (e.g. mental health, genetic data etc.	HIPAA, GDPR	US (Healthcare), EU		0: No handling procedures 1: Limited handling procedures 2: Handling procedures with some exceptions 3: Comprehensive handling procedures.
Financial Services	13. How does your organisation handle the collection and processing of financial data, such as credit card information?	GLBA, GDPR	US, EU		0: No handling procedures 1: Limited handling procedures 2: Handling procedures with some exceptions 3: Comprehensive handling procedures
Financial Services	14. Does your organisation have a process in place to verify the integrity of users before granting their access to financial data?	GLBA, GDPR	US, EU		0: No process 1: Limited process 2: Process mostly in place 3: Comprehensive process
Data Storage & Security	1. How does your organisation store and secure users' personal data?	GDPR, CCPA, LGPD, PIPEDA	EU, US (California), Brazil, Canada		0: No security measures 1: Basic security measures 2: Intermediate security measures 3: Advanced security measures
	2. What measures are in place to protect against data breaches or unauthorised access?	GDPR, CCPA, LGPD, PIPEDA	EU, US (California), Brazil, Canada		0: No Protection 1: Minimal Protection 2: Moderate protection 3: Comprehensive protection
	3. Are data backups regularly created and securely stored	GDPR, CCPA, LGPD, PIPEDA,	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No data backups 1: Infrequent data backups

	to ensure data availability and integrity?	HIPAA, Australian Privacy Act			2: Regular data backups with limited security 3: Regular, secure data backups
	4. Does your organisation encrypt users' personal data both in transit and at rest?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian privacy act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No encryption 1: Encryption only in transit or at rest 2: Encryption in transit and at rest but with exceptions 3: Comprehensive encryption in transit and at rest
	5. Does your organisation have a dedicated Data Protection Officer (DPO) or equivalent role?	GDPR, CCPA, LGPD, PIPEDA, Australian privacy act	EU, US (California), Brazil, Canada, Australia		0: No DPO or equivalent 1: Part-time DPO or equivalent 2: Full time DPO or equivalent with limited responsibilities 3: Full-time DPO or equivalent with comprehensive responsibilities.
	6. Does your organisation have a documented incident response plan in case of a data breach or security incident?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No incident response plan 1: Limited incident response plan 2: Incident response plan mostly in place 3: Comprehensive incident response plan
	7. How does your organisation manage and control access to personal data internally?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No access control 1: Limited access control 2: Moderate access control 3: Comprehensive access control
	8. Does your organisation regularly perform security audits or assessments to identify vulnerabilities and risks?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No security audits 1: Infrequent security audits 2: Regular security audits with limited scope 3: Regular, comprehensive security audits

	9. Does your organisation have a process for securely disposing of personal data when it is no longer needed?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No secure disposal process 1: Limited secure disposal process 2: Secure disposal process mostly in place 3: Comprehensive secure disposal process
	10. How does your organisation handle data transfers to and from countries or regions with different data protection laws?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No data transfer management 1: Limited data transfer management 2: Moderate data transfer management 3: Comprehensive data transfer management
Healthcare	11. How does your organisation ensure the secure transmission of health data, particularly when sharing it with other healthcare providers or third parties?	HIPAA, GDPR	US (Healthcare), EU		0: No secure transmission 1: Limited secure transmission 2: Secure transmission with some exceptions 3: Comprehensive secure transmission
Healthcare	12. Does your organisation have a process for managing access to electronic health records (EHRS) and ensuring only authorised personnel can access them?	HIPAA, GDPR	US (Healthcare), EU		0: No process 1: Limited process 2: Process mostly in place 3: Comprehensive process
Financial Services	13. How does your organisation ensure the secure storage of sensitive financial data (e.g. encryption, tokenization etc.)?	GLBA, GDPR	US, EU		0: No secure storage 1: Limited secure storage 2: Secure storage with some exceptions 3: Comprehensive secure storage

Financial Services	14. Does your organisation have a process for monitoring and detecting potential fraud or unauthorised access to financial data?	GLBA, GDPR	US, EU		0: No process 1: Limited process 2: Process mostly in place 3: Comprehensive process
User Rights	1. How does your organisation inform users about their rights under privacy laws?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian privacy act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No information provided 1: Limited information provided 2: Most information provided 3: Comprehensive information provided
	2. What mechanisms are in place for users to access, correct, or delete their personal data?	GDPR, CCPA, LGPD, PIPEDA	EU, US (California) Brazil, Canada		0: No mechanisms 1: Limited mechanisms 2: Most mechanisms available 3: Comprehensive mechanisms available
	3. Do users have the right to access their personal data held by your organisation?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No access 1: Limited access 2: Access with some exceptions 3: Comprehensive access
	4. Do users have the right to rectify or update their personal data held by your organisation?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No rectification 1: Limited rectification 2: Rectification with some exceptions 3: Comprehensive rectification
	5. Do users have the right to erasure or deletion of their personal data held by your organisation?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No erasure 1: Limited erasure 2: Erasure with some exceptions 3: Comprehensive erasure
	6. Do users have the right to restrict the processing of their personal data?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No restriction 1: Limited restriction 2: Restriction with some exceptions 3: Comprehensive restriction

