An Analysis of Privacy Issues and Policies of eHealth Apps

Omar Haggag[1], John Grundy[1][a] and Mohamed Abdelrazak[2]
[1] *HumaniSE Lab, Department of Software Systems and Cybersecurity, Faculty of IT, Monash University, Australia*
[2] *A2I2, Deakin University, Australia*
{*omar.haggag, john.grundy*}*@monash.edu, mohamed.abdelrazek@deakin.edu.au*

Keywords: eHealth apps, Privacy Policies, Data Use Agreements, User Reviews, Ethics, Guidelines, Recommendations

Abstract: Privacy issues in mobile apps have become a key concern of researchers, practitioners and users. We carried out a large-scale analysis of eHealth app user reviews to identify their key privacy concerns. We then analysed eHealth app privacy policies to assess if such concerns are actually addressed in these policies, and if the policies are clearly understood by end users. We found that many eHealth app privacy policies are imprecise, complex, require substantial effort to read, and require high reading ability from app users. We formulated several recommendations for developers to help address issues with app privacy concerns and app privacy policy construction. We developed a prototype tool to aid developers in considering and addressing these issues when developing their app privacy behaviours and policies.

1 INTRODUCTION

Most people use eHealth apps to monitor and improve their health, where these apps collect substantial personal data, including sensitive information under GDPR and APA regulations (Rowland et al., 2020; Parker et al., 2019; Bradford et al., 2020). eHealth apps gather details like names, genders, ages, and medical histories. Due to the data's sensitive nature, eHealth apps pose significant privacy risks, making user awareness significant before download or usage (Parker et al., 2019; O'Loughlin et al., 2019). Many eHealth apps require access to device features like cameras and contacts, raising concerns about the misuse of personal information, as some of these apps can function without these permissions (Benjumea et al., 2020; Papageorgiou et al., 2018; Tahaei et al., 2022). The lack of transparency in how much sensitive data is collected is worrisome, especially with apps that are ad-supported or may sell user data (O'Loughlin et al., 2019; Robillard et al., 2019; Huckvale et al., 2015). This data sharing often happens without users' knowledge or consent and exposes them to privacy breaches by third parties (ur Rehman, 2019; Hinds et al., 2020; Hu, 2020).

To protect user privacy, eHealth app developers must adhere to guidelines like HIPAA, CalOPPA, and CCPA in the U.S. These laws require apps collecting data from Californians to provide a clear privacy policy outlining data types, collection methods, and purposes (Chen et al., 2021; Zimmeck et al., 2021). eHealth apps must display their privacy policy and terms of service before release on platforms like the App Store or Google Play (Sunyaev et al., 2015). Users have rights over their data, including opting out of data collection and restricting data sale or sharing (Dehling et al., 2015). European GDPR regulations reinforce this, demanding user consent for data collection and allowing users to access, copy, and request deletion of their data (Mulder, 2019; Liu et al., 2021).

Many eHealth app users accept privacy policies without fully reading them, often because these policies are lengthy and complex, and users lack the time for thorough understanding (Okoyomon et al., 2019; Ibdah et al., 2021). Surveys reveal the average Australian encounters 116 privacy policies totalling 467,000 words (Choice, 2022), and a US study found that understanding a company's data practices from a privacy policy takes over 15 minutes (Times, 2019). Consequently, users frequently express privacy-related complaints and issues in eHealth app reviews.

To further investigate this problem we conducted a comprehensive study to better understand (i) user concerns with eHealth app privacy; (ii) the privacy policies of a range of eHealth apps; (iii) the readability and understandability of these policies; and (iv) key areas for improvement. The key contributions of

[a] https://orcid.org/0000-0003-4928-7076

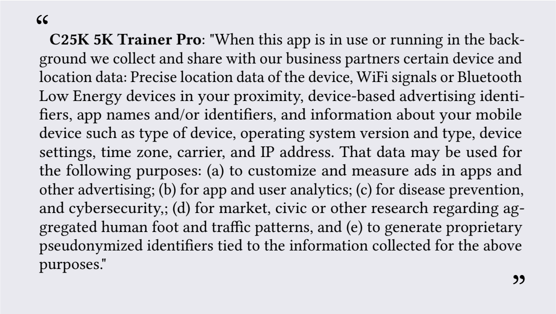
this work include:

- Automated and manual analysis of about 5.1 million user reviews of 276 eHealth apps, categorising privacy issues into 8 key areas;
- In-depth analysis of privacy policies and data use agreements of these apps, highlighting the need for better user awareness of app privacy behaviours;
- Evaluation of the complexity and readability of these privacy policies, finding most are complex and take over 15 minutes to read

2 MOTIVATION

eHealth apps, handling sensitive data, face significant risks if this information is mishandled or unintentionally shared (Robillard et al., 2019). Countries often legally require eHealth apps to have a Privacy Policy when collecting or sharing personal information (Arellano et al., 2018). This policy signifies compliance with local and global laws (Jensen and Potts, 2004). Google Play and the Apple App Store also require eHealth developers to include a privacy policy before app publication (Andow et al., 2019; O'Loughlin et al., 2019). Additionally, a Privacy Policy reflects the developers' commitment to user privacy (O'Loughlin et al., 2019; Andow et al., 2019).

Understanding eHealth app privacy policies is crucial for users (Zhou et al., 2019). Lack of comprehension may lead to inadvertent privacy breaches or data misuse (Glenn and Monteith, 2014). Clear policies enable informed decisions, enhancing trust in app providers (Khan et al., 2016). Trust is vital in health-related apps, and transparent, ethical data handling improves user satisfaction and engagement (Khan et al., 2016). However, many eHealth app policies use complex legal or technical language, challenging for users without specific expertise (Ravichander et al., 2019; Powell et al., 2018). For instance, the C25K 5K Trainer Pro App's policy, demonstrating data sharing with third parties, exemplifies such complexity as shown in Figure 1.



“

C25K 5K Trainer Pro: "When this app is in use or running in the background we collect and share with our business partners certain device and location data: Precise location data of the device, WiFi signals or Bluetooth Low Energy devices in your proximity, device-based advertising identifiers, app names and/or identifiers, and information about your mobile device such as type of device, operating system version and type, device settings, time zone, carrier, and IP address. That data may be used for the following purposes: (a) to customize and measure ads in apps and other advertising; (b) for app and user analytics; (c) for disease prevention, and cybersecurity,; (d) for market, civic or other research regarding aggregated human foot and traffic patterns, and (e) to generate proprietary pseudonymized identifiers tied to the information collected for the above purposes."

”

Figure 1: An example privacy policy snippet

Addressing key privacy issues in eHealth apps holds significant importance in today's digital health era (Wagner et al., 2016). Firstly, it enhances user trust by ensuring their sensitive health data is managed responsibly (Wagner et al., 2016). It also helps regulatory compliance, ensuring alignment with stringent regulations such as GDPR and HIPAA (Braghin et al., 2018). By addressing user privacy concern feedback, developers can prioritise privacy, enhancing user satisfaction and creating a competitive edge in the market (Tangari et al., 2021). In the digital health era, addressing privacy issues in eHealth apps is crucial (Wagner et al., 2016). It builds user trust by ensuring responsible handling of sensitive health data (Wagner et al., 2016), aids in regulatory compliance with laws like GDPR and HIPAA (Braghin et al., 2018), and by responding to user privacy concerns, developers can prioritise privacy, improving user satisfaction and gaining a competitive market advantage (Tangari et al., 2021). Our research, complementing existing studies on eHealth app privacy policies (Zimmeck et al., 2017; Harkous et al., 2018; Liu et al., 2021), focuses on understanding the challenges users face with these policies and the privacy concerns reported in user reviews. We aim to analyse the correlation between user reviews and app privacy policies, evaluating developers' strategies in addressing privacy and handling personal data. By assessing policy complexity and length, we will estimate the reading time required for an average user. We also intend to explore why users often accept terms without fully understanding data usage (Ibdah et al., 2021), considering the potential for developers to provide policy summaries for time-constrained users. Our study is guided by the following two key research questions:

RQ1 - What are the most common privacy issues reported by eHealth app users?

RQ2 - How do eHealth app developers say they handle privacy issues and users' personal information in their developed apps?

