An Analysis of Privacy Regulations and User Concerns of Finance Mobile Applications

Alessandro Pedace[a], Omar Haggag[a], Shidong Pan[b] and John Grundy[a]

[a] Monash University, Clayton, VIC, Australia
[b] Australian National University, Canberra, Australia

ARTICLE INFO

Keywords:
Privacy Regulation
Software Engineering
User Review
Financial Mobile Apps
GDPR

Abstract

Context: Financial applications handle sensitive data, including personal details, banking information, and transaction histories, making them prime targets for cyber-attacks. As privacy concerns grow, users and regulators are increasingly analysing how these apps manage data in different legal contexts.
Objective: This study examines user privacy concerns and assesses the impact of privacy regulations on mobile financial applications in Germany, Australia, and the United States. It aims to evaluate how laws such as the GDPR in the EU, the Privacy Act in Australia, and various U.S. state and federal laws shape app privacy policies. Additionally, the study explores the readability and accessibility of privacy policies.
Method: User reviews from app stores were analysed to identify recurring privacy issues and regional differences in concerns. The study also reviewed privacy laws in the EU, Australia, and the U.S. to assess their influence on financial app policies. To analyse the user-friendliness of privacy documents, a readability analysis was conducted using the Flesch Reading Ease score and estimated reading times.
Results: The findings revealed that users are highly concerned about the handling of their data, with significant demand for greater transparency and more robust privacy protections. Regional differences in privacy concerns were identified, with varying levels of engagement with privacy issues in each region. The study also found significant discrepancies in the readability of privacy policies, with many policies proving too complex for the average user to understand.
Conclusion: The study concludes that financial app developers need to simplify their privacy policies and improve transparency to build user trust. It also emphasises the need for stronger regulatory frameworks to address evolving privacy challenges. Recommendations are made for developers and policymakers to enhance data protection and improve user experience in financial services.

1. Introduction

Smartphones have become indispensable for managing many aspects of our lives. We can now access a wide variety of financial apps on our smartphones that offer a range of features and services: Users can transfer money, buy stocks, and even file their taxes with the aid of these apps. Without having to physically visit banks or other financial institutions, their accessibility on mobile devices allows customers to gain real-time insights into their financial condition. Both the revenues of stock trading apps and the user numbers of online banking have increased accordingly in recent years [1, 2]. Additionally, the creation of digital wallets and mobile payment platforms like Apple Pay [3] and Google Pay [4] has completely changed how we make payments. Using these apps, users no longer need to carry cash or cards. The wide adoption of these mobile payment options includes 78 participating countries for Apple Pay [5] and 61 participating countries for Google Pay [6]. In the course of the recent COVID-19 pandemic and the associated reduction in contact, the relevance of this became particularly clear. According to a study by the European Central Bank, 40 % of respondents reduced their cash payments and almost 90 % wanted to continue doing so in the future [7]. The great interest of users in finance apps is also reflected in download numbers, with 2.6 billion downloads in the finance category in 2022 [8].

✉ alessandro.pedace@unibw.de (A. Pedace); omar.haggag@monash.edu (O. Haggag); shidong.pan@anu.edu.au (S. Pan); john.grundy@monash.edu (J. Grundy)
ORCID(s):

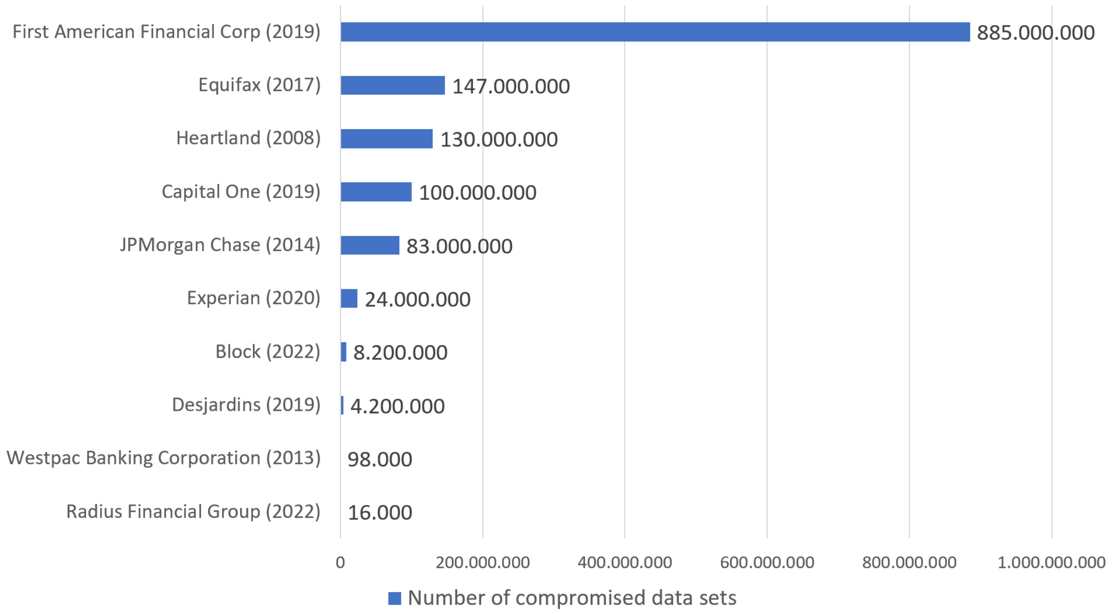

Figure 1: Largest data breaches in financial industry worldwide as of May 2022 [11]

However, as interest in financial apps has grown, so have the concerns of users about the security and privacy of their personal information, as financial apps collect highly sensitive data such as bank account information, credit card numbers and transaction data, making them a desirable target for hackers. In 2022, cyberattacks on the finance and insurance industry accounted for 18.9 % of global cyberattacks, which, in addition to the active damage caused by the attacks themselves, also cause severe secondary consequences such as the loss of customers and damage to the image of the companies [9, 10]. Figure 1 shows how serious cyberattacks and other data leaks in the financial industry can be for the data of users. As can be seen, data breaches occur quite frequently with millions of data records being compromised and immense privacy consequences for users.

Even without external intervention or data breaches, data protection is an increasingly important issue, especially in the finance industry. Although many developers are making efforts to protect user data, if only for legal reasons, privacy issues remain a major concern. People are becoming increasingly aware of the value of their personal data and its potential use by companies and financial institutions, which can range from simple targeted advertising to surveillance. They are thus developing a growing interest in how these applications manage, store and share it. To address these privacy concerns, many (financial) apps have detailed privacy policies describing what data is collected and why, and sometimes offer features such as the ability to request data deletion or opt-out of things like personalized advertising. The complexity and readability of privacy policies are critical factors that affect users' ability to understand the terms and conditions associated with financial applications. In addition, app developers are required to comply with privacy regulations from the various countries in which the apps are offered, which aim to protect the privacy of users and give them more control over their data, mitigating potential risks, and improving the trust between users and financial institutions. As financial apps play an important role in managing personal finances and are likely to become even more important in the future due to increased digitization and the shift away from cash, data protection and data security will become even more important as the number of users increases.

Despite the critical role financial apps play in managing personal finances, there is limited research that systematically analyzes the privacy concerns expressed by users. Given that financial apps handle sensitive data, it is essential to understand whether users perceive these apps as transparent and whether privacy policies provide sufficient clarity. User reviews serve as an invaluable resource for identifying real-world privacy concerns, yet they remain underutilized in privacy research. By recognizing the prevalent privacy issues and flaws that users have brought up, app developers can be encouraged to prioritize adequate privacy safeguards and even reevaluate the total extent of data acquired. Fixing the problems that users express could also result in more positive reviews, which would lead to higher download numbers and greater success for the app [12, 13]. This paper addresses this gap by analyzing privacy-related user reviews of financial apps, focusing on transparency issues, privacy policy accessibility, and compliance with regulatory frameworks.

To achieve this, this study analyzes user reviews of financial apps from three countries, Germany, Australia, and the United States (USA), which represent diverse financial environments and distinct privacy and data protection regulatory frameworks. We first collected and examined 15 leading financial mobile applications, their privacy policies, and their user reviews from the market. By examining user feedback in these countries, we aim to uncover common privacy concerns, evaluate how privacy policies communicate data practices, and assess whether regulatory differences influence user perceptions of privacy. Additionally, we investigate the readability and accessibility of privacy policies, using the Flesch Reading Ease score [14] and estimated reading times to assess how easily users can comprehend these documents. This metric evaluates textual complexity based on sentence length and word difficulty, providing a numerical score where higher values indicate easier readability. The Flesch Reading Ease formula has been widely used in previous research to assess the accessibility of legal and regulatory texts [15, 16]. Our analysis also considers the extent to which privacy concerns differ across regions and how regulatory variations impact financial app privacy policies. The findings highlight that users across all three countries express significant concerns about data handling, transparency, and privacy protections. Furthermore, we observe notable disparities in privacy policy readability, with many documents proving too complex for the average user. Based on these insights, we discuss implications for app developers and regulators, emphasizing the need for clearer privacy communication, improved transparency, and stronger regulatory measures to enhance data protection in financial applications.

In summary, the key contributions of this paper are as follows:

- A systematic analysis of user privacy concerns in financial apps, based on real-world user reviews.
- A cross-country comparison of privacy perceptions in Germany, Australia, and the USA, considering regulatory and financial ecosystem differences.
- An evaluation of financial app privacy policies, assessing their clarity, readability, and accessibility.
- Insights into how privacy concerns influence user trust, app adoption, and potential regulatory improvements.

2. Related Work

The financial sector is a well-researched area, encompassing a range of topics from competition to data protection. Studies have examined the interplay between data privacy and law enforcement within the financial sector, highlighting the tension between extensive data collection for legal purposes and privacy regulations that emphasize data minimization [17, 18, 19].

Despite the extensive research on the financial sector, the focus on financial apps and their unique data protection challenges remains relatively underexplored. With the recent surge in data protection laws, studies specifically targeting financial apps are still emerging. Anurag Kumar Jain and Devendra Shanbhag [20] offer a comprehensive overview of security and privacy risks associated with mobile apps. They emphasize the need for secure mobile application development due to the sensitivity of the data these apps handle. Johannes Huebner et al. [21] focus specifically on financial apps, analyzing user reviews to understand the factors influencing app ratings. Although their study does not concentrate on privacy issues, it provides valuable insights into user expectations and the importance of various app features. They employed machine learning techniques to analyze reviews from 1,610 finance apps, categorizing user feedback and linking it to quality indicators based on the Kano customer satisfaction model. Sebastian Zimmeck et al. [22] developed an automated system to analyze and predict the privacy compliance of Android apps. By examining 17,991 apps, they identified significant inconsistencies between stated privacy policies and actual app behavior. Their system combines machine learning and static code analysis to enhance transparency and enforce privacy laws, highlighting the widespread issue of privacy non-compliance in mobile apps. Hengshu Zhu et al. [23]

propose a mobile app recommendation system that addresses security and privacy concerns. Unlike traditional recommendation systems that prioritize popular apps, their system evaluates security risks based on app permissions. Omar Haggag et al. [24] analyze user reviews for mobile health apps to identify key issues and compliments, aiming to improve app quality and user satisfaction. While their focus is on health apps, their methodology of extracting, classifying, and analyzing user feedback is relevant and similar to the approach used in this paper.

These related works provide a foundation for understanding the various challenges faced by financial apps, particularly concerning security and privacy. However, the geodifference of privacy regulations and privacy concerns are not discussed. In this paper, our research builds on these insights by specifically focusing on the user privacy concerns in financial apps in different regions. By addressing this research gap, this study contributes to enhancing privacy practices and user trust in financial applications.

Previous studies have explored various aspects of privacy concerns in mobile applications, particularly within the financial sector. For instance, prior research [25, 26, 27] has investigated the impact of excessive permission requests on user trust, showing that users often reject applications that demand access to sensitive data without sufficient justification. These studies primarily rely on quantitative survey data and permission analysis, whereas our study takes a qualitative approach by analyzing user reviews to uncover privacy concerns expressed in real-world contexts.

Moreover, while works such as [28, 29] examine the effects of regulatory policies (e.g., GDPR) on privacy expectations, they do not explore how user perceptions differ across regions. Our study fills this gap by comparing financial app privacy concerns across Germany, Australia, and the USA, highlighting cross-country differences in privacy expectations and trust levels.