	7. Do users have the right to data portability of their personal data?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No portability 1: Limited portability 2: Portability with some exceptions 3: Comprehensive portability
	8. Do users have the right to object to the processing of their personal data for specific purposes, such as direct marketing?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No objection 1: Limited objection 2: Objection with some exceptions 3: Comprehensive objection
	9. Does your organisation have a process in place to handle user requests regarding their rights?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No process 1: Limited process 2: Process mostly in place 3: Comprehensive process
	10. How does your organisation inform users about their rights regarding their personal data?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No information 1: Limited information 2: Clear information 3: Comprehensive and clear information
Healthcare	11. How does your organisation handle patient requests for accessing, correcting, or deleting their health data?	HIPAA, GDPR	US (Healthcare), EU		0: No handling procedures 1: Limited handling procedures 2: Handling procedures with some exceptions 3: Comprehensive handling procedures
Healthcare	12. Does your organisation have a process for notifying patients in case of a data breach involving their health data?	HIPAA, GDPR	US (Healthcare), EU		0: No process 1: Limited process 2: Process mostly in place 3: Comprehensive process
Third-Party Data Sharing	1. Does your organisation share users' personal data with	GDPR, CCPA, LGPD, PIPEDA	EU, US (California), Brazil, Canada		0: No sharing 1: Limited sharing

	third parties? If so, for what purposes?				2: Moderate sharing 3: Extensive sharing
	2. How does your organisation ensure that third parties comply with privacy laws?	GDPR, CCPA, LGPD, PIPEDA	EU, US (California), Brazil, Canada		0: No measures 1: Basic measures 2: Intermediate measures 3: Comprehensive measures
	3. Does your organisation share user data with third parties? If so, for what purposes?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No sharing 1: Limited sharing 2: Moderate sharing 3: Extensive sharing
	4. Does your organisation have a process to evaluate the privacy practices of third-party vendors?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No process 1: Limited process 2: Process mostly in place 3: Comprehensive process
	5. How does your organisation ensure that third-party vendors comply with privacy laws and regulations?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No assurance 1: Limited assurance 2: Assurance with some exceptions 3: Comprehensive assurance
	6. Does your organisation have a process in place to monitor and audit third-party vendors' privacy practices?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No process 1: Limited process 2: Process mostly in place 3: Comprehensive process
	7. How does your organisation inform users about third-party data sharing and obtain their consent?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No information or consent 1: Limited information and consent 2: Clear information with some exceptions 3: Comprehensive and clear information and consent

	8. Does your organisation have a procedure to terminate contracts with third-party vendors who fail to comply with privacy laws and regulations?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No procedure 1: Limited procedure 2: Procedure mostly in place 3: Comprehensive procedure
	9. Does your organisation restrict the use of user data by third-party vendors to only the agreed-upon purposes?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No restrictions 1: Limited restrictions 2: Restrictions with some exceptions 3: Comprehensive restrictions
	10. How does your organisation ensure that third-party vendors delete or return user data when the contractual relationship ends?	GDPR, CCPA, LGPD, PIPEDA, HIPAA, Australian Privacy Act	EU, US (California), Brazil, Canada, US (Healthcare), Australia		0: No assurance 1: Limited assurance 2: Assurance with some exceptions 3: Comprehensive assurance
Healthcare	11. Does your organisation have a process for verifying that third-party healthcare providers or vendors comply with privacy regulations before sharing health data with them?	HIPAA, GDPR	US (Healthcare), EU		0: No process 1: Limited process 2: Process mostly in place 3: Comprehensive process
Healthcare	12. How does your organisation ensure that health data shared with third parties is used only for the intended	HIPAA, GDPR	US (Healthcare), EU		0: No assurance 1: Limited assurance 2: Assurance with some exceptions 3: Comprehensive assurance

	purpose and not repurposed or sold?				
Financial services	13. Does your organisation have a process for verifying that third-party financial service providers or vendors comply with privacy regulations before sharing financial data with them?	GLBA, GDPR	US, EU		0: No process 1: Limited process 2: Process mostly in place 3: Comprehensive process

The table beneath is a supplementary table for the privacy compliance questionnaire, in which an organisation will be able to see a bit more about the questions being asked of them, including things like best practices and more explanation towards the score of the questionnaire, this provides organisations with guidance on how they can improve their privacy practices in these areas.