3 Method

3.1 eHealth Apps Selection

We selected the top 50 free and paid trending apps in the fitness and health category from both Apple and Google Play stores based on criteria like download rates and usage. This selection was conducted in Australia, the US, and the UK, initially totalling 600 apps. We removed duplicates appearing on both

Table 1: Privacy sub-aspects used in our user reviews classification (adapted from (Authors, 2021) and (Huebner et al., 2018))

Privacy Sub-Aspect	**A privacy-related user review containing...**
Policy	...concerns related to privacy policies or data-use agreements, such as complex policies or discussions about policy regulations.
Advertising	....mentions of ads or adware-related matters, like tracking users and displaying relevant ad banners or pop-ups.
Location	...mentions of tracking user locations or handling data in various locations.
Security	...references to security issues, such as phishing, hacking, or encryption problems.
Data Access and Sharing	...information about collecting, accessing, or sharing users' data or information.
Permissions	...concerns about app permissions, such as excessive permission requests or unnecessary requested permissions.
Trust and Safety	...discussions regarding user trustworthiness or safety.
Scam	...reports of scam-related issues, like unauthorized billing or subscriptions, privacy-related problems, or in-app purchases concerns.

Apple and Google Play lists and excluded apps with fewer than 500 user reviews to focus on prevalent issues in widely-used eHealth apps. After filtering, we analysed reviews from 276 distinct eHealth apps.

3.2 User Reviews Analysis

We analysed how privacy concerns impact user ratings through an extensive review analysis. Our automated tool extracted and classified over 5.1 million eHealth app user reviews, identifying 37,663 privacy-related reviews from both Apple and Google Play stores, covering 276 eHealth apps. These reviews were automatically categorised into eight sub-aspects: policy, location, data access and sharing, permissions, ads, security, trust and safety, and scams, with a review possibly mentioning multiple aspects. Using a "bag of keywords" method, our tool examined the influence of these privacy sub-aspects on app ratings (Authors, 2022). We correlated these findings with the apps' star ratings to pinpoint strengths and weaknesses in privacy.

1. We use GooglePlay and AppleStore open APIs to extract user reviews, translating non-English reviews into English using Google Translate API library (Translate, 2021).
2. Review preprocessing includes: correcting spelling errors, removing stopwords, and stemming the text.
3. Our tool detects privacy-related words or phrases in reviews, indicating a likely focus on privacy issues.
4. We automatically categorise each privacy-focused review into one or more of 8 privacy sub-aspects, based on a keyword list developed from extensive manual review analysis.
5. We generate summary statistics by app category, app aspect, app store, and overall metrics.

Additionally, we manually analysed 4,000 randomly chosen privacy-related reviews, 500 for each of the eight privacy sub-aspects, to identify key issues and provide evidence-based recommendations.

3.3 Privacy Policies and Data Use Agreements Analysis

While previous studies have analysed privacy policies and data-use agreements of mobile and eHealth apps (Zimmeck et al., 2016; Harkous et al., 2018; Liu et al., 2021; O'Loughlin et al., 2019; Powell et al., 2018), there has been no large-scale systematic study on the most frequently mentioned privacy concerns in eHealth app reviews. Our goal was to understand how user-expressed privacy concerns correlate with the apps' stated privacy policies and settings and to examine how eHealth app creators manage user privacy and sensitive information. To achieve this, we focused on several questions to manually analyse how eHealth app developers claim to address privacy concerns and handle user data:

Are users' data used beyond the eHealth app scope or shared with third parties? Investigating if an app uses data beyond its stated function is crucial for assessing privacy risks.

Does the eHealth app collect excess data? Many eHealth apps track user behaviour and interactions, potentially leading to the over-collection of data.

Can users delete their data permanently? The right to erase data is fundamental to privacy, demanding that eHealth apps allow user data removal or auto-delete it when unnecessary.

Does the app require permissions to function properly? Do apps transparently request necessary permissions or obscure this process, risking the exposure of user identities and behaviour patterns.

Does the free app include ads, in-app purchases, or subscriptions? Free apps often use ads, monitoring user interactions for targeted advertising, which raises ethical and security concerns.

Can users opt out of data collection and still use the app? The possibility of opting out of data collection while using the app reflects its commitment to privacy and whether user data is essential for its operation.