Additionally, prior research on privacy nudging and user behavior [30, 31] has demonstrated that transparent privacy policies can mitigate trust issues. However, these studies do not analyze whether financial applications effectively communicate their privacy practices to users. Our analysis incorporates readability assessments of privacy policies and examines how their clarity influences user trust.

Key Distinctions of Our Work:

- Unlike large-scale automated permission analysis studies, we take a qualitative user review approach to identify privacy concerns directly from user feedback.
- We offer a cross-regional privacy perception analysis, which is largely absent in previous financial app studies.
- We assess privacy policy readability and transparency, linking it to user trust and regulatory compliance.

By drawing these comparisons, we position our study as a complementary and novel contribution to the existing literature, emphasizing the importance of user feedback in shaping privacy policies and financial application trust. Future work could integrate both qualitative and quantitative methodologies to provide an even more comprehensive understanding of privacy concerns in financial applications.

3. Privacy Regulations in Germany, Australia, and US

Privacy regulations protect consumers and influences consumers privacy awareness. This section provides a comprehensive overview of requirements of financial applications in data protection laws in Germany (Section 3.1), Australia (Section 3.2) and the USA (Section 3.3). We chose these three countries as they have a very high uptake of financial apps, diverse privacy regulations, and the apps we wanted to study are all in their respective app and google play stores.

3.1. Germany

Individual rights and data protection are highly valued in Germany. Its data protection is primarily governed by two laws: The European General Data Protection Regulation (GDPR) [32] and the German Federal Data Protection Act (German: Bundesdatenschutzgesetz, BDSG) [33].

GDPR: The GDPR is an extensive law that came into effect in 2018 and oversees how personal data is processed. It covers all organizations, regardless of where they are situated, that process personal data of individuals within the European Union (EU), accordingly also Germany. The GDPR gives people various data rights that give them control over their personal data. These rights include the ability to access and transfer their data, restrict processing, request erasure, and object to processing activities [32, 34]. Another crucial component of the GDPR is the prompt notification of data breaches. Within 72 hours of learning of a data breach that threatens the rights and freedoms of the people, organizations are required to notify the appropriate supervisory authority immediately. There are severe consequences for non-compliance under the GDPR. If an organization does not follow the rules, they risk paying heavy fines that might total 4 % of their annual global turnover or 20 million EUR, whichever is higher. Supervisory authorities are in charge of enforcing the GDPR, carrying out investigations, giving warnings and reprimands, and imposing fines. [32]

BDSG: The BDSG, first passed in 1977 and frequently updated, was Germany's primary data protection law before the GDPR. It mandates that personal data be collected directly from the data subject, who must be informed about the data collection entity, purposes, and recipients. Consent must be freely given. Anonymization is encouraged when feasible. Automated processing must be reported to the relevant authority. Entities are liable for damages from unauthorized data handling, with public entities liable regardless of fault. Offenses include improper data handling and negligence, with fines up to 50,000 EUR, or more for severe cases. Intentional misuse can result in imprisonment up to two years. Severe offenses involve unlawful data handling, with fines up to 300,000 EUR and similar imprisonment terms. [33]

3.2. Australia

Privacy Act 1988: The Commonwealth Privacy Act plays a crucial role in safeguarding personal information within Australia. Responsible for enforcing the Privacy Act is the Office of the Australian Information Commissioner (OAIC). The Act applies to a wide range of organizations within Australia, including credit reporting agencies as well as individuals, by providing the latter with certain rights with respect to the handling of their personal information by organizations covered by the Act. Certain Australian organizations and activities can be exempt from certain Privacy Act provisions. For example, small businesses with annual revenues under three million AUD are exempt from some privacy regulations, such as the need for privacy policies and limitations on direct marketing, but they still have to comply with the Australian Privacy Principles (APP), which will be explained in more detail later. Another example is journalism-related activities. Some media organizations are granted a small number of exemptions that strike a balance between private rights and press freedom, like not being obligated to comply with all APPs or the ability to potentially justify the use and disclosure of personal information by demonstrating that it is in the public interest [35]. An entity can be deemed in violation of the Act, if the entity (repetitively) performs an act or engages in a practice that significantly interferes with the privacy of one or more individuals. For contraventions committed by individuals (excluding body corporates), the maximum penalty for such violations is set at 2.5 million AUD.

Australian Privacy Principles: The Australian Privacy Principles (APPs) encompass 13 fundamental principles guiding the handling of personal information. These are guidelines that aim to protect the privacy of individuals by ensuring responsible handling of personal information. They promote transparency, accuracy, and security in the collection, use, and disclosure of data. The principles grant individuals rights to access and correct their information and provide a framework for addressing privacy concerns. By adhering to the APPs, organizations and agencies can maintain the trust of individuals, protect their privacy rights, and ensure responsible data management.

3.3. United States of America

Unlike Germany and Australia, the USA lacks a single, extensive national privacy law. Instead, there is a mixture of federal and state legislation that offers various degrees of protection for the personal data of consumers, with not even each state having its own law. [36]

Federal-Level Privacy Laws: There are many specific privacy-related laws in the USA, such as the Health Insurance Portability and Accountability Act (HIPAA) [37] from 1996 for healthcare providers, the Children's Online Privacy Protection Act [38], the Family Educational Rights and Privacy Act [39], or the Electronic Communications Privacy Act [40]. However, this paper is about financial apps, which is why the following section focuses on laws that deal with privacy in the financial sector. Again, there are several laws that deal with this, but the two most relevant are the GLBA [41] and the Fair Credit Reporting Act (FCRA) [42].

GLBA: The GLBA [41] is a federal law from 1999 that regulates financial institutions like banks or insurance companies and focuses on the privacy and security of consumer financial information. Financial institutions are obligated to continuously respect the privacy of their customers and actively protect the confidentiality of their non-public personal information. They must implement safeguards that include administrative, technical, and physical measures to ensure the security and confidentiality of customer records. Financial institutions are required to provide notices to consumers at the beginning of the customer relationship and annually thereafter. These notices must clearly detail the institution's privacy policies, including how consumer information is shared with third parties and the measures in place to protect such information. Additionally, consumers must be informed of their right to opt-out of having their information shared with non-affiliated third parties.

FCRA: The FCRA [42] is a federal law that regulates the collection, dissemination, and use of consumer credit information. While the FCRA primarily focuses on credit reporting, it does contain provisions related to privacy. The FCRA regulates the collection, dissemination, and use of consumer credit information, ensuring that consumer reporting agencies operate with respect for consumer privacy. Permissible uses of consumer reports are strictly defined, and agencies must provide consumers with access to their files upon request. Additionally, consumer reporting agencies are required to establish a system for consumers to opt out of lists and must notify consumers about the uses of collected information. The Act also stipulates that agencies implement procedures to ensure the accuracy and privacy of the information, restrict disclosures to authorized purposes, and comply with consumer requests for information blocking or correction.

State-level Privacy Regulations: In addition to the federal-level laws, there are also many state-specific laws. However, many states have no law at all, and in many states, the legislative process for privacy laws is currently inactive [43, 44]. Active laws include Virginia Consumer Data Protection Act [45], the Connecticut Data Privacy Act [46], the Colorado Privacy Act [47], and the most well-known one, California Consumer Privacy Act (CCPA) [48]. The CCPA is a data privacy law that went into effect in 2020 and primarily focuses on protecting the privacy rights of California residents. It applies to businesses that collect and process personal information of them, regardless of where they are located. The CCPA imposes comprehensive obligations on businesses handling the personal information of California residents. Businesses must inform consumers about the types of personal information collected, the purposes for collection, and if the information is sold or shared [49]. They are required to ensure that any data collection, use, retention, and sharing are necessary, proportionate, and compatible with specified purposes. Businesses must also provide consumers with the rights to request the deletion or correction of their personal information and to opt out of the sale or sharing of their information. Violations of the CCPA can lead to fines of up to 2,500 USD per violation or up to 7,500 USD for intentional violations or those involving minors under 16.

4. Study Methodology

Given these diverse privacy laws many financial apps need to navigate, we wanted to study the privacy concerns expressed by users about their financial applications in different jurisdictions, and whether app privacy policy declarations meet the laws of their jurisdictions of use. A systematic approach is essential to ensure that the findings are representative and meaningful. Thus, we selected representative target mobile apps and extracted user reviews from the Google Play Store. This section focuses on our methodology of analyzing the collected reviews, which is composed by the following four major modules.

- **Section 4.1 & 4.2**. We downloaded and extracted user reviews by *Google-Play-Scraper* python library.
- **Section 4.3.** We employed translation tools to translate non-English reviews into English by *googletrans* python library.
- **Section 4.4.** We employed a raw classifier to automatically classify collected reviews into subtopics.
- **Section 4.5.** Review sampling and analysis. 1) We employed **stratified random sampling** to get 200 reviews, from apps in Germany, Australia, and the USA, and the ratings (one-star and two-star), respectively. As the goal of this step is to identify the potential misclassifications, we tried to sample reviews from every sources (countries/apps, ratings). 2) We manually checked whether the review matches with its class (i.e., the subtopics), and about 12% reviews were misclassified. 3) We then

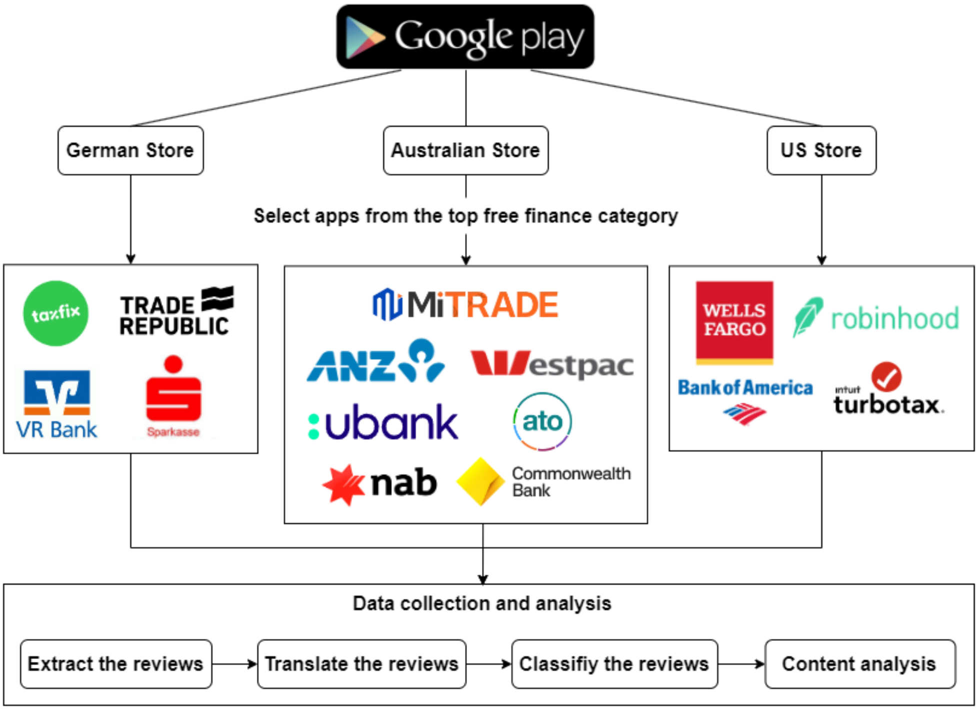

Figure 2: Data collection and processing procedure.

refined the keyword list and incorporated additional linguistic cues to filter out common sources of false positives. 4) We then re-classified all reviews, and randomly selected 500 reviews from each country (1,500 in total) for following analysis.

Also, we explain the approach to analyze privacy policies, and data use agreements of selected financial applications.

4.1. Dataset

The Android mobile application is a common choice to academic research [50]. There are many app markets for the Android platform, but according to AppBrain [51] (a famous Android market statistic website), the Google Play Store is the largest (with over two million apps) and the most accessible app market. We only select the Google Play Store in this study. Initially, we selected four apps from the Google Play Store in the top free finance category from Germany, Australia and the USA (as of 17 April, 2023). The ranking of the apps there is significantly influenced by their popularity and thus offers a good starting point to select the apps that are most relevant for users [52]. One tax app, one investment app and two bank apps were selected to provide diversity within the financial subcategories and to focus on banks, as these affect the majority of people. Since far fewer people live in Australia, the apps there also have significantly fewer reviews. We selected three more apps for Australia so that the number of reviews per country is roughly relative to the ratio of the number of inhabitants. The apps are selected based on their rankings at that time for their respective category. The selected apps are *Taxfix* [53], *Trade Republic* [54], *Sparkasse* [55] and *VR Bank* [56] for Germany, *TurboTax* [57], *Robinhood* [58], *Wells Fargo* [59], and *Bank of America* [60] for the USA, as well as *Mitrade* [61], *Australian Taxation Office* [62], *Commonwealth Bank* [63], *ANZ* [64], *Westpac* [65], *NAB* [66] and the *UBank Money App* [67] for Australia. This results in a total of 15 apps with a combined total of nearly 1.2 million reviews. This significant amount of user reviews provides a rich source of insight into the privacy concerns of users of financial apps. While we recognise that larger-scale studies, such as Huebner et al. [21], have analyzed over 1,620 mobile financial apps using machine learning techniques to categorize user feedback, our study takes a different approach by prioritizing a focused, qualitative examination of widely used apps

Table 1
The initial keyword list for classification.