Category	**Question**	**Best practices**	**Score explained**
Data Collection & Processing	What specific purposes does your organization use the collected data for?	Clearly define the purposes of data collection in a transparent and easily understandable manner	Higher scores indicate that the organization clearly defines the purposes of data collection and limits it to what is necessary. Lower scores suggest vague or excessive data collection practices.
	Does your organization collect data from third-party sources? If so, how is this data used?	Only collect third-party data that is relevant to the organization's purposes. Ensure transparency	Higher scores indicate responsible and transparent use of third-party data. Lower scores suggest a lack of transparency

		in how third-party data is used and obtained.	or excessive third-party data collection.
Data Storage & Security	How long does your organization retain user data, and do you have a data retention policy in place?	Establish a clear data retention policy, specifying the duration for retaining user data and reasons for it. Regularly review and update the policy.	Higher scores indicate a well-defined data retention policy and adherence to it. Lower scores suggest unclear or missing data retention policies.
	What security measures does your organization implement to protect user data from unauthorized access, alteration, or disclosure?	Implement strong security measures such as encryption, access control, and regular security audits. Train staff on data security practices.	Higher scores indicate robust security measures and staff training. Lower scores suggest weak security practices or insufficient staff training.
User Rights	Do users have the right to access, correct, or delete their personal data held by your organization?	Implement a clear process for users to access, correct, or delete their personal data. Communicate this process to users.	Higher scores indicate a well-defined process and effective communication. Lower scores suggest unclear or missing processes.
	How does your organization handle user requests relate to their data protection rights under applicable laws?	Ensure timely and effective handling of user requests, adhering to relevant legal requirements. Train staff on handling such requests.	Higher scores indicate efficient handling of user requests and staff training. Lower scores suggest inadequate handling or training.
Third-party Data Sharing	Does your organization share user data with third parties? If yes, under what circumstances?	Clearly outline circumstances under which data is shared with third parties. Share data only when	Higher scores indicate transparent and limited data sharing with user consent. Lower scores

		necessary and with user consent.	suggest unclear or excessive sharing.
	What measures does your organization take to ensure that third parties adhere to privacy requirements?	Conduct regular audits of third parties, include privacy requirements in contracts, and monitor their compliance with privacy policies.	Higher scores indicate strong measures to ensure third-party compliance. Lower scores suggest weak or insufficient measures.

After completing the questionnaire, calculate your total score by adding up the scores for every question. Keep in mind that not every question may apply to your organisation, so focus on those that are relevant to you whether that's via industry or region.

Scoring interpretation:

- 0-25% of maximum possible score: Your organisation has significant room for improvement in privacy compliance. Consider revisiting your privacy policies and practices to ensure they comply with relevant laws and regulations, and address the concerns highlighted by the questionnaire.
- 26-50% of maximum possible score: Your organisation has made some progress in privacy compliance, but there's still work to be done. Review the areas in which you scored poorly and take proactive steps to address the gaps in your privacy practices.
- 51-75% of maximum possible score: Your organisation demonstrates a good level of privacy compliance, but there is potential for further improvement. Analyse the areas where you scored lower and consider implementing additional measures to enhance your privacy practices.
- 76-100% of maximum possible score: Your organisation exhibits strong privacy compliance. Continue to monitor and update your privacy policies and practices as necessary and stay informed about changes in privacy regulations and industry best practices.

Steps to improvement:

1. Identify the areas in which your organisation scored lower and prioritise addressing these gaps in your privacy practices.
2. Consult with legal and privacy experts to ensure your organisations policies and procedures are compliant with relevant laws and regulations.
3. Educate your employees about the importance of privacy and data protection and provide regular training on privacy best practices.
4. Implement technical and organisational measures to enhance the security of the personal data you collect, process and store.
5. Regularly review and update your privacy policies and practices to stay current with changes in privacy regulations and industry best practices.
6. Be transparent with your users about your data collection, processing and sharing practices, and ensure they have easy access to their data and rights.

By following these suggestions and focusing on the relevant questions or section from the questionnaire, your organisation will be well on its way to improving its privacy compliance, should it need it, minimizing the risk of data breaches and regulatory penalties.

Testing and Evaluation of Artefact

Case Study: SocialSnap Innovations

SocialSnap Innovations is a fast-growing social media company with a user base that spans across the globe. The platform allows users to share photos, videos and messages with their followers, making it an attractive space for people to connect and communicate. As the company continues to grow, it becomes increasingly important for SocialSnap Innovations to ensure that it adheres to privacy regulations and maintains user trust.

Upon completing the questionnaire, HealthTech Innovations scores 50% of the maximum possible score. Here is a summary of their scores across different categories.