3.4 Privacy Policies Readability and Duration Analysis

The Flesch Reading Ease metric, a well-established tool, assesses text readability by evaluating sentence length and word syllables. Scores range from 1 to 100, with higher scores signifying greater readability. eHealth app developers can use this metric to make their privacy policies more accessible, aiming for clarity without oversimplifying or omitting essential details. Implementing this approach ensures that privacy policies effectively and transparently convey data practices to users.

We developed a Python tool to automatically calculate the readability of privacy policies using the Flesch Reading Ease score, a metric ranging from 1 to 100, with higher scores indicating easier readability. This tool also estimates the average time needed to read each eHealth app's privacy statement. Scores between 70 and 80 are considered easily understandable for the average adult (Spadero, 1983). Citing (Brysbaert, 2019), which found the average silent reading speed for English adults to be 238 words per minute (wpm) for non-fiction, we used this rate to compute the average reading time for each privacy policy. Therefore, the average reading time for each analysed privacy policy is calculated based on a reading speed of 238 wpm.

$$\text{Avg. reading time} = \left(\frac{\text{Total number of words in privacy policy}}{238} \right)$$

4 RQ1 – Most common privacy issues reported by eHealth app users

Our automated review analysis tool (Authors, 2022) was used to extract, translate, and categorise over 5.1 million user reviews of various eHealth mobile apps into 8 privacy sub-aspects, with 37,663 reviews specifically addressing app privacy. Figure 2 shows the frequency of these privacy issues, noting that a review may mention multiple sub-categories. The most common privacy sub-aspects mentioned were Scam (52%), Trust and Safety (21%), Permissions (16%), Data Access and Sharing (15%), Security (10%), Location (7%), Ads (3%), and Policy (3%).

Figure 3 presents a comparison of user ratings and privacy sub-categories mentioned in reviews. Apps with Scam-related reviews were the lowest rated, followed by those with Ads and Policy issues. Conversely, Trust and Safety was the highest-rated sub-aspect, followed by Security and Location. Specifically, 89% of users discussing Scam issues gave only one star, 75% did the same for Ads issues, and 74% for Policy issues. For Trust and Safety, only 24% of reviews gave one star, followed by 37% for both Security and Location issues. The subsequent subsections delve into the key issues and problems identified for each privacy sub-aspect, including example review quotes (☞) and our recommendations for improvement (✓).

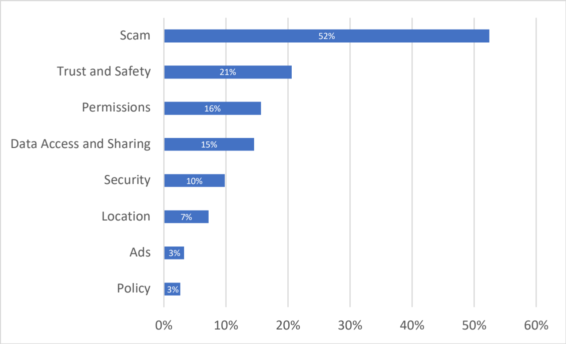


Figure 2: User reviews raising privacy related sub-aspects

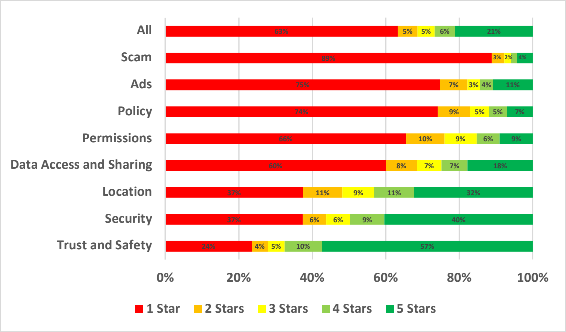


Figure 3: Distribution of star ratings across all privacy sub-aspects (percentages shown in bars)

4.1 Scam

Scam issues were the most common issues, reported in 52% of the privacy-related user reviews analysed in our study. Commonly mentioned Scam issues are discussed below.

Unapproved Charges: Many eHealth app users report multiple unauthorised or unexpected charges, often tied to subscriptions they never agreed to or trial periods that converted into full subscriptions without clear notification:

☞ ***User Review***: *"I thought the app is free. After using it for a week, they charged me! There was no clear warning about this. It feels like a scam." 1★*
✓ ***Recommendation***: *Transparency in Pricing - eHealth app creators must ensure clarity in subscriptions, costs, and trial periods.*

Misleading Descriptions: Certain eHealth apps overstate their capabilities in descriptions, failing to deliver promised health benefits or features upon use. This discrepancy between promises and actual functionalities erodes user trust in digital health solutions, highlighting the need for authenticity and transparency in this sensitive sector.