Category	Initial keywords
policy	agreement, policy, regulation, compliance, terms, guidelines, rules, protocols, etc.
location	gps, location, map, coordinates, geolocation, positioning, navigation, tracking, etc.
data access	behavior, information, sharing, access, retrieval, storage, usage, distribution, etc.
permission	authorization, consent, permission, approval, access, license, clearance, sanction, etc.
ad	ad, advertisement, adware, commercial, promotion, marketing, publicity, sponsorship, etc.
security	encryption, hacked, insecure, breach, protection, defense, safeguarding, vulnerability, etc.
trust	protected, spyware, trustworthy, reliable, credible, dependable, authentic, secure, etc.
scam	fraud, ripoff, scam, deception, swindle, hoax, con, trickery, etc.

across three distinct regulatory environments. Huebner et al. leveraged automated analysis to identify trends in user satisfaction and app features, but their work did not deeply investigate privacy concerns or the impact of regulatory frameworks on user perceptions. By selecting 15 high-ranking financial applications from Germany, Australia, and the USA, our study allows for an in-depth exploration of privacy-related user feedback within different legal contexts, highlighting region-specific concerns that may not be evident in a purely large-scale, automated approach. This method enables us to examine privacy policy transparency, data handling practices, and compliance issues in a way that complements large-scale statistical findings with rich and qualitative insights. Moreover, our manual review of privacy policies ensures a nuanced understanding of how financial apps communicate their data practices, a factor that may be overlooked in algorithm-driven studies. While our dataset is smaller, it provides a strong foundation for identifying critical privacy challenges that users face. Future research could extend this analysis to a larger set of applications, combining qualitative and quantitative methods to validate and expand upon our findings.

4.2. Review Extraction

After selecting the apps, user reviews must be extracted and then further processed to make them analyzable. Various Python scripts are used to automate these steps, since it is a fast and easy-to-use programming language, which provides several libraries for this purpose [68]. To extract the reviews from the Google Play Store, the *Google-Play-Scraper* library [69] is used, because it is a lightweight library that provides easy-to-use functions for this case and is not limited to a certain amount of reviews.

4.3. Review Translation

Since the extracted app reviews may be written in different languages, including at least German, a crucial step is the translation of the extracted reviews into English. This translation process aims to ensure that the reviews are uniformly accessible for further analysis and interpretation. To accomplish this, the *googletrans* library [70] is used, a free and unrestricted Python library that implements the Google Translate API. Google Translate supports 133 languages and uses various approaches to translation, including statistical and example-based machine translation as well as neural translation technology, with an overall accuracy level of over 82.7 % and is therefore considered sufficient for this use case [71, 72, 73].

4.4. Review Classification

Once the app reviews are translated into English, the reviews need to be classified into one or more privacy subtopics. The objective here is to filter out all the reviews that are privacy-related and group them based on the specific privacy-related topics they address. This allows for a more detailed, systematic analysis of the various privacy concerns expressed by users, while also increasing efficiency, as all non-privacy-related reviews, which are not relevant to this paper, are not considered due to the prior filtering. A bag of keywords approach is used to classify the privacy-related reviews into eight subcategories. In this approach, texts – in this case the reviews – are tokenized, meaning they are divided into their individual components, and their content is checked for the inclusion of certain keywords, regardless of context and order [74]. This approach is chosen because it enables rapid processing of large amounts of reviews due to its low complexity, allowing for quick identification of reviews addressing privacy, and therefore helping narrow down the dataset, even though it may not capture all privacy-related reviews. In addition, the approach ensures consistency throughout the classification process, eliminating subjective interpretations. The categories and the keyword lists were elaborated by Omar Haggag et. al. [73] in a previous paper and were provided for this paper. The keyword lists are shown in Table 1. Table 2 shows how many reviews of the respective apps are privacy related according to the classification. As can be seen, with an average of 1.84 %, only a fraction of reviews are privacy related.

4.5. Review Sampling and Analysis

After all reviews are classified and filtered, the analysis is divided into a quantitative statistical and a qualitative manual analysis. For this purpose, both automatic tools for statistical analysis are used and samples of reviews are analyzed manually. Such an approach allows for the collection of quantitative data and facts, such as the distribution of reviews among categories and the ratio of user ratings. Additionally, it enables the detailed collection of qualitative data regarding the specific privacy issues expressed by users in their reviews. Although a single researcher conducted the initial thematic analysis of user reviews, the results were independently reviewed by two other authors to mitigate potential bias. All four authors discussed discrepancies in interpretation and refined the identified themes collaboratively. This multi-step validation process helped ensure the reliability of findings and consistency across the dataset.

The method used to select the samples for the manual analysis is *stratified random sampling*. In this method, a dataset is divided into homogeneous, mutually exclusive groups and a certain number of random samples are selected from each group [75]. The dataset in this case are the reviews from Germany, Australia and the USA respectively, and the group to be distinguished is the ratings.

While keyword-based classification provides a scalable approach to identifying privacy-related user reviews, it is susceptible to false positives when words appear in different contexts. To minimize this, we employed a multi-stage filtering approach:

1. Keyword Expansion and Refinement: We iteratively refined our keyword list by manually inspecting an initial sample of classified reviews to ensure contextual relevance.

2. Stratified Manual Validation: To quantify false positives, we randomly selected 200 classified reviews across different categories and manually verified their relevance to privacy concerns. Our analysis found that approximately 12% of classified reviews were misclassified due to ambiguous language.

3. Context-Aware Filtering: We incorporated additional linguistic cues to filter out common sources of false positives, such as financial terminology that overlaps with privacy-related keywords but does not indicate actual privacy concerns.

By integrating these measures, we improved classification accuracy and reduced the likelihood of false alarms in our dataset. We acknowledge that further refinement is possible, and future work could explore more advanced NLP techniques to enhance classification reliability.

Given that this study focuses on privacy-related concerns, we adopt a disproportionate sampling approach, prioritizing reviews with one- and two-star ratings, as negative reviews are more likely to highlight privacy issues [76]. The number of samples from each rating category is determined independently of their overall representation in the dataset, ensuring sufficient coverage of critical privacy-related concerns [77]. Unlike coding-based qualitative methodologies such as Grounded Theory, our qualitative analysis follows a direct thematic approach, where a researcher manually reads through the selected reviews to identify and interpret privacy-related themes. Since user reviews are relatively concise and the dataset size is manageable, this straightforward approach is effective in extracting key privacy concerns without requiring a complex coding framework.

In summary, a total of 1,500 reviews (500 per country) are selected for manual analysis, with an emphasis on reviews highlighting privacy-related issues. The findings from this analysis are presented in Section 5.1, providing insights into the specific privacy concerns voiced by users in different regulatory environments.

4.6. Privacy Policy

To comprehensively understand how financial apps handle user data, we conducted an in-depth analysis of the privacy policies of the selected apps. First, we obtained their privacy policies from the official websites of the financial applications by navigating to the ‘Privacy Policy’ or ‘Legal’ section typically found in the footer of the website. Additionally, privacy policies were collected from the app listings on the Google Play Store, where developers often link their privacy policies directly in the app store description to comply with app store requirements. For any privacy policies not readily available through the above methods, we reached out directly to the app developers via email or customer support channels to request the necessary documents. We ensured that the privacy policies collected were the most recent versions by checking the date of the last update, typically mentioned at the top or bottom of the document. Historical versions were also considered to understand any changes over time.

Once collected, the privacy policies were subjected to a thorough textual analysis. There are some automated privacy policy analysis methods, symbolic NLP method (e.g., PoliGraph [78]) and learning-based NLP methods (e.g., Polisis [79]). Even though those automated methods can analyze privacy policies in a large scale, they commonly underperform compared to manual analysis [50, 80]. In total, we collected the 15 privacy policy documents. We then manually and carefully read and analyzed them as below. Specifically, we identified the types of data collected by each app, categorizing them into personal information (e.g., name, email address), financial information (e.g., bank account details, transaction history), and device information (e.g., IP address, device ID). The stated purposes for data collection were analyzed, such as improving service functionality, personalized advertising, or compliance with legal obligations. We examined with whom and under what conditions user data is shared, including third-party service providers, business partners, and government entities. The rights granted to users regarding their data were noted, including rights to access, correct, delete, or restrict the processing of their data. The security measures mentioned to protect user data were reviewed, such as encryption, access controls, and anonymization techniques. Statements regarding compliance with relevant privacy regulations (e.g., GDPR, CCPA) were identified to understand the legal frameworks governing data practices.

An essential part of our analysis involved checking the compliance of the privacy policies and data use agreements with relevant regional regulations. For apps operating in Germany, we verified compliance with the GDPR. This included checking for the lawful basis for data processing (e.g., consent, contract necessity), user rights such as data access, rectification, erasure, and portability, data protection impact assessments for high-risk processing activities, and the designation of a Data Protection Officer (DPO) where required. For apps operating in Australia, we ensured compliance with the Privacy Act 1988 and the APPs, focusing on transparent handling of personal information, user rights to access and correct their data, obligations for direct marketing and data security, and requirements for cross-border data transfers. For apps operating in the USA, we verified compliance with various federal and state laws. Federal laws like the GLBA and the FCRA were checked, as well as specific state laws like the CCPA, ensuring user rights to opt-out, access, and delete their personal information were upheld.

Instances of non-compliance or vague descriptions were documented. This included a lack of clear consent mechanisms for data processing, inadequate explanations of data sharing practices, and missing information on user rights and how they can be exercised. Additionally, the privacy policies and data use agreements were compared against industry best practices to identify areas of improvement. This involved reviewing guidelines from data protection authorities and industry standards. By conducting this detailed analysis, we aimed to provide a comprehensive understanding of the privacy practices of financial apps and their alignment with legal requirements and user expectations.

4.7. Readability and Accessibility Analysis of Privacy Policies

The complexity and readability of privacy policies are critical factors that affect users’ ability to understand the terms and conditions associated with financial applications. High readability scores suggest that a document is easier to understand, while low scores indicate a more complex and potentially inaccessible text. Furthermore, the time required to read through these policies is another important aspect of accessibility, as longer policies may deter users from fully engaging with the content. To assess the readability and accessibility of the privacy policies of the selected financial applications, we utilized the following methods:

Table 2
User review classification results.

App Name	Total	Privacy-related
Taxfix	26906	108
Trade Republic	21434	302
Sparkasse	147551	2003
VR Bank	18773	407
TurboTax	58832	847
Robinhood	242453	5851
Wells Fargo	254252	3978
Bank of America	342100	5963
Mitrade	654	16
Australian Taxation Office	897	13
Commonwealth Bank	21526	402
ANZ	21965	497
Westpac	11396	246
NAB	11376	241
UBank Money App	2888	79
In Total	1183003	20953

- Flesch Reading Ease Score: This score was calculated for each privacy policy to determine the complexity of the language used. The score ranges from 1 to 100, with higher scores indicating easier readability.
- Average Reading Time: The estimated reading time was calculated based on a standard reading speed of 238 words per minute (wpm). This provides an indication of the time commitment required to thoroughly read each policy.

5. Results

5.1. Quantitative Analysis

About 1.2 million reviews from 15 different financial apps from three countries were extracted, translated, classified and filtered into subtopics according to privacy relatedness. Figure 3 shows the distribution of these reviews among the individual categories. Three types of reviews dominate: security-related (40.9 %), trust-related (29.2 %), and scam-related ones (19 %), which together account for almost 90 % of all privacy-related reviews. Next come permission-related reviews with 5.6 % and data access-related reviews with 4.6 % of the total. A vanishingly small fraction of the reviews are location-related (0.3 %), ad-related (0.2 %), or policy-related (0.2 %), which together account for less than one percent of the total.