1. Data Collection & Processing: SocialSnap Innovations scored well in this category, as they have clear purposes for data collection and have implemented safeguards to prevent unnecessary data collection. However, the company falls short in implementing strict measures to limit data collection to the minimum necessary and in obtaining user consent for specific purposes.
2. Data Storage & Security: The company has implemented data encryption and secure storage methods, but they do not have a comprehensive plan for addressing data breaches or a regular schedule for reviewing and updating their security measures.
3. User Rights: SocialSnap Innovations allows their users to access and correct their data, but there is no clear procedure for handling data deletion requests or providing data in a portable format.
4. Third-Party Data Sharing: The company has agreements in place with third-party vendors to ensure the protection of shared data. However, they do not perform regular audits of these vendors' compliance with privacy laws, and their process for obtaining user consent before sharing data could be more transparent.
5. Industry-specific Questions: SocialSnap Innovations scores relatively low in this category, as they are lacking a process for verifying the compliance of third-party healthcare providers before sharing data with them. Additionally, they lack a clear policy on using health data for secondary purposes, such as research or marketing.

Based on their scores, SocialSnap Innovations has room for improvement in several areas, particularly in user rights and industry-specific concerns. They should prioritise addressing these gaps in their privacy practices, consult with privacy experts, and provide regular employee training on privacy best practices.

Case Study: ConnectSphere

ConnectSphere is a well-established social media platform that enables users to build their personal and professional networks by connecting with others, sharing content, and engaging in discussions. With a large and diverse user base spanning multiple countries, ConnectSphere places a strong emphasis on privacy and compliance with international regulations.

To ensure that their privacy practices align with global standards, ConnectSphere decide to use the privacy compliance questionnaire. The company's management team diligently answers each question in the questionnaire, reflecting their comprehensive approach to privacy and data protection.

Upon completion, ConnectSphere achieves a high score of 90%. This demonstrates the company's commitment to protecting user privacy and adhering to regulatory requirements.

Key strengths identified in the questionnaire include;

1. Data Collection & Processing: ConnectSphere has implemented robust policies and procedures for data collection and processing, limiting data collection to what is necessary and obtaining explicit user consent for specific purposes. Their privacy policy is transparent, comprehensive, and easily accessible to users.
2. Data Storage & Security: The company employs state-of-the-art encryption techniques and conducts regular security audits to protect user data. Data retention policies are in place, ensuring that data is not stored longer than necessary. Additionally, staff members receive regular training on privacy and security best practices.
3. User Rights: ConnectSphere has established clear and user-friendly processes for individuals to exercise their rights to access, correct, and delete personal data. The company is also responsive to user requests and inquiries, ensuring that users feel empowered and informed about their privacy rights.
4. Third-Party Data Sharing: ConnectSphere maintains strict criteria for selecting third-party partners and closely monitors their privacy practices. Data sharing agreements are in place, and ongoing audits are conducted to ensure compliance with privacy regulations.

While ConnectSphere's high score on the privacy compliance questionnaire reflects their strong commitment to privacy, the company recognises that maintaining compliance is an ongoing process. As such, they continually evaluate and update their privacy practices to stay ahead of evolving regulations and user expectations.

Case Study: BuzzChatter

BuzzChatter is a rapidly growing social media platform that focuses on real-time conversations and content sharing. Despite its increasing popularity, the platform has struggled with adequately addressing privacy concerns and compliance with international regulations.

The primary weaknesses identified in the questionnaire include:

1. Data Collection & Processing: BuzzChatter collects a significant amount of user data without clearly specifying the purposes for which it will be used. Their privacy policy is difficult to understand and lacks transparency regarding data collection practices. Users are not provided with a clear option to opt out of data collection for non-essential purposes.
2. Data Storage & Security: The company's data storage and security practices are inadequate, with weak encryption and infrequent security audits. Data retention policies are unclear, leading to the storage of user data for indefinite periods. Staff members have not received adequate training on privacy and security best practices.
3. User Rights: BuzzChatter has not implemented user-friendly processes for individuals to exercise their rights to access, correct, or delete their personal data. The company is slow to respond to user requests and inquiries, leaving users feeling frustrated and uninformed about their privacy rights.
4. Third-Party Data Sharing: The platform shares user data with third-party partners without adequately vetting their privacy practices. Data sharing agreements are either absent or not consistently enforced, leading to potential privacy breaches and regulatory violations.

BuzzChatter’s low score on the privacy compliance questionnaire is a wake-up call for the company to address the numerous privacy and compliance issues that they’re facing. To rebuild trust with their user base and avoid potential fines and legal consequences, BuzzChatter needs to invest in improving their privacy practices, implementing user-friendly policies and procedures, and ensuring compliance with international regulations. This will require a dedicated effort to prioritising privacy and data protection as the platform continues to grow.

Evaluation

My artifact, a comprehensive privacy compliance questionnaire, aims to help organisations identify gaps in their privacy practices and ensure compliance with global privacy laws. I think my artifact is user-friendly due to the modular delivery, in which the categories are consistent throughout my project.