> ☞ ***User Review**: "The features advertised don't exist in the app. Downloaded it thinking it would track my heart rate, but it doesn't. Very misleading." 1★*
> ✓ ***Recommendation**: Accurate Descriptions - eHealth app creators must include authentic and precise descriptions of app functionalities without exaggeration.*

Fake Reviews: Many eHealth app users realised a surge in overly positive reviews for some eHealth apps, especially those with very generic reviews, which might indicate that the developer is padding the app's rating with fake reviews. As an example:

> ☞ ***User Review**: "Noticed a ton of 5-star reviews that all sound the same. Seems like the developer is flooding the app with fake reviews to boost their rating." 1★*
> ✓ ***Recommendation**: Review Integrity - eHealth app creators must implement measures to prevent fake reviews and promote genuine user feedback.*

Unresponsive Customer Service: Lack of response from customer service in eHealth apps leads to user frustration and suspicion about the developer's legitimacy. Users often express aggravation in reviews when their concerns or issues are ignored by app creators or support teams, especially when finding it difficult to contact user support, leading to accusations of scamming.

> ☞ ***User Review**: "I've been trying to reach out to their support team regarding a billing issue for 3 weeks now. I've sent multiple emails and tried their in-app support, but there's no response. For a health app where I'm supposed to trust them with my data, this unresponsiveness is deeply concerning." 1★*
> ✓ ***Recommendation**: Responsive Support - eHealth app creators must prioritise timely and effective customer service through easily accessible channels.*

Scam Accounts: Several eHealth apps allow users to create profiles within the app and share information with each other. These community features allow scammers to create fake profiles and bots to bother and scam other authentic and genuine users in several ways, as shown in this review:

> ☞ ***User Review**: "A LOT OF SCAMMERS. The community is full of fake profiles and people asking for money and soliciting for private information upon first message. BEWARE!" 1★*
> ✓ ***Recommendation**: User Profile Security - eHealth app creators must enhance user verification to prevent scam accounts and ensure community safety.*

Inability to Activate Premium Features: Some users who paid for extras within the app later discovered they were not granted access to the premium features. This led to them being charged more than once for the same thing. As an example:

> ☞ ***User Review**: "Paid for premium but couldn't access features. Tried again, got double-charged! Fix this and refund me!" 1★*
> ✓ ***Recommendation**: Reliable Premium Access - eHealth app creators must ensure users immediately receive what they pay for and no redundant charges.*

4.2 Trust and Safety

Trust and Safety issues were noted in 21% of all user reviews analysed in our study, as summarised in Figure 3. Most reviews mentioning Trust and Safety were associated with positively rated (four and five-star) apps, indicating that mentions of Trust and Safety issues are generally positive, unlike some other privacy sub-aspects.

Lack of Clinical Validity: Some users are worried about eHealth apps that provide medical advice or diagnostic tools without proper validation from reputable medical institutions or experts:

> ☞ ***User Review**: "A running app is giving health suggestions, where's the validation from trusted medical sources? Can't trust it!" 1★*
> ✓ ***Recommendation**: Clinical Validity - eHealth app creators should where possible partner with medical experts to ensure advice or diagnostic tools are clinically valid.*

Poorly Moderated Communities eHealth apps with community features such as forums can raise concerns if there is a lack of moderation, leading to misinformation or harmful advice:

> ☞ ***User Review**: "The community feature is full of misinformation and scammers and there's clearly no moderation. Not what I expected from a TOP fitness app in the market." 1★*
> ✓ ***Recommendation**: Community Oversight - eHealth app creators must enforce strong moderation for community features to prevent misinformation and ensure the sharing of safe, accurate advice.*

4.3 Permissions

Permission issues were reported in 16% of the privacy-related user reviews analysed in our study. Our analysis of user reviews has shown that many people grant eHealth app permissions without fully understanding the implications. Users often wonder why their eHealth apps need these permissions if they do not affect the app's fundamental functionality.