Interestingly, if looking at Figure 5, it can be seen that although all ratings are mainly about permissions, data access, trust, security and scam, all categories become smaller as the rating increases, except for trust and security. This shows that although some users have concerns in this regard that need to be addressed, many users are satisfied with the app and trust it. This is also particularly evident in Figure 6, which shows the distribution of the ratings of the privacy-related reviews among the selected apps. Apart from two tax apps and the trading apps - the latter are presumably dragged down by the scandal described above - the reviews are generally primarily positive, which shows that users with privacy concerns tend to be in the minority, although their concerns are equally important and must be taken into account.

In order to interpret these results, it is important to take certain circumstances into account. For one, reviews can belong to different categories at the same time. For example, reviews that are primarily concerned with permissions and data access may be additionally categorized as security-related due to the presence of certain keywords, such as the following review:

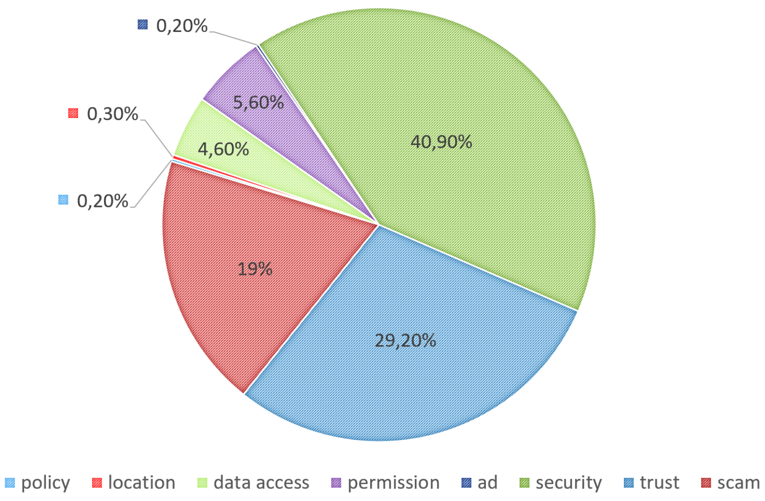

Figure 3: Distribution of all privacy-related reviews among the categories

> "The security of this app should be paramount! Why you are spying on my data and access to my camera is beyond me. [...]", 1★[a]
>
> [a] The stars denote the ratings of the app alongside this review, ranging from 1 (lowest) to 5 (highest).

While the issue addressed is primarily about data and camera access, the review is also classified under security due to the statement that security should be a priority. For the other, the figure shows the distribution of categories across *all* privacy-related reviews. However, as mentioned earlier in the paper, issues are usually more likely to be mentioned in reviews with a low score. The relevance of this becomes clear when looking at Figure 4. As can be seen, the reviews with low scores are mostly found in the scam, permission and policy categories, with around 80 % of reviews with a score of one or two. Whereas the categories security and trust, which are generally the most represented, consist of almost 70 % reviews with high scores of four or five. Considering this, it can be seen that a large representation of certain categories in the aggregate can also be caused by many positive reviews, which for example praise the security of the app, and it does not automatically mean that most issues are part of the category. An exact statement about the most mentioned issues of the users can be made through the qualitative, manual analysis of the review samples.

5.2. Qualitative Analysis

In the qualitative analysis section, we identified different types of privacy issues and concerns raised by users in their reviews for those financial applications.

5.2.1. Excessive Permission Requested

Many users express their concerns about the excessive permission requested and data access required by many of the finance and banking apps analyzed. For example:

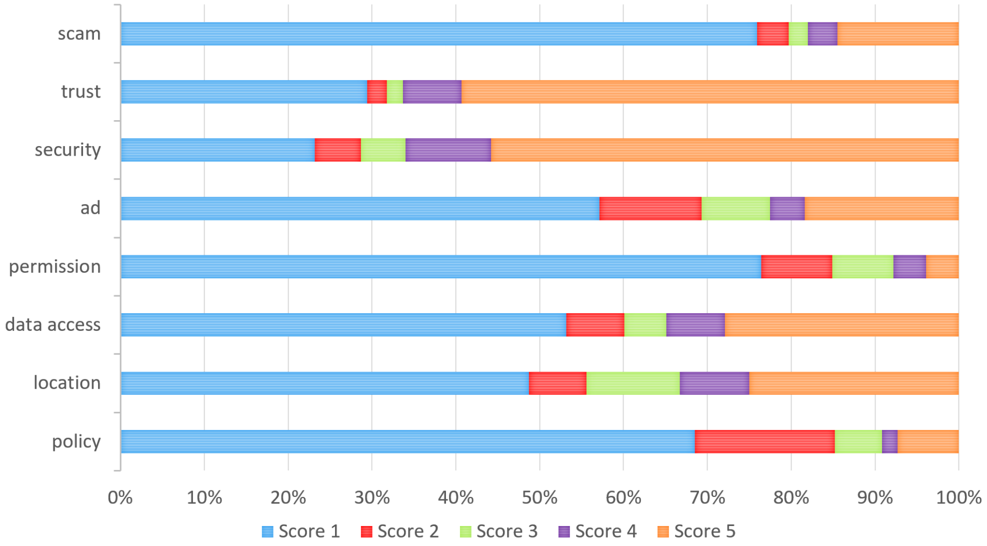

Figure 4: Distribution of ratings among the categories

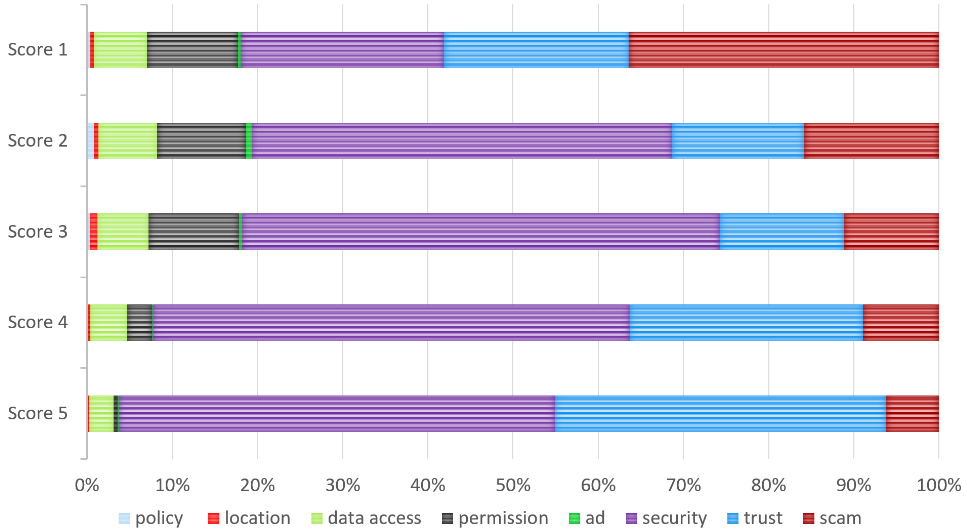

Figure 5: Distribution of categories among the ratings.

- “Uninstalled as requires so many permissions like precise location, phone calls, network information. No I don’t trust my bank.”, 1★
- “The new permission to view browser bookmarks and app activity is invasive and unacceptable. Find a way to do without that permission.”, 2★
- “I really enjoyed the app but after the latest security update wanted to see all my apps on my phone I’ve uninstalled the app. [...]”, 2★

Many reviews express concerns about the sheer number of permissions the apps demand, as well as the specific types of permissions they are requesting. Often, reviews criticize the access to the exact location,

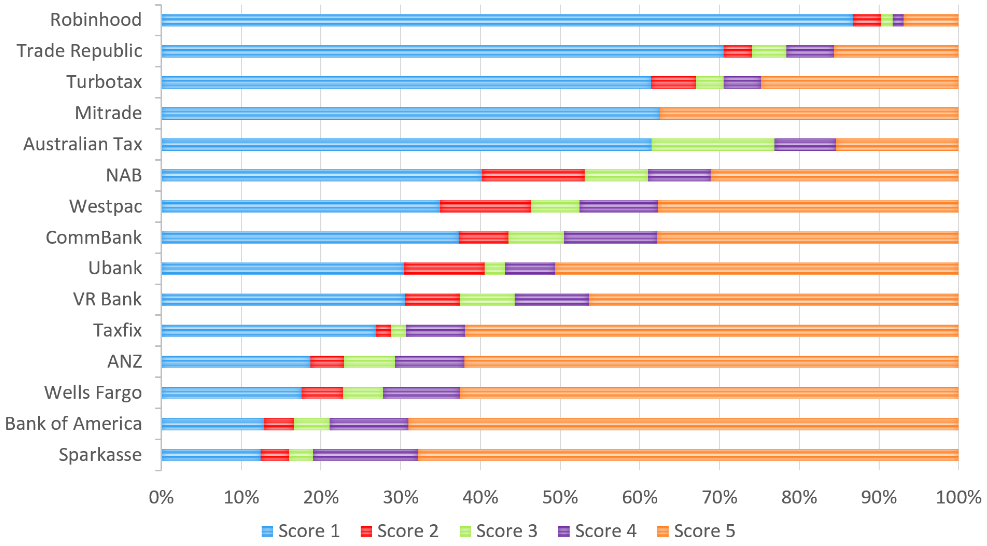

Figure 6: Distribution of ratings among the respective apps.

app activity or browser history, which shows that users are particularly concerned when apps request access to information that is sensitive to them. Such requests unsettle users regarding their privacy and security, leading them to question the trustworthiness of the app and the intentions behind these permissions. This even goes so far that when such permissions are newly introduced, some then uninstall the app altogether because they do not want to share this data. Others consider switching to other apps or services that they perceive to be more respectful of their privacy and require less invasive permissions.

5.2.2. *All-or-Nothing Permission Control*

Furthermore, the lack of optionally respectively the perceived “forcing” of consent is often criticized in the context of permissions and data access. This is stated in reviews such as:

- “The app is fine. What angers me is all the additional permissions required with this update. I didn’t want to accept the update but the older version no longer connects so I am forced to. [...]”, 1★
- “You need to consent to obtrusive permission required to use the app. [...] If you don’t agree, you’ll get logged out instantly.”, 1★
- “Latest version forces you to agree to location tracking, device usage tracking. Wow. Seriously disturbing stuff. [...]”, 1★

The lack of choice in app permissions is a major point of contention for users. In many cases, users do not have the option to decline permissions and have no choice but to agree to all requested permissions if they want to continue using the app. The practice of withholding app features until – what users perceive as – excessive permissions are granted exacerbates privacy and data misuse concerns. In addition, implicitly “forcing” consent contributes to a lack of trust between users and app developers. When users feel they are being forced to provide access to their personal information, they may question the intentions of the app and wonder why the app is so insistent on collecting certain information. This lack of trust can have a long-term negative impact on the reputation of the app and user retention.

5.2.3. Nontransparent and Non-understandable Privacy Policy

Besides the permissions and data access themselves, another key issue expressed by users is the perceived lack of or inadequate explanation by developers within the app interface or privacy policy regarding how requested permissions are used. While some users may not have reviewed the privacy policy, their reviews indicate that they were unable to easily find or understand relevant explanations. Corresponding reviews include the following:

- "Why does this app require access to my contacts and phone call logs? [...] Why is it not explained how these are used?", 1★
- "[...] Can any of you developers explain to us people why do you need to access my photos or media files for the app to work. [...] I would never install an app asking all those permissions, unless it has legitimate reason [...]", 2★
- "What is the point of accessing Bluetooth devices? Can the developer of the app tell me this maybe even ONCE? [...]", 3★

Users want to understand why certain permissions, such as accessing contacts, their camera, location, or Bluetooth devices, are necessary for the app to function properly. They seek clarity on how their personal data will be used and whether it will be handled responsibly and securely. However, many user reviews suggest that this information is either missing, difficult to locate, or not clearly explained within the app or privacy policy. Without clear and comprehensive explanations from developers, users may feel hesitant to grant these permissions, as they worry about potential misuse or unauthorized sharing of their data.