The questions within the questionnaire are designed to be clear, concise, and easy to understand. They're formulated using simple language and avoid technical jargon, making them accessible to individuals with varying levels of expertise in privacy matters. This approach is user-friendly and makes it easier for organisations to answer the questions and assess their privacy practices efficiently and accurately.

The inclusion of region and industry-specific questions makes my artifact adaptable to the unique requirements of different organisations, this design ensures that the artifact is relevant to a wide range of organisations, regardless of their size, location, or industry.

My artifact includes a scoring system that provides a quantifiable measure of an organisation's privacy practices. The clear instructions and guidance on how to use the questionnaire and interpret the scores make the artifact more user-friendly, allowing organisations to easily identify areas for improvement and take appropriate action.

Not only is the modular design of the questionnaire user-friendly, but it also adds flexibility to the questionnaire, allowing organisations to choose if they want to complete the entire questionnaire, or just focus on specific sections relevant to their concerns.

I believe I have solved my research problem for now, as my research problem revolves around the lack of clarity surrounding privacy on a global scale and the potential consequences organisations might face when not adhering to privacy laws. My artifact allows organisations to evaluate their privacy policies and practices, this helps organisations identify gaps in their compliance and avoid potential fines or other negative consequences.

Evaluation and Conclusion of Project

Throughout the course of this project, the goal has been the same. This consistency has allowed for the integration of new ideas and improvements while ensuring that my project is still aligned with the initial objective. From the beginning, the focus was on the privacy landscape and organisational practices.

Although I view this project as a success, there are always areas for improvement and things that could've been done differently. I think that my quantitative research was well-structured and informative, though I also think I could've provided a more detailed and comprehensive analysis of the regulatory landscape surrounding privacy and data protection. While GDPR was discussed extensively, and is the regulation most relevant to myself, there could be other regulations which could've been included in my quantitative research.

Furthermore, I believe my qualitative research was well-designed and provided me with valuable insight into user attitudes and behaviours regarding privacy. My questions focused on key areas of interest, such as users' awareness and concern about privacy issues, as well as their use of privacy-enhancing tools like VPNS. These varying questions provided me with a more nuanced understanding of the issues. Though, an area of improvement for my qualitative research would be the sample size of my survey, I think it could've been better to obtain a larger and more representative sample of users, allowing for more robust analysis and greater confidence in my results.

My qualitative research provided valuable insights into user attitudes and behaviours regarding privacy, combining this with quantitative methods such as the privacy policy reviews allows me to gain a more comprehensive understanding of the complex and multifaceted issues surrounding privacy in the digital age.

I believe that my project has successfully produced a valuable tool that has the potential to help organisation's ensure privacy compliance. The artifact developed in this project can help organisations identify areas for improvement, reduce legal risks and ultimately contribute to the protection of user privacy. If I could create my artifact again, I would develop an interactive online tool or a software application to guide organisations through the questionnaire and automatically generate compliance reports. This would've further improved user experience and streamlined the evaluation process and a more technical artifact may have been better for a project like this.

Future research in the field of information privacy could explore various avenues to enhance the effectiveness and applicability of the artifact developed in this project. As mentioned before, the development of interactive tools that facilitate an organisations' engagement with the questionnaire, making it more user friendly and accessible, this could take the form of a web-based platform or mobile application.