Excessive Permissions Users frequently raise concerns about eHealth apps requesting more permissions than needed for their core functions. For example, a basic medication reminder app should not require access to photos or contacts. Concerns also arise when eHealth apps access features like cameras or microphones without explicit permission or when inactive. Users express dissatisfaction when essential app features are contingent upon granting permissions that appear unrelated, such as a fitness app's tracking feature only being accessible with constant location data access.

☞ ***User Review***: *"The medication reminder notification asked for access to my photos and contacts? Plus, I noticed the app is accessing my camera without my go-ahead. And why lock the fitness tracker behind always-on location data? Suspicious!" 1★*
✓ ***Recommendation:*** *Minimise Permissions - eHealth app creators must only request permissions crucial for the app's primary functionality and avoid unnecessary access, especially for core features.*

Lack of Clarity Many eHealth apps fail to adequately explain the need for certain permissions, leading to user suspicion and confusion about the app's true intentions. Users often become wary when permissions appear irrelevant to the app's primary functions, suspecting data collection for unmentioned purposes like selling to third parties or ad targeting. Additionally, eHealth apps integrating with services or devices, such as wearables, frequently lack clarity on the permissions required by these third parties. Users also express concern when an app's permissions change substantially after an update, particularly if these changes are not transparently communicated.

☞ ***User Review***: *" Why does this app need so many unrelated permissions? It's unclear, especially with the wearable integration. The last update changed permissions and no explanation was provided. Makes me wonder what they're really doing with my data." 1★*
✓ ***Recommendation***: *Transparent Communication - eHealth app creators must provide explicit explanations for each required permission, ensure transparency about third-party integration and update users about any permission changes.*

4.4 Data Access and Sharing

Data Access and Sharing issues were reported in 15% of the privacy-related user reviews analysed in our study. Users were very upset when the app collected and shared their data with third parties. Some users even raised the concern that some apps send users' information to other countries to be handled. Commonly mentioned data access and sharing issues are discussed below.

Unauthorised Data Sharing or Sale: eHealth app users often express concern about the possibility of their health data being collected and sold to third parties, like companies, advertisers, or medical research institutions, without clear consent. Alarms are raised when personal health data is shared with third parties, particularly without explicit user consent or knowledge. Additionally, significant worries exist regarding eHealth apps' integration with other platforms or services and the potential misuse of health data by these third parties.

☞ ***User Review***: *"Beware... Just found out this app is selling my fitness health data without my consent. Why is my personal info going to third parties? Really concerning!!" 1★*
✓ ***Recommendation***: *Clear Consent - eHealth app creators must obtain explicit user approval before sharing data with third parties and provide transparent information about any integrations with other platforms or services.*

Inadequate Data Deletion Protocols: Many concerns were raised in reviews about how long the eHealth app retains personal health data, and whether users can delete their data. When eHealth app users delete the app or their account, they often expect all their data to be deleted. Reviews indicate dissatisfaction when users discover that their data remains accessible or is not completely deleted from the app's servers after account deletion:

☞ ***User Review***: *"Deleted the app and signed up again to find out my data's still on their servers... Expected better privacy practices from a popular app. Not cool" 1★*
✓ ***Recommendation***: *Data Deletion - eHealth app creators must ensure clear protocols for data retention and allow users to fully delete their data upon account termination, while communicating the deletion process and timeline.*

Mandatory Data Collection: eHealth app users raised in some hesitancy or frustration with apps that require them to share sensitive health data to access basic functionalities:

☞ ***User Review***: *"Why do I need to provide all my personal information and health data just to use the basic features of diet programs??!! It's uncomfortable being forced to share so much personal info" 1★*
✓ ***Recommendation***: *Limit Data Collection - eHealth app creators must collect only necessary data for core app functions and offer basic functionalities without mandating sensitive data sharing.*

4.5 Security

Security issues were reported in 10% of the user reviews. Through our analysis of user reviews, we can see that the following problems are prevalent:

Logging and Sign-up Problems: Many eHealth apps mandate user signup and login before first use for a secure and personalised experience. Users, particularly the elderly with limited technical knowledge, have expressed dissatisfaction with complex app store registration processes, making some apps difficult to access. Reviews often cite issues with the login process, including the requirement for excessive information during registration, errors in registration forms, and problems with receiving OTPs and similar issues.