Since these are financial applications, which often involve sensitive personal and financial information, the lack of transparency is an even bigger concern. Some users specifically complain that the privacy policy is not linked at the point when permissions are requested within the app interface. Additionally, they note that while update descriptions inform them of newly added permissions and data access requirements, they do not clarify why these changes were made or how the data will be used. Among the apps considered in this paper, the apps from *Wells Fargo*[59] and *Sparkasse*[55], for example, do not provide a direct link to their privacy policy on their Play Store home pages, which may further contribute to user confusion. In addition, reviews frequently highlight the contrast between the core functionality of the app and the seemingly unrelated permissions it demands. Users find it difficult to justify why a simple banking or trading app would need access to their call logs or browsing history, for example. The perceived disconnect between the purpose of the app and the requested permissions raises skepticism and fuels concerns about potential data misuse. Again, some users express that they will not use the app until they receive an explanation or even uninstall the app altogether because of it. It is also notable that most of these reviews, despite explicitly asking for clarification, do not receive responses from the developers. However, popular finance apps receive a large number of reviews, making it difficult to respond to each one. Nonetheless, the absence of responses can leave users feeling ignored, reinforcing their perception that transparency and user concerns are not a priority for the developers.

5.2.4. Financial Data Selling

As a special case, trading apps are often criticized for selling user data to hedge funds. In this context, scam accusations are also frequently raised. However, this seems to be specifically related to the Gamestop scandal[1], in which users of the social media platform Reddit organized themselves to buy Gamestop shares, which subsequently drove up the price of the stock. In connection with subsequent losses of billions of dollars for large hedge funds, some trading apps removed the functionality to buy more of these shares, so that it was only possible to sell the shares and the value of the stock fell again. This caused great outrage among users, who accused the apps of collaborating with hedge funds. It is therefore not clear whether the apps really sell data to the hedge funds and thus pose a legitimate privacy issue for the users, or whether it is part of the loss of trust in these apps. [81, 82]

[1] https://www.theguardian.com/business/2021/jan/28/gamestop-how-reddits-amateurs-tripped-wall-streets-short-sellers1

5.2.5. Inadequate Security Measurements

Aside from permissions and data access, the other big topic that most reviews comment on is security measurements. Not all security topics are necessarily privacy-related, but data protection is also ensured by the security of the app, which is why it makes sense to also examine this more closely. In this respect some users criticize the lack of usability of Virtual Private Networks (VPN) when they want to use the app, as can be seen in the following reviews:

- "Can't sign in when using VPN. Turn VPN off and sign in works. VPN compatability should be a basic ticket to play feature on an app that has significant financial info. [...]", 1★
- "Does not work with VPN's. When using a VPN, the app will not allow you to login (the login screen fails before you can enter your username or password). Considering the security concerns, you think that you would work seamlessly regardless of using a VPN or not.", 2★

VPNs are a great way for users to generate additional security for themselves. They use powerful encryption algorithms to protect the internet traffic of users by creating a secure tunnel between their device and the VPN server. This makes VPNs especially crucial for users who access finance apps on the road since they protect users from potential eavesdropping and cyberattacks, which are more prevalent on unprotected or public Wi-Fi networks. This allows the user to further increase their level of privacy, even outside of the options offered by the app. If financial apps do not support VPN services, this can be a significant barrier for users who value security and privacy when accessing their financial data. Therefore users may be forced to choose between using the app without the added security of a VPN or finding alternatives that provide both the financial services they want and the level of security and privacy they require. [83]

Beside VPNs also some other security issues are addressed. Other reviews that relate to security aspects that are also relevant to privacy are, for example, the following:

- "[...] Security is a big issue, when you begin screen switching, the ANZ app displays your account balances. Although you have to PIN again to use the app, it should not display account balances when switching apps.", 2★
- "Why isn't there a near-instant, push-message, warning of potential fraudulent activity? A simple feature like that might help thwart those who keep causing me to have to file fraud claims. [...]", 2★
- "If I forget my password for the app, it is enough to simply reinstall it, you can then simply set a new one... so a piece of cake to crack the first of the 3 security levels. [...]", 1★

5.2.6. Password-related Concerns

Users often criticize password-related things, such as that only four-digit PINs are allowed, which are far too easy to determine, or that it is not possible to insert passwords (from password managers), which practically forces people to choose easier passwords that they can remember themselves. Also mentioned are missing logout buttons, which give users the feeling that their account is always half active (even if the app automatically logs out after closing). While such issues are not directly related to privacy, they do have an impact on it, because part of privacy is not only what data is collected and how it is handled, but also how it is protected from access by others. In the context of this, insecure password rules or the inadequate fraud warning measures mentioned in the review above can make users uncertain whether their sensitive financial data is sufficiently protected by the app. Which is why, especially in the area of security, it is necessary to make a distinction between issues that are generally common and those that are only temporary errors and were not intended as such.

In summary, the qualitative analysis of user reviews shows that users mainly have problems with excessive data access and permission requests from apps. Users express concern about the amount and selection of permissions on private data, and the lack of optionality in granting permissions also causes distrust. Also criticized are insufficient explanations about this. The other main topic is security, with specific criticism of the partial lack of support for VPNs, but also general other issues such as inadequate password policies and fraud warning systems. In general, these issues make users doubt the trustworthiness of the apps and may lead them to look for competitors with better privacy policies and security measures.

5.3. User Reviews and Privacy Regulations

User Reviews Reflect Privacy Regulations. The analysis of user reviews in this study reveals a close connection between the concerns raised by users and the requirements established by privacy regulations. Many of the issues highlighted in the reviews, such as lack of transparency, excessive permissions, and inadequate security measures, directly align with the core tenets of these regulations. For instance, in terms to the privacy policy transparency, GDPR Article 13 has specifically stipulated:

> Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
> (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
> ...
> (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
> ...

And CCPA §1798.130(a)(5) states:

> Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its internet website, and update that information at least once every 12 months:
> ...
> (i) A list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.
> (ii) The categories of sources from which consumers' personal information is collected.
> (iii) The business or commercial purpose for collecting, selling, or sharing consumers' personal information.
> (iv) The categories of third parties to whom the business discloses consumers' personal information.
> ...

The user reviews analysed in this study suggest that many financial apps fall short of these expectations. Users frequently report feeling uninformed about why certain data is being collected and how it will be used. For instance, user reviews of Bank of America say:

> - Not Working Well These Days Functions like mobile check cashing causes crashes, they want too much personal information and their **privacy policy** is weak... 2★
> - App keeps asking for social security number or tax ID. Does not seem to think security is important. It use to have security question, but not any more. Funny the **privacy policy** states they will not ask for social security number.. ever. 1★

Those requirements emphasize the need for transparent and accountable privacy policies in data handling, ensuring that users are fully informed about how their personal information is collected, used, and shared.

The Gap. Despite the existence of robust privacy regulations such as the GDPR and CCPA, there remains a significant gap between the regulatory frameworks and their practical implementation, as highlighted by user reviews. This discrepancy can be attributed to several factors:

- **Implementation Challenges**: While regulations like the GDPR and CCPA set clear expectations, the practical application of these rules is complex. For instance, ensuring that privacy policies are both comprehensive and easily understandable to the average user is a challenge that many financial apps have yet to fully address. The language used in privacy policies is often legalistic and dense, making it difficult for users to grasp the full extent of how their data is being used.

- **Global Applicability**: Financial apps often operate in multiple jurisdictions, each with its own privacy laws and regulations. Balancing compliance across these varied legal landscapes can lead to inconsistencies in how privacy practices are implemented, potentially leaving gaps in protection for users in certain regions.

- **User Trust and Perception**: Even when apps technically comply with privacy regulations, there is often a disconnect between compliance and user perception. If users feel that their privacy is not being respected, as evidenced by complaints about excessive permissions and unclear data usage policies, their trust in the app can erode. This gap between regulatory compliance and user trust underscores the importance of not only following the letter of the law but also addressing user concerns proactively.

5.4. Readability, Accessibility and Usefulness of Privacy Policies

Previous studies adopt the Flesch Reading Ease Scores to reflect the readability of privacy policies [84, 85]. The analysis revealed significant variations in the readability of privacy policies across different financial applications. As shown in Table 3, the scores ranged from a high of 50.19 for Sparkasse, indicating a moderate level of readability, to a low of 8.06 for Bank of America, suggesting that the text is very difficult to read. The average readability score is 29.09, indicating that many policies require college graduate level education background to read and understand them. The estimated average reading times also varied significantly, with the Australian Taxation Office's policy requiring the longest time at 136.66 minutes, and ANZ's policy being the shortest at 10.11 minutes. These findings highlight the potential burden on users to fully engage with lengthy and complex privacy documents.

The results of the readability and accessibility analysis reveal significant variations in the complexity of the privacy policies among the financial applications studied. The Flesch Reading Ease scores ranged from as high as 50.19 for Sparkasse, indicating moderate readability, to as low as 8.06 for Bank of America, suggesting that the document is very difficult to read. Additionally, the estimated reading times varied widely, with the Australian Taxation Office's policy requiring over two hours to read, while ANZ's policy could be read in approximately 10 minutes. These findings highlights the challenges users may face in understanding these documents.

As we observed in this paper, many privacy policies are written too long and too complex for users to read and understand. This is technically contrary to the requirements of the GDPR or BDSG in Germany, the Privacy Act of Australia and partly the GLBA of the USA, which all require *clear* and *easy* to understand privacy statements that explain the privacy practices of the respective company. This shows that "clear and understandable" are elastic terms and that policies that are perceived by law and by companies as understandable do not automatically have to be understandable to the user.

In order to evaluate the user understanding of privacy policies, a small survey was then conducted to see how the perception of users changes in relation to the original policy to the policy summary. The policy summary only contains information about personal information collected and purposes. We recruited ten users of aforementioned financial apps and divided them into two groups with five for each. The first group that received the original policy of the app is henceforth referred to as the "Original Group", while the other group that received the policy summary is referred to as the "Summary Group". The demographic of participants is listed below.

- Age-wise, the participants are very similar, with eight out of ten people being in the 18 to 25 age group. Only two people in the original group deviate from this with ages of 47 and 52.

Table 3
Flesch Reading Ease Scores and Estimated Reading Times of Privacy Policies

Application	Flesch Reading Ease Score	Reading Time (minutes)
Trade Republic	36.17	40.39
Sparkasse	50.19	19.11
VR Bank	46.78	25.01
TurboTax	27.66	40.02
Robinhood	29.75	17.53
Wells Fargo	20.83	13.34
Bank of America	8.06	16.69
Mitrade	19.16	11.14
Australian Taxation Office	16.31	136.66
Commonwealth Bank	26.33	29.63
ANZ	27.12	10.11
Westpac	45.79	46.26
NAB	27.63	28.04
UBank	25.52	14.26
Average	**29.09**	**32.01**

- In terms of educational attainment, the three younger members of the original group all have a Bachelor's degree, while the two older ones have a secondary school diploma. In the summary group, two have an A-level, and three also have a Bachelor's degree.

- In each of the two groups there is one person who has already had experience with data privacy and one person who does not use any financial apps. Likewise, of those who use financial apps, one per group has never given a thought to the privacy of that apps. In the original group, privacy in financial apps is (very) important to everyone, while in the summary group it is (very) important to four out of five participants, and surprisingly one does not care at all.

In the original group, the participants took an average of 18 minutes to read through the privacy policy, which everyone felt was far too long. Interestingly, no clear general age or educational differences can be identified in the understanding of the policy. While the oldest participant is the only one who found the policy difficult to understand, there is only one who found it easy, and the other three found it neither easy nor difficult. So on average, the original policy is moderately understandable. In general, the group had a moderate to good understanding of the tone and language of the policy, and they found it well-organized and structured. For one person the terms "*Werbe ID*" (engl. advertising ID) and "*HTTP Header incl. SDK Version*" were difficult to understand, for the others there were no specific difficult terms. It was rather moderately possible for the group to grasp the main points of the policy, but at the same time, it tended to be able to answer all of the privacy questions posed by the participants. However, all participants in the group agree that they would definitely not have read the policy if they had wanted to install the app.

In the summary group, the reading time was reduced considerably, with an average reading time of three minutes. However, even though the reading time was significantly reduced, the group still tended to perceive it as too long, although not as much as the group with the original policy. So it seems that even short reading times of a few minutes are not enough for users, but rather they want an overview that gives them all the information they need at a glance. The understandability of privacy policies is improved by the summary. Compared to the original group, the summary group praised that the policy summary is to read and understand, which means it improved from moderately understandable to rather easy to understand. Specifically, the tone and language, jargon of computer science, and the ability to grasp the main points are main factors behind the better understandability.