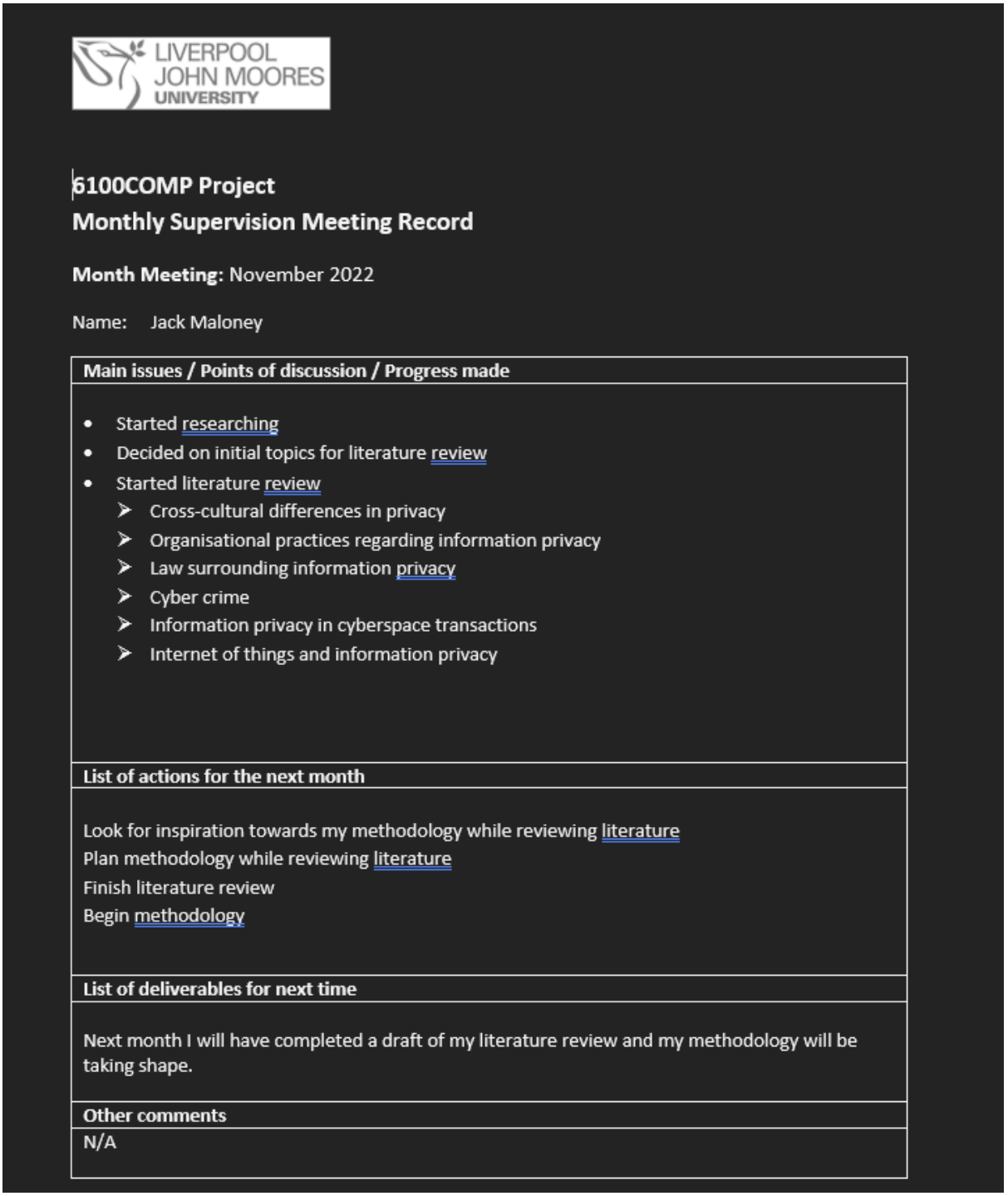
Expanding the scope of the artifact to include additional privacy-related concerns could lead to a more comprehensive assessment of an organisation's privacy practices. For instance, future research could investigate the impact of emerging technologies on privacy and incorporate these considerations into the privacy compliance questionnaire.

It's also essential to acknowledge that privacy laws and regulations are constantly evolving, and the artifact created in this project will eventually become outdated. Consequently, future research should also focus on continuously updating the artifact to reflect the latest privacy-related developments and legal requirements. By exploring these research directions, future work can

further enhance the artifact's utility and relevance in promoting compliance regarding information privacy.

Overall, I believe my project has achieved its goals through creating a tool to help organisations assess their privacy practices, however there is still room for further development and refinement, such as creating an interactive online tool, addressing more industry-specific privacy challenges, and expanding the scope of the artifact to include additional privacy-related concerns. By building on the foundation of this project, we can continue to contribute to the broader goal of improving information privacy and security on a global scale.

Appendix



LIVERPOOL JOHN MOORES UNIVERSITY

6100COMP Project
Monthly Supervision Meeting Record

Month Meeting: November 2022

Name: Jack Maloney

Main issues / Points of discussion / Progress made
• Started researching • Decided on initial topics for literature review • Started literature review ➢ Cross-cultural differences in privacy ➢ Organisational practices regarding information privacy ➢ Law surrounding information privacy ➢ Cyber crime ➢ Information privacy in cyberspace transactions ➢ Internet of things and information privacy
List of actions for the next month
Look for inspiration towards my methodology while reviewing literature Plan methodology while reviewing literature Finish literature review Begin methodology
List of deliverables for next time
Next month I will have completed a draft of my literature review and my methodology will be taking shape.
Other comments
N/A

LIVERPOOL JOHN MOORES UNIVERSITY

6100COMP Project
Monthly Supervision Meeting Record

Month Meeting: January 2023

Name: Jack Maloney

Main issues / Points of discussion / Progress made
• Completed first draft of literature review • Planned methodology
List of actions for the next month

• Decide on my research questions
• Begin quantitative research
  o Conduct a content analysis of security policies
  ▪ How have they changed?
  ▪ Are the policies complex?
  ▪ Compliant with GDPR, HIPAA, CCPA or relevant?
  o Decide on which three websites I'll use that handle user data
  ▪ *Discord*
  ▪ *Facebook(?)*
  ▪ *Tiktok(?)*
• Begin qualitative research
  o Observe the actions an individual will take to protect their privacy
  ▪ How have they changed?
  ▪ Survey?