☞ ***User Review***: *"Tried to use the app, but the signup process was nightmare! Many details required and never got the OTP. Not user-friendly, especially for old people like me. Fix the login issues!" 1★*
✓ ***Recommendation***: *User-Friendly Registration - eHealth app creators must streamline the signup and login processes to be user-friendly, especially considering elderly or non-tech-savvy users and address common issues like OTP retrieval, etc.*

App Data Breach: A data breach involving unauthorised access or loss of sensitive information mandates user notification under the Notifiable Data Breaches Scheme. For instance, in March 2018, MyFitnessPal app's creators informed users about a platform attack compromising user data:

☞ ***User Review***: *"Just got an email about a data breach on this app. It's very frustrating to think my personal health info might be compromised. Expected better security from such a prominent app." 1★*
✓ ***Recommendation***: *Data Breach Measures - eHealth app creators must enhance security measures to prevent breaches while staying compliant with local and international data breach regulations, ensuring a clear notification plan is in place for users if breaches occur.*

4.6 Location

Location issues were reported in 7% of the privacy-related user reviews analysed in our study. Users of eHealth apps frequently asked app creators why they access their location even when they are not using the apps or if the apps do not require users' locations to function properly. Some users linked the location tracking to the ads shown in the app, while others correlated that with sharing this location information with third parties.

Unnecessary Location Tracking: Users frequently question the necessity of eHealth apps accessing their location, especially when the app's primary function does not appear to need it. Concerns mount when the reason for using location data is unclear, or when the app tracks location continuously or in the background, even when inactive. Users are particularly worried if they cannot opt out of location tracking or if disabling it compromises the app's main functionalities. Additionally, continuous location tracking is often associated with quicker battery drainage, a concern frequently mentioned in user reviews.

☞ ***User Review***: *"Just noticed that fitness pal tracks my location even when I'm not using it. I don't see why a health tracker needs this. It's concerning and feels invasive. Please explain or update the app permissions!" 1★*
✓ ***Recommendation***: *Limit Location Tracking - eHealth app creators must access user location only when essential for core app functions, offer a clear explanation for its use, and ensure users can easily opt-out without losing functionalities.*

Misuse or Sale of Location Data: eHealth app users often raise flags about location data being shared with unknown third parties or for unclear reasons. eHealth app users get worried when they start seeing location-specific ads within the app, suggesting their location data is being used for targeting. This also leads to major concerns or suspicions that the app developers might be selling location data to third parties or using it for purposes outside the app's main functionalities.

☞ ***User Review***: *" Recently started seeing ads in the app related to places near me. Why? I'm worried my location data is being sold or misused. I downloaded this for improving my health, not to be targeted with ads based on my location. Please be transparent about how you're using our data" 1★*
✓ ***Recommendation***: *Transparent Location Data Use - eHealth app creators must clearly communicate any location data sharing practices and guarantee that location data is neither sold nor used for unsolicited ad targeting while maintaining updated location data policies in line with user expectations.*

4.7 Advertisements

In our study, 3% of privacy-related user reviews mentioned advertisement issues. Mobile app developers often depend on revenue from in-app advertisements, a key financial support for offering free apps. This is common in free eHealth apps, where revenue is generated through banner ads within the app. Users have expressed dissatisfaction with ads that are inappropriate or irrelevant to the app's content. While these ads are vital for app success, complaints include them being intrusive and distracting, sometimes leading to app uninstallation.

Intrusive Ads: Users find pop-up or full-screen video ads disruptive, particularly during workouts or activities requiring concentration. Excessive ads, interrupting at short intervals, can obstruct app functionalities or buttons, often leading to accidental clicks. The lack of an option to buy an ad-free version or subscribe to remove ads adds to the frustration.