Interestingly, even though that summary group shows a greater reading willingness of privacy policy compared to original group, three of the participants still said that they would rather not have read the policy even in this form (i.e. summary). This means that although the reading time could be significantly reduced and the overall understanding improved in relation to the original policy, it still does not seem to be motivating for users to read it. There could be various reasons for this. On the one hand, the group still felt that the summary tended to be too long, which means that reading length could be a significant factor for users in deciding whether to deal with it or not. On the other hand, some users may not be strongly interested in reading privacy policies in general, because they believe that their personal information is collected by various services and platforms anyway and therefore have no motivation to read it.

It is important to recognize the limitations of this survey. Due to the small sample size and homogeneous demographic characteristics of the participants, the results cannot be simply generalized to the entire population. Nevertheless, the results offer promising evidence that the use of summaries can improve the understanding of privacy policies among users. However, they also highlight the difficulty of getting users to read them in the first place, which may require further research.

5.5. Comparative Analysis with Existing Literature

Prior research has explored the impact of privacy concerns on app trust and adoption rates [26, 25, 27]. Our findings align with studies indicating that user trust in financial applications is strongly influenced by the number and nature of permissions requested. Specifically, apps requesting access to sensitive data (e.g., location, contacts) tend to receive lower trust ratings, consistent with the observations in [26].

Furthermore, studies such as [25] highlight that permission transparency improves user acceptance. In our analysis, financial apps with clearly stated privacy policies and well-explained permission requests had significantly higher trust ratings than those with ambiguous policies. This finding reinforces previous work in [27], which showed that user comprehension of permission rationale positively impacts trust.

To quantify this effect, we examined the correlation between trust ratings and the number of permissions requested across the 15 selected financial apps. We observed a negative correlation ($r = *0.63, p < 0.01$), indicating that apps requiring extensive permissions generally received lower trust scores. This relationship aligns with prior studies on user privacy perceptions in mobile apps [26].

User Awareness and Psychological Factors: Beyond the statistical correlation, our findings also resonate with psychological models of user decision-making in privacy contexts. According to [28], users tend to exhibit privacy paradox behavior, where they express high concerns about data privacy but continue to grant permissions under perceived necessity or convenience. This phenomenon was particularly evident in finance-related apps, where users often tolerate high permission requests if the app is deemed essential for daily transactions. However, apps with vague explanations of data use still suffered from reduced trust scores, reinforcing the importance of privacy communication clarity.

Regulatory Influence on Privacy Perception: Additionally, our study aligns with previous research on the influence of regional privacy regulations on user trust. Studies on GDPR and similar frameworks [86] have shown that regulatory environments significantly affect user expectations and tolerance toward permission requests. We observed that users from the EU (Germany) exhibited stronger negative sentiments toward apps with excessive permission requests compared to users in Australia and the USA, where privacy regulations are relatively less stringent. This aligns with previous work on regulatory influence in user privacy perception [29].

Behavioral Trends in Financial App Trust: Another noteworthy trend from our study is that financial applications with robust user authentication mechanisms (such as two-factor authentication or biometric login) received higher trust ratings, even when requiring multiple permissions. This supports findings from [30], which argue that perceived security measures mitigate privacy concerns and enhance user trust. However, when security features were absent or unclear, the presence of excessive permissions led to higher distrust and negative reviews.

By integrating these comparisons, we provide a broader perspective on the significance of permission requests in shaping user trust, further emphasizing the need for transparent privacy practices in financial applications. Future work could expand this analysis by incorporating a larger dataset, cross-platform comparisons (e.g., iOS vs. Android), and user behavior tracking to assess how privacy concerns evolve over time.

6. Discussion

6.1. Comparison between Germany, Australia, and US

Although the privacy regulations are distinctly different, especially between the USA and the other two, it is interesting to note that there are little visible differences in privacy issues raised by users between these countries. Due to the state-level privacy laws approach of the USA, the limited scopes and partly specific definitions, there are significant differences and gaps in data protection, allowing some entities, which are not covered by any law, to exploit the data of their users [36]. That this can really cause differences in user rights is shown by the policy of *Robinhood* [87]. Users from California and Virginia are given extra rights due to specific privacy laws in those states. This includes, but is not limited to, the right to request details about the categories and specific elements of personal information collected by Robinhood in an easily usable format, the right to request deletion of their personal information, and the right to opt out of things like sharing their information with third parties or targeted advertising. At the same time, however, it is made clear that the laws, due to their limited scopes, do not apply to most of the information collected by Robinhood. The data protection situation and the related rights of users in the USA are significantly less comprehensive than in Germany and Australia, where general (almost) all-encompassing data protection laws apply. Therefore, it could be assumed that there should be more privacy issues in US apps, but this is apparently not the case. Our analysis of user reviews did not reveal any significant differences in the privacy issues of users in finance apps from the USA, Germany or Australia. Figure 6 also shows that the US apps do not stand out with negative scores. This means that even if there are considerable legal differences in data privacy in the three countries under consideration, these do not seem to have an significant effect on the user issues experienced by them (at least not in the case of the apps considered here).

The fact that no visible differences between the countries could be identified in the privacy issues expressed by users in financial apps may be due to the nature of these apps. Financial apps are a product of financial institutions, which often operate internationally and offer the app worldwide. As a result, they might implement global standards for privacy and security when developing their apps to meet the requirements and concerns of their customers as well as the legal frameworks of different countries. Further, financial apps tend to offer similar functions regardless of their geographic location, as things like banking and trading are the same internationally. Since the apps have similar functions, the associated privacy issues may also be similar. Following the same logic, users in different countries could also have similar behaviors when using financial apps, which would also lead to similar privacy concerns arising. Thus, similar privacy practices can be enforced internationally regardless of local laws, which could also be a reason for the similarity of the issues users have. However, this does not mean that the data protection problems in the countries are generally the same and that the laws make no difference, but only that there were no real noticeable differences in the issues expressed by the users in the context of this paper.

6.2. Permissions in Android Mobile Apps

Permissions are the pillar of data privacy management in Android mobile apps. In our analysis of user reviews in finance apps, a common user issue is the number and type of permissions requested, which seem to be disproportionate to the functionality of many finance apps, such as wanting camera or location access. One reason for this could be that it is easier for developers to ask for all the permissions that are needed for all the functionalities of the app from the start, rather than asking for them when they are actually needed. Especially things like location access are often used, sometimes even when the app is not actively used at all. Constant location access should actually be restricted by data protection laws such as the GDPR in Germany due to the prescribed data minimization, but can be justified by the developers with fraud protection. Thus, it is also possible that developers ask for all permissions in order to be able to collect more data about their users. On the other hand, users could also misjudge the permissions of the app. For example, if an app needs access to the gallery of the user in order to allow him to upload photographed invoices, the user may perceive it as if the app processes all his pictures, even though this is not the case. Regardless of whether the "fault" lies with the developers or the users, in both cases the problem is ultimately related to the other two core issues users have regarding permissions, namely lack of optionality and explanations.

If optionality was offered everywhere possible and all required permissions and data usage were clearly and comprehensively explained, then the aforementioned problems should also disappear. The reason why

Country	Regulation	Scope	Key Principles	Enforcement and Penalties
Germany	**GDPR**	Applies to all organizations processing personal data of EU residents, regardless of location.	Data minimization, purpose limitation, transparency, accountability, security, and lawful processing.	Enforced by Data Protection Authorities; fines up to €20M or 4% of global turnover.
	BDSG	Complements GDPR with national-level requirements, including specific employee data protection rules.	Ensures transparency in data collection and promotes anonymization where feasible.	Fines up to €300K for severe violations; imprisonment for intentional misuse.
Australia	**Privacy Act 1988**	Covers businesses with annual revenue above 3M AUD, government agencies, and some small businesses.	Defines how personal information must be collected, used, and disclosed; includes breach notification requirements.	Enforced by OAIC; penalties up to 2.5M AUD for serious violations.
	Australian Privacy Principles (APPs)	A set of 13 principles outlining responsible handling of personal data.	Focuses on transparency, access rights, security, and purpose limitation.	Organizations must comply with APPs or face enforcement actions by OAIC.
USA	**GLBA**	Applies to financial institutions handling consumer financial data.	Requires financial privacy notices, security programs, and opt-out mechanisms.	Enforced by FTC and federal banking agencies; non-compliance can result in fines and imprisonment.
	FCRA	Regulates consumer credit reporting and data sharing.	Defines permissible uses of consumer credit reports and mandates consumer rights to access and dispute inaccuracies.	Enforced by CFPB and FTC; violations can lead to fines and damages to affected consumers.
	CCPA California	Grants California residents privacy rights over their personal data.	Right to access, delete, and opt-out of data sales; businesses must disclose data practices.	Enforced by California Attorney General; fines up to $7,500 per intentional violation.

Table 4
Comparison of Privacy Laws in Germany, Australia, and USA.

developers do not offer optionality everywhere will probably have the same reasons as mentioned before. They may also assume that most users will agree to the permissions either way, so they tend to follow a “all-or-nothing” approach.

6.3. Privacy Policy Existence of Financial Apps

Not all apps link their privacy policy on their homepage, let alone have one. This was also confirmed by the apps selected in this paper. The *Sparkasse* and *Wells Fargo* apps both do not have a privacy policy linked in the Google Play app store, which represents a deficiency, especially considering the size and significance of these banks. So when users encounter apps that do not link a privacy policy, they may not search for it externally but assume that there is none and complain accordingly that there are no explanations for their privacy practices. On the other hand, other works have shown that privacy policies are also often simply not being read [85, 88]. Be it because of their length or the sometimes difficult way they are written. One reason for the explanation issue of many users could accordingly be that they do not (want to) undertake the work to read the privacy policy and do not get any information when the request for permissions is made, which is why there is a lack of explanations for them. It can also be that they read the policy, but it is not precise enough or written too complex, so they still do not understand it. For example, many apps also use collective terms to describe the reasons why certain permissions are necessary, such as “app functionality” or “marketing purposes”, thus fulfilling what is sometimes a legal requirement but still not providing users with valuable information.

Since 2022, the Google Play app store had required all apps to disclose their privacy practices, so it could be assumed that users should be informed about what permissions are required and why [89]. However, in a paper by David Rodriguez et. al. [89] it was shown that 44.3 %, so almost half of the 822 apps they analyzed, ask for permissions for data that is not listed in the app pages of their privacy practices. So the information in the app stores cannot be relied upon either. So there are various reasons why users lack explanations for the various permissions that the apps ask for. Since this problem occurs among users in all three countries considered in this paper, it can also be concluded that the laws still need to be improved in this regard.

6.4. Implicit Privacy Concerns

It is noticeable that the main privacy issues identified by users are generally only “direct” problems, such as permissions required by the app, missing explanations, no VPN functionality, or insufficient PIN settings. Users mainly notice things as problematic that they actively encounter. Privacy aspects, such as to whom the collected data is passed on and for what purpose, are also very important, but they happen in the background and are therefore not really present for the users. Many users are probably not really involved with such details, which is why issues that have a direct influence on the app and its functionalities dominate.

In addition to the privacy issues, it became clear in our analysis that privacy-related reviews generally make up a very small proportion of the reviews and that despite many issues mentioned, many users also praise the security and privacy of the respective apps. One reason for this could be that many users probably look at the app as a whole. As long as it fulfills its purpose in terms of design and functionality and there are no obvious data protection or security problems, such as the lack of a password prompt in a banking app, users could rate it positively despite possible privacy concerns. Furthermore, many users may not be fully informed about privacy issues or understand the actual impact that certain permissions and data uses of the app have on their privacy. In such cases, they may still consider the app to be safe and privacy-friendly.

6.5. Implications for App Developers

App persmissions: Major issues for many finance app users is the large amount of permissions, their lack of optionality, and insufficient explanations for why they are needed. Many users have clear expectations about how their data should be handled, and finance app developers should strive for a balance between app functionality and user privacy. To achieve this, app developers should examine the permissions their apps require and analyze which of those are truly mandatory in order to limit the number of permissions to what is necessary.

Opt-in permissions: Whereever possible, users should be given the option to specifically grant or deny permissions. Especially for data accesses that are not directly related to the app functionality, such as collecting device information for marketing purposes, users should be asked whether they want to share this data or not. The app should still be able to function in the main without some of these permissions being granted.

User-specified and one-time permissions: it may be possible to introduce individual one-time permissions for specific cases, which are queried again each time they are to be used. This could include cases such as when a banking app wants to have access to the camera of the user in order to be able to photograph bills directly in the app. By changing this from a continuous permission to a one-time permission, the app could avoid the feeling of the user that the app can continuously access his or her camera and record what it sees. Providing choices allows users to customize their app experience while maintaining control over their data. App developers could also implement their data access rules directly as a settings option in the app, where users can easily adjust their permissions or request to delete collected data if they wish.