References

1. Trepte, S., 2022. A cross-cultural perspective on the privacy calculus. [online] SAGE Journals. Available at: https://journals.sagepub.com/doi/full/10.1177/2056305116688035 [Accessed 9 November 2022].
2. Smith, J., n.d. JSTOR. [online] JSTOR. Available at: https://www.jstor.org/stable/249477 [Accessed 12 December 2022].
3. Posey, C., n.d. Taking stock of organisations' protection of privacy: Categorising and ... [online] Taylor & Francis. Available at: https://www.tandfonline.com/doi/full/10.1057/s41303-017-0065-y [Accessed 12 December 2022].
4. Brasseur, K., 2022. Discord fined $830K for GDPR lapses. Compliance Week. [online] Available at: https://www.complianceweek.com/regulatory-enforcement/discord-fined-830k-for-gdpr-lapses/32372.article [Accessed 12 December 2022].
5. Solove, D., n.d. Information privacy law. [e-book] Google Books. Available at: https://books.google.co.uk/books?hl=en&lr=&id=zdmXEAAAQBAJ&oi=fnd&pg=PR1&dq=information%2Bprivacy%2B&ots=O7MhGB3vZZ&sig=YnkvlS-SaM066phiv4GEzM4LdUw&redir_esc=y#v=onepage&q=information%20privacy&f=false [Accessed 12 December 2022].
6. Wu, K.-W., Huang, S.Y., Yen, D.C., Popova, I. et al., 2012. The effect of online privacy policy on Consumer Privacy Concern and Trust. Computers in Human Behavior. [online] Pergamon. Available at: https://www.sciencedirect.com/science/article/pii/S0747563211002767 [Accessed 1 January 2023].
7. Akhter, S., n.d. Privacy Concern and Online Transactions: The Impact of Internet Self-efficacy and Internet Involvement. [online] Marquette University. Available at: https://epublications.marquette.edu/cgi/viewcontent.cgi?article=1138&context=market_fac [Accessed: January 13, 2023].
8. Bellman, n.d. International differences in Information Privacy Concerns: A global survey of consumers. [online] Taylor & Francis. Available at: https://www.tandfonline.com/doi/abs/10.1080/01972240490507956 [Accessed 13 January 2023].
9. Smith, n.d. JSTOR. [online] JSTOR. Available at: https://www.jstor.org/stable/249477 [Accessed 13 January 2023].
10. Posey, n.d. Taking stock of Organisations' protection of privacy: Categorising and assessing threats to personally identifiable information in the USA. [online] Taylor & Francis. Available at: https://www.tandfonline.com/doi/abs/10.1057/s41303-017-0065-y [Accessed 13 January 2023].
11. Presthus, W. and Sørum, H., n.d. Consumer Perspectives on Information Privacy following the implementation of the GDPR. International Journal of Information Systems and Project Management. [online] Available at: https://revistas.uminho.pt/index.php/ijispm/article/view/3637 [Accessed 13 January 2023].
12. Iwaya, L.H., Iwaya, G.H., Fischer-Hübner, S. and Steil, A.V., 2022. Organisational Privacy Culture and Climate: A Scoping Review. IEEE Access, 10, pp.73907-73930. doi: 10.1109/ACCESS.2022.3190373.
13. Dinev, T. et al., 2006. An extended privacy calculus model for E-Commerce Transactions. Information Systems Research. [online] Available at: https://pubsonline.informs.org/doi/10.1287/isre.1060.0080 [Accessed 16 January 2023].