Alternate permissions and functions: For some app permissions, where it is possible, it could be considered to offer alternative functions for users, in case they do not want to grant permissions that would be necessary for certain functions. For example, if a banking app wants to access the location of the users in order to provide them with information about ATMs in their area, if they refuse, only a general map with all available ATMs could be displayed, in which they can search for their location themselves. In this way, the basic functionalities of the app could be preserved without users, who are concerned about their privacy, having to give up anything.

Better explained permissions: Communicating the purpose and need for the various permissions requested in a transparent and clear manner can significantly contribute to users trusting the app more. After all, when users are asked to allow access to their data or device features, they rightly expect a detailed explanation of the purpose for which the app requires these permissions and how their data will be used. As could be seen from the reviews, without this transparency, some users are otherwise reluctant to continue using the app or to install it at all, because they fear possible misuse of their data or general monitoring by the app provider. One solution for this could be to integrate the explanations for the respective permissions directly into the app. When users are first asked to grant certain permissions, developers could display brief and easy-to-understand explanations of why each of those permissions is necessary for the functionality of the app [88].

Responding to reviews: Developers should try to respond to reviews that express concerns about app data usage and app permissions and explain them to requesters. By publicly responding to questions and concerns raised by users, they could better demonstrate their commitment to transparency and user satisfaction.

More readable and accessible privacy policies: The readability and accessibility analysis provides critical insights into the user experience of engaging with privacy policies. Policies with lower Flesch Reading Ease scores and longer reading times are likely to be more challenging for users to comprehend, potentially leading to lower levels of engagement and trust. Our analysis suggests that financial applications need to prioritize the simplification of their privacy policies to make them more accessible to a broader audience. By doing so, they can enhance transparency and encourage greater user trust, which is essential for maintaining compliance with privacy regulations and ethical standards. Moreover, our analysis of privacy policies found many are too complex in terms of language and take too long to read. In addition, it is unclear to many users from their reviews that they understand the implications of some privacy policy elements, along with some app permissions requested. Additionally, in the app and on the app page in the respective store, a comprehensive privacy policy should be linked, which is tailored to the app. However, this is not done for most of apps so far [85, 80]. In this way, the needs of users who want to know in detail and for whom brief explanations are not enough could also be met.

7. Threats to Validity

Despite the robustness of our methodology, certain limitations and threats to validity should be considered when interpreting our findings. While these limitations exist, we believe that our multi-method approach ensures a balanced, in-depth analysis of privacy concerns in financial applications. By outlining these limitations, we aim to provide transparency and guide future work in refining privacy analysis methodologies.

Selection Bias and Dataset Representativeness: Our dataset consists of 15 financial applications selected based on their popularity in the Google Play Store across three countries. While this ensures the inclusion of widely used apps, it may not fully capture the diversity of financial applications available on alternative platforms, such as the Apple App Store or region-specific marketplaces. Future studies could broaden the dataset by incorporating a wider selection of apps to enhance generalizability.

Qualitative Evaluation and Observer Bias: The qualitative analysis in this study involved manually reviewing and categorizing user reviews. While efforts were made to ensure consistency and objectivity, including cross-validation by multiple researchers, the possibility of observer bias remains. To mitigate this, we applied a stratified random sampling approach to ensure diverse representation of user reviews. However, future research could incorporate automated NLP-based techniques, such as thematic clustering or sentiment analysis, to reduce subjectivity in qualitative assessments.

Focus on Negative Reviews and Privacy Concerns: One of the methodological choices in our study was to concentrate primarily on one- and two-star user reviews. This decision aligns with our specific focus on privacy-related concerns in financial applications. Negative reviews are more likely to contain explicit complaints about perceived privacy violations, confusing permission requests, or dissatisfaction with data handling practices. While this focus strengthens our ability to extract relevant insights about privacy issues, it also introduces a potential limitation in terms of scope. Reviews with neutral or positive ratings may still contain valuable feedback on privacy practices, including endorsements of transparency or satisfaction with policy clarity. However, since our study aimed to capture the most pressing and critical concerns, we intentionally limited our qualitative review to the most negative cases. This may reduce the representation of more balanced or positive experiences. Future work could address this by incorporating a broader spectrum of user ratings, including neutral reviews, to provide a more comprehensive view of privacy perceptions across the full range of user experiences.

Temporal Validity and Dynamic Privacy Policies: Financial applications frequently update their privacy policies and data handling practices in response to regulatory changes (e.g., GDPR updates) and user feedback. As a result, some findings in this study may become outdated over time. Future research could adopt a longitudinal approach, analyzing how privacy policies evolve over extended periods and how these changes influence user perceptions.

Regional Differences in Privacy Perceptions: While our study compares financial apps from Germany, Australia, and the USA, privacy concerns and regulatory frameworks vary across different jurisdictions. This study focuses on three regions with distinct regulatory landscapes, but the findings may not be fully generalizable to other countries with different privacy expectations and enforcement mechanisms. Future studies could expand the geographical scope to include additional countries with varying privacy laws and cultural attitudes toward data protection.

Reliability of User Reviews as a Data Source: User reviews serve as a valuable resource for understanding privacy concerns, but they also present certain limitations. Users may not always articulate their privacy concerns explicitly, leading to potential underrepresentation of specific issues. Moreover, fake or manipulated reviews could influence the analysis. To address this, we filtered out low-quality and spam-like reviews, but future research could explore sentiment-weighted ranking algorithms to further refine review credibility assessments.

8. Conclusion

In this paper, we explored the privacy concerns and regulatory landscapes of financial mobile applications in Germany, Australia, and the United States. Our analysis includes a detailed review of user feedback from app stores, highlighting prevalent privacy issues and regional differences in user concerns. We identified six primary privacy concerns in user reviews, including excessive permission requests, all-or-nothing permissions, non-transparent privacy policies, finance data sale, inadequate security measures, and password-related concerns. Despite large privacy law differences, we found no significant differences in user privacy concerns about their financial apps between countries of use. This study also highlights the importance of readability and accessibility in the design of privacy policies for financial applications. The analysis of Flesch Reading Ease scores and estimated reading times reveals that many of these documents are difficult to read and require significant time commitments, which may deter users from fully engaging with them. To improve user comprehension and trust, it is recommended that financial applications simplify their privacy policies, making them more accessible and user-friendly. Such efforts are crucial not only for ensuring compliance with legal requirements but also for enhancing the overall user experience and fostering a more transparent digital environment. This work has contributed to a better understanding of key privacy concerns of financial app users and for increased data security, more informed user decisions, and more effective communication of software privacy practices in the financial apps sector.

9. Data Availability

The full code used in this paper and the reviews and survey results are stored in a GitHub repository, which can be found at the following link:
https://github.com/HumaniSELab/An_Analysis_of_Privacy_Regulations_and_User_Concerns_of_Finance_Mobile_Applications

Acknowledgements

Haggag is supported by a National Intelligence Post-doctoral Fellowship. Grundy and Haggag were supported by ARC Laureate Fellowship FL190100035 and Discovery Project DP200100020.

References

[1] D. Curry, Finance App Revenue and Usage Statistics (2023), https://www.businessofapps.com/data/finance-app-market/, accessed: 29.07.2023.

[2] J. Research, Number of active online banking users worldwide in 2020 with forecasts from 2021 to 2024, by region, https://www.statista.com/statistics/1228757/online-banking-users-worldwide/, accessed: 29.07.2023.

[3] apple.com, Apple Pay, https://www.apple.com/au/apple-pay/, accessed: 17.05.2023.

[4] google.com, Google Pay, https://pay.google.com/, accessed: 17.05.2023.

[5] support.apple.com, Countries and regions that support Apple Pay, https://support.apple.com/en-au/HT207957, accessed: 17.05.2023.

[6] support.google.com, Countries or regions where you can make payments with Google, https://support.google.com/googlepay/answer/12429287?hl=en#zippy=%2Cpay-in-store, accessed: 17.05.2023.

[7] E. C. Bank, Study on the payment attitudes of consumers in the euro area (SPACE), https://www.ecb.europa.eu/pub/pdf/other/ecb.spacereport202012~bb2038bbb6.en.pdf, accessed: 29.07.2023.

[8] statista.com, Finance - Worldwide, https://www.statista.com/outlook/dmo/app/finance/worldwide, accessed: 16.05.2023.

[9] A. Petrosyan, Distribution of cyber attacks across worldwide industries in 2022, https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/, accessed: 20.05.2023.

[10] A. Petrosyan, Most important consequences of cyber attacks worldwide in 2022, https://www.statista.com/statistics/1327148/main-consequences-cyber-attacks-cybersecurity-worldwide/, accessed: 20.05.2023.

[11] A. Petrosyan, Largest data breaches in financial industry worldwide as of May 2022, by number of compromised records, https://www.statista.com/statistics/1323568/largest-data-breaches-in-financial-sector-worldwide/, accessed: 29.07.2023.

[12] W. Maalej, Z. Kurtanović, H. Nabil, C. Stanik, On the automatic classification of app reviews, Requirements Engineering 21 (3) (2016) 311–331. doi:10.1007/s00766-016-0251-9.
URL https://doi.org/10.1007/s00766-016-0251-9

[13] S. Mcilroy, W. Shang, N. Ali, A. E. Hassan, User reviews of top mobile apps in Apple and Google App Stores, Communications of the ACM 60 (2017) 62–67. doi:10.1145/3141771.

[14] R. Flesch, A new readability yardstick, Journal of Applied Psychology 32 (3) (1948) 221–233. doi:10.1037/h0057532.

[15] W. H. DuBay, The Principles of Readability, Impact Information, Costa Mesa, CA, 2004.
URL https://www.impact-information.com/impactinfo/readability02.pdf

[16] J. Kim, J. Barone, N. Elhadad, J. Vasilakes, Readability of consumer health information: An analysis of the cdc website, Studies in Health Technology and Informatics 264 (2019) 1952–1953. doi:10.3233/SHTI190721.

[17] F. Boissay, T. Ehlers, L. Gambacorta, H. S. Shin, Big Techs in Finance: On the New Nexus Between Data Privacy and Competition, Springer International Publishing, Cham, 2021, pp. 855–875. doi:10.1007/978-3-030-65117-6_31.
URL https://doi.org/10.1007/978-3-030-65117-6_31

[18] V. Ferrari, Crosshatching Privacy: Financial Intermediaries' Data Practices between Law Enforcement and Data Economy, Eur. Data Prot. L. Rev. 6 (2020) 522.

[19] A. I. Antón, J. B. Earp, Q. He, W. Stufflebeam, D. Bolchini, C. Jensen, Financial Privacy Policies and the Need for Standardization, IEEE Security & Privacy 2 (2004) 36–45. doi:10.1109/MSECP.2004.1281243.

[20] A. K. Jain, D. Shanbhag, Addressing Security and Privacy Risks in Mobile Applications, IT Professional 14 (5) (2012) 28–33. doi:{10.1109/MITP.2012.72}.

[21] J. Huebner, R. M. Frey, C. Ammendola, E. Fleisch, A. Ilic, What People Like in Mobile Finance Apps: An Analysis of User Reviews, in: Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia, MUM '18, Association for Computing Machinery, New York, NY, USA, 2018, pp. 293—-304. doi:10.1145/3282894.3282895.
URL https://doi.org/10.1145/3282894.3282895

[22] S. Zimmeck, Z. Wang, L. Zou, R. Iyengar, B. Liu, F. Schaub, S. Wilson, N. Sadeh, S. Bellovin, J. Reidenberg, Automated Analysis of Privacy Requirements for Mobile Apps, in: The 2016 AAAI Fall Symposium Series: Privacy and Language Technologies, 2017, pp. 286–296. doi:10.14722/ndss.2017.23034.

[23] H. Zhu, H. Xiong, Y. Ge, E. Chen, Mobile App Recommendations with Security and Privacy Awareness, in: Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD '14, Association for Computing Machinery, New York, NY, USA, 2014, pp. 951—-960. doi:10.1145/2623330.2623705.
URL https://doi.org/10.1145/2623330.2623705

[24] O. Haggag, J. Grundy, M. Abdelrazek, S. Haggag, A large scale analysis of mHealth app user reviews, Empirical Software Engineering 27 (7) (2022) 196. doi:10.1007/s10664-022-10222-6.
URL https://doi.org/10.1007/s10664-022-10222-6

[25] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, D. Wagner, Android permissions: User attention, comprehension, and behavior, in: Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS), ACM, 2012, pp. 3:1–3:14.

[26] J. Lin, S. E. Smith, J. I. Hong, N. Sadeh, Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings, in: Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS), USENIX, 2014, pp. 199–212.

[27] H. Almuhimedi, F. Schaub, N. Sadeh, A. Acquisti, L. F. Cranor, Your location has been shared 5,398 times! a field study on mobile app privacy nudging, Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI) (2015) 787–796.

[28] A. Acquisti, L. Brandimarte, G. Loewenstein, Privacy and human behavior in the age of information, Science 347 (6221) (2015) 509–514. doi:10.1126/science.aaa1465.

[29] F. Trevisan, K. Girginova, Regulating privacy in the digital age: Users' attitudes towards gdpr and online privacy practices, Telematics and Informatics 61 (2021) 101603. doi:10.1016/j.tele.2021.101603.

[30] P. Sun, X. Yuan, Y. Zeng, Exploring the relationship between perceived security, trust, and adoption of mobile financial services, in: Proceedings of the International Conference on Information Systems (ICIS), AIS, 2018, pp. 1–17.

[31] J. Tsai, S. Egelman, L. F. Cranor, A. Acquisti, The effect of online privacy information on purchasing behavior: An experimental study, in: Information Systems Research, Vol. 22, INFORMS, 2011, pp. 254–268.

[32] europa.eu, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, accessed: 04.06.2023.

[33] B. der Justiz, Bundesdatenschutzgesetz (BDSG), https://www.gesetze-im-internet.de/bdsg_2018/BDSG.pdf, accessed: 04.06.2023.

[34] D. Zhang, P. Finckenberg-Broman, T. Hoang, S. Pan, Z. Xing, M. Staples, X. Xu, Right to be forgotten in the era of large language models: Implications, challenges, and solutions, arXiv preprint arXiv:2307.03941.

[35] legislation.gov.au, Privacy Act 1988, https://www.legislation.gov.au/Details/C2022C00361, accessed: 06.06.2023.

[36] L. Barrett, Confiding in Con Men: US privacy law, the GDPR, and information fiduciaries, Seattle UL Rev. 42 (2018) 1057.

[37] govinfo.gov, HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996, https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf, accessed: 15.06.2023.

[38] ecfr.gov, CHILDREN'S ONLINE PRIVACY PROTECTION RULE, https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312, accessed: 15.06.2023.

[39] nces.ed.gov, Family Educational Rights and Privacy Act (FERPA), https://nces.ed.gov/forum/dataethicscourse/additional-materials/family-educational-rights.pdf, accessed: 15.06.2023.

[40] justice.gov, PUBLIC LAW 99-508—OCT. 21, 1986, https://www.justice.gov/sites/default/files/jmd/legacy/2013/09/06/act-pl99-508.pdf, accessed: 16.06.2023.

[41] govinfo.gov, GRAMM–LEACH–BLILEY ACT, https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf, accessed: 16.06.2023.

[42] ftc.gov, Fair Credit Reporting Act, https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf, accessed: 15.06.2023.

[43] A. Chander, M. E. Kaminski, W. McGeveran, Catalyzing privacy law, Minn. L. Rev. 105 (2020) 1733.

[44] A. Desai, US State Privacy Legislation Tracker, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/, accessed: 13.07.2023.

[45] law.lis.virginia.gov, Chapter 53. Consumer Data Protection Act., https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/, accessed: 19.06.2023.

[46] cga.ct.gov, Substitute Senate Bill No. 6, https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF, accessed: 19.06.2023.

[47] leg.colorado.gov, SENATE BILL 21-190, https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf, accessed: 19.06.2023.

[48] cppa.ca.gov, CALIFORNIA CONSUMER PRIVACY ACT OF 2018, https://cppa.ca.gov/regulations/pdf/cppa_act.pdf, accessed: 19.06.2023.

[49] M. Si, S. Pan, D. Liao, X. Sun, Z. Tao, W. Shi, Z. Xing, A solution toward transparent and practical ai regulation: Privacy nutrition labels for open-source generative ai-based applications, arXiv preprint arXiv:2407.15407.

[50] S. Pan, D. Zhang, M. Staples, Z. Xing, J. Chen, X. Xu, T. Hoang, Is it a trap? a large-scale empirical study and comprehensive assessment of online automated privacy policy generators for mobile apps, in: 33rd USENIX Security Symposium (USENIX Security 24), USENIX Association, Philadelphia, PA, 2024, pp. 5681–5698.
URL https://www.usenix.org/conference/usenixsecurity24/presentation/pan-shidong-trap

[51] Appbrain, https://www.appbrain.com/, Accessed: 2022-08-26.

[52] support.google.com, App Discovery and Ranking, https://support.google.com/googleplay/android-developer/answer/9958766?hl=en, accessed: 24.05.2023.

[53] play.google.com, Taxfix: Online Steuererklärung, https://play.google.com/store/apps/details?id=de.taxfix&hl=de&gl=de, accessed: 28.05.2023.

[54] play.google.com, Trade Republic: Aktien, Crypto, https://play.google.com/store/apps/details?id=de.traderepublic.app&hl=de&gl=de, accessed: 28.05.2023.

[55] play.google.com, Sparkasse Ihre mobile Filiale, https://play.google.com/store/apps/details?id=com.starfinanz.smob.android.sfinanzstatus&hl=de&gl=de, accessed: 28.05.2023.

[56] play.google.com, VR Banking - einfach sicher, https://play.google.com/store/apps/details?id=de.fiduciagad.banking.vr&hl=de&gl=de, accessed: 28.05.2023.

[57] play.google.com, TurboTax: File Your Tax Return, https://play.google.com/store/apps/details?id=com.intuit.turbotax.mobile&hl=en&gl=US, accessed: 28.05.2023.

[58] play.google.com, Robinhood: Stocks & Crypto, https://play.google.com/store/apps/details?id=com.robinhood.android&hl=en_US, accessed: 28.05.2023.

[59] play.google.com, Wells Fargo Mobile, https://play.google.com/store/apps/details?id=com.wf.wellsfargomobile&hl=en&gl=US, accessed: 28.05.2023.

[60] play.google.com, Bank of America Mobile Banking, https://play.google.com/store/apps/details?id=com.infonow.bofa&hl=en&gl=US, accessed: 28.05.2023.

[61] play.google.com, Mitrade - Trade Global Markets, https://play.google.com/store/apps/details?id=com.mitrade.mobile&hl=en_AU&gl=au, accessed: 28.05.2023.

[62] play.google.com, Australian Taxation Office, https://play.google.com/store/apps/details?id=au.gov.ato.ATOTax&hl=en_AU&gl=au, accessed: 28.05.2023.

[63] play.google.com, CommBank, https://play.google.com/store/apps/details?id=com.commbank.netbank&hl=en_AU&gl=au, accessed: 28.05.2023.

[64] play.google.com, ANZ Australia, https://play.google.com/store/apps/details?id=com.anz.android.gomoney&hl=en_AU&gl=au, accessed: 28.05.2023.

[65] play.google.com, Westpac, https://play.google.com/store/apps/details?id=org.westpac.bank&hl=en_AU&gl=au, accessed: 28.05.2023.

[66] play.google.com, NAB Mobile Banking, https://play.google.com/store/apps/details?id=au.com.nab.mobile&hl=en_AU&gl=au, accessed: 28.05.2023.

[67] play.google.com, Ubank Money App, https://play.google.com/store/apps/details?id=au.com.bank86400&hl=en_AU&gl=au, accessed: 28.05.2023.

[68] H. P. Langtangen (Ed.), Advanced Python, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008, pp. 319–449. doi:10.1007/978-3-540-73916-6_8.
URL https://doi.org/10.1007/978-3-540-73916-6_8

[69] JoMingyu, Google-Play-Scraper, https://github.com/JoMingyu/google-play-scraper, accessed: 24.05.2023.

[70] S. Han, Googletrans, https://github.com/ssut/py-googletrans, accessed: 29.05.2023.

[71] I. Caswell, Google Translate learns 24 new languages, https://blog.google/products/translate/24-new-languages/, accessed: 28.06.2023.

[72] M. O. Prates, P. H. Avelar, L. C. Lamb, Assessing gender bias in machine translation: a case study with google translate, Neural Computing and Applications 32 (2020) 6363–6381. doi:https://doi.org/10.1007/s00521-019-04144-6.

[73] O. Haggag, S. Haggag, J. Grundy, M. Abdelrazek, COVID-19 vs Social Media Apps: Does Privacy Really Matter?, in: 2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS), 2021, pp. 48–57. doi:10.1109/ICSE-SEIS52602.2021.00014.

[74] K. Soumya George, S. Joseph, Text classification by augmenting bag of words (BOW) representation with co-occurrence feature, IOSR Journal of Computer Engineering 16 (1) (2014) 34–38.

[75] I. Rufai, E. Ilker, Comparison of quota sampling and stratified random sampling, Biometrics & Biostatistics International Journal 10 (1) (2021) 24–27. doi:10.15406/bbij.2021.10.00326.

[76] S. McIlroy, N. Ali, H. Khalid, A. E. Hassan, Analyzing and automatically labelling the types of user issues that are raised in mobile app reviews, Empirical Software Engineering 21 (2016) 1067–1106. doi:https://doi.org/10.1007/s10664-015-9375-7.

[77] A. S. Acharya, A. Prakash, P. Saxena, A. Nigam, Sampling: Why and how of it, Indian Journal of Medical Specialties 4 (2) (2013) 330–333.

[78] H. Cui, R. Trimananda, A. Markopoulou, S. Jordan, ˆPoliGraph‘: Automated privacy policy analysis using knowledge graphs, in: 32nd USENIX Security Symposium (USENIX Security 23), 2023, pp. 1037–1054.

[79] H. Harkous, K. Fawaz, R. Lebret, F. Schaub, K. G. Shin, K. Aberer, Polisis: Automated analysis and presentation of privacy policies using deep learning, in: 27th USENIX Security Symposium (USENIX Security 18), 2018, pp. 531–548.

[80] S. Pan, T. Hoang, D. Zhang, Z. Xing, X. Xu, Q. Lu, M. Staples, Toward the cure of privacy policy reading phobia: Automated generation of privacy nutrition labels from privacy policies, arXiv preprint arXiv:2306.10923.

[81] Y. Li, GameStop, Reddit and Robinhood: A full recap of the historic retail trading mania on Wall Street, https://www.cnbc.com/2021/01/30/gamestop-reddit-and-robinhood-a-full-recap-of-the-historic-retail-trading-mania-on-wall-street.html, accessed: 22.07.2023.

[82] A. Abdel-Qader, German Retail Brokers Suffer Trading Outage Amid GameStop Saga, https://www.financemagnates.com/forex/brokers/german-retail-brokers-suffer-trading-outage-amid-gamestop-saga/, accessed: 22.07.2023.

[83] nordvpn.com, What is a VPN?, https://nordvpn.com/what-is-a-vpn/, accessed: 22.07.2023.

[84] W. G. Voss, Looking at european union data protection law reform through a different prism: The proposed eu general data protection regulation two years later, Journal of Internet Law 17 (9).

[85] S. Pan, D. Zhang, M. Staples, Z. Xing, J. Chen, X. Xu, J. Hoang, A large-scale empirical study of online automated privacy policy generators for mobile apps, arXiv preprint arXiv:2305.03271.

[86] E. Union, General data protection regulation (gdpr) 2018, Official Journal of the European Union.
URL https://eur-lex.europa.eu/eli/reg/2016/679/oj

[87] robinhood.com, Robinhood Privacy Policy, https://robinhood.com/us/en/support/articles/privacy-policy/, accessed: 25.07.2023.

[88] S. Pan, Z. Tao, T. Hoang, D. Zhang, T. Li, Z. Xing, S. Xu, M. Staples, T. Rakotoarivelo, D. Lo, ˆA New Hope‘: Contextual privacy policies for mobile applications and an approach toward automated generation, arXiv preprint arXiv:2402.14544.

[89] D. Rodriguez, A. Jain, J. M. del Alamo, N. Sadeh, Comparing Privacy Label Disclosures of Apps Published in Both the App Store and Google Play Stores, in: 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE Computer Society, 2023, pp. 150–157.