14. Parks, R., 2017. Examining the intended and unintended consequences of organisational privacy safeguards. Digital Object Identifier System. [online] Available at: https://doi.org/10.1057/s41303-016-0001-6 [Accessed 16 January 2023].
15. Hoofnagle, C.J. et al., 2010. How different are young adults from older adults when it comes to information privacy attitudes and policies? SSRN. [online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864 [Accessed 16 January 2023].
16. Cruz-Cunha, M., n.d. Handbook of Research on Cyber Crime and Information Privacy. [e-book] Google Books. Available at: https://books.google.co.uk/books?hl=en&lr=&id=wLkIEAAAQBAJ&oi=fnd&pg=PP1&dq=cyber%2Bcrime%2Band%2Binformation%2Bprivacy&ots=Htb1_jZ04P&sig=enLbLAbUh-BLDf8dtTArsiQH8fM&redir_esc=y#v=onepage&q=cyber%20crime%20and%20information%20privacy&f=false [Accessed 21 January 2023].
17. Luna, R. et al., 2016. Cyber threats to health information systems: A systematic review. Technology and Health Care. [online] IOS Press. Available at: https://content.iospress.com/articles/technology-and-health-care/thc1102 [Accessed 21 January 2023].
18. Internet Archive, n.d. Internet archive: Wayback Machine. [online] Available at: https://archive.org/web/ [Accessed 13 March 2023].
19. Facebook GDPR, n.d. Facebook. [online] Available at: https://en-gb.facebook.com/business/gdpr [Accessed 13 March 2023].
20. R.M., J., 2010. Facebook double size of Data Center. Data Center Knowledge. [online] Available at: https://www.datacenterknowledge.com/archives/2010/07/30/facebook-will-double-size-of-oregon-data-center [Accessed 13 March 2023].
21. Clay, L.T., 2021. Rethinking Data Center Design for Singapore. Engineering at Meta. [online] Available at: https://engineering.fb.com/2019/01/14/data-center-engineering/singapore-data-center/ [Accessed 13 March 2023].
22. Meta, 2019. An update on the security issue. [online] Available at: https://about.fb.com/news/2018/10/update-on-security-issue/ [Accessed 13 March 2023].
23. Welch, C., 2014. Facebook will let users log into third-party apps anonymously. The Verge. [online] Available at: https://www.theverge.com/2014/4/30/5668750/facebook-announces-anonymous-login [Accessed 13 March 2023].
24. Privacy policy update and GDPR FAQ – discord, n.d. [online] Available at: https://support.discord.com/hc/en-us/articles/360003858092-Privacy-Policy-Update-and-GDPR-FAQ [Accessed 13 March 2023].
25. Discord, n.d. Privacy policy. [online] Available at: https://discord.com/privacy#3 [Accessed 13 March 2023].
26. Case study: Discord, n.d. Cloudflare. [online] Available at: https://www.cloudflare.com/case-studies/discord/ [Accessed 13 March 2023].
27. API docs for bots and developers, n.d. Discord Developer Portal. [online] Available at: https://discord.com/developers/docs/resources/audit-log [Accessed 13 March 2023].
28. TikTok, 2019. Delivering on our US data governance. Newsroom. [online] Available at: https://newsroom.tiktok.com/en-us/delivering-on-our-us-data-governance [Accessed 13 March 2023].
29. TikTok, 2019. Our first transparency report. Newsroom. [online] Available at: https://newsroom.tiktok.com/en-us/our-first-transparency-report [Accessed 13 March 2023].

30. Transparency center homepage meta, 2021. TikTok. [online] Available at: https://www.tiktok.com/transparency/en-us/ [Accessed 13 March 2023].
31. Vedova, H. and Technology, T.F.T.C.O., 2022. FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook. Federal Trade Commission. [online] Available at: https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook [Accessed 24 April 2023].
32. Molléri, J.S., Blekinge Institute of Technology et al., 2016. Survey guidelines in software engineering: Proceedings of the 10th ACM/IEEE International Symposium on Empirical Software Engineering and measurement. ACM Conferences. [online] Available at: https://dl.acm.org/doi/10.1145/2961111.2962619 [Accessed 24 April 2023].
33. Shore, J. and Steinman, J., n.d. Did you really agree to that? The evolution of Facebook's Privacy Policy. Technology Science. [online] Available at: https://techscience.org/a/2015081102/ [Accessed 30 April 2023].
34. Mazaji, J., n.d. Privacy issues on social networking platforms: The case of Facebook. [online] ResearchGate. Available at: https://www.researchgate.net/publication/306137574_Privacy_Issues_on_Social_Networking_Platforms_the_Case_of_Facebook[Accessed 30 April 2023].
35. Esteve, A., n.d. The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. Academic.oup.com. [online] Available at: https://academic.oup.com/idpl/article-abstract/7/1/36/3097625 [Accessed 30 April 2023].
36. Discord, n.d. How long discord keeps your information – discord - discord help center. [online] Available at: https://support.discord.com/hc/en-us/articles/5431812448791-How-long-Discord-keeps-your-information [Accessed 30 April 2023].
37. Discord, n.d. Privacy policy. [online] Discord. Available at: https://discord.com/privacy[Accessed 30 April 2023].
38. CountyNews, n.d. Tiktok: It's hip, it's fun and it's a security risk - naco.org. [online] Available at: https://www.naco.org/articles/tiktok-its-hip-its-fun-and-its-security-risk [Accessed 30 April 2023].
39. CISecurity, 2020. Why TikTok is the latest security threat. [online] CIS. Available at: https://www.cisecurity.org/insights/blog/why-tiktok-is-the-latest-security-threat [Accessed 30 April 2023].
40. Hill, S., n.d. Best practices in data collection and preparation... - Sage Journals. [online] Available at: https://journals.sagepub.com/doi/abs/10.1177/1094428119836485? [Accessed 30 April 2023].
41.