☞ ***User Review***: *"Was trying to focus on my exercises and got bombarded with pop-up ads! It's hard enough to concentrate and these constant interruptions make it worse. The ads even cover important buttons sometimes. I'd happily pay for an ad-free version, but there's no option." 1★*
✓ ***Recommendation***: *User-Centric Ad Experience - eHealth app creators must minimise intrusive ads and offer options for an ad-free experience and ensure ads are relevant and non-disruptive.*

Ads Relevant to Medical Data: Concerns arise when users see ads that seem to be tailored based on their health data, leading to privacy fears or with ads that seem to offer medical advice or make health claims, which can be misleading or even dangerous. Given the sensitivity of eHealth app data, users are particularly sensitive to ads that may be seen as inappropriate or not in line with the app's theme:

☞ ***User Review***: *"Noticed that ads showing to me match my health data. It is frustrating to know that my data is used for targeted ads. Also, some ads are giving medical advice, which feels misleading." 1★*
✓ ***Recommendation***: *Sensitive and Relevant Ad Content - eHealth app creators must prioritise ads that align with the app's theme and avoid those seemingly based on sensitive health data or offer unverified medical advice.*

Data Usage Concerns and Battery Drain: Ad-heavy apps can cause faster battery drainage. Video ads can consume significant data, leading to concerns about data usage and associated costs. Some users link app crashes or performance lags to the presence of advertisements, especially if they are resourceheavy:

> ☞ ***User Review***: *"Can we get a less ad-heavy version? The constant video ads eat up my data and kill my battery fast. Noticed more lags and crashes too." 1★*
> ✓ ***Recommendation***: *Optimised Ad Integration - eHealth app creators must monitor ads' impact on app performance and battery life, ensuring they do not degrade user experience or consume much data.*

4.8 Policy

Policy issues were reported in 3% of the privacy-related user reviews analysed in our study. A complete privacy policy should always be available to eHealth apps. We found that some users were concerned about the following categories of information being shared: names, phone numbers, emails, birth locations, geolocations, medical records, ages, birthdays, and identification numbers. Others include DNA and genetic information, biometric data (such as fingerprints or facial recognition), data from devices, IP addresses, browsing histories, credit card details, automatic cookie data, and sensitive personal data (e.g., race, ethnicity, sexual orientation).

Lack of Transparency and Policy Accessibility: eHealth users complain about unclear terms of service and privacy policies that are overly-complex or do not specify how sensitive personal health data is used or stored. Criticism includes policies being buried deep within the app or being presented in a format that is hard to read or understand. Users raised worries about the app sharing health data with third parties, especially without explicit user consent:

> ☞ ***User Review***: *"Why the privacy it so complex? How exactly is my health data being used and shared? There needs to be more transparency." 1★*
> ✓ ***Recommendation***: *Transparent Policies - eHealth app creators must ensure clear, jargon-free privacy policies that are easily accessible, outlining data use, storage, and sharing practices.*

Sudden Policy Changes: eHealth app users expressed frustration when app policies are updated without clear notification, especially if these changes might compromise their privacy, particularly when sensitive health data is involved. Given the sensitive nature of health information, users expect and deserve transparent communication regarding any alterations in data handling practices. When users have initially chosen an app based on its privacy policies and those policies change without due notice, it can feel like a breach of the initial agreement:

> ☞ ***User Review***: *"I chose this eHealth app for its privacy stance, only to discover they changed policies without notifying us! With sensitive health data at stake, this is a breach of trust." 1★*
> ✓ ***Recommendation***: *Clear Communication on Changes - eHealth app creators must notify users about significant policy updates in advance and explain the rationale behind them.*

Consent Concerns and Lack of Opt-Out Options: A major concern among users is the lack of control over personal health data in eHealth apps. These apps handle highly sensitive personal details, emphasising the importance of consent. Users are dissatisfied with broad consent agreements that lack clarity on what they entail. This ”all or nothing” approach to consent can make users feel compelled to agree to everything to access necessary health tools or services. Furthermore, the lack of clear opt-out options for particular data sharing or collection practices heightens user frustration.

> ☞ ***User Review***: *"Very upset with the app. I only want use the nutrition feature you have and forced to sharing all my health data" 1★*
> ✓ ***Recommendation***: *User Control Over Consent - eHealth app creators must offer multiple consent options and clear opt-out mechanisms, emphasising user control over personal health data.*

Jurisdictional and Legal Concerns: Some users raised issues about where the health data is stored and which country's laws apply to their data, especially for international users.

> ☞ ***User Review***: *"Where's my health data stored and which country's laws are protecting it? I am in Europe so why my data is sent to the US? We need some clarity as international users" 1★*
> ✓ ***Recommendation***: *Address Data Jurisdiction - eHealth app creators must specify where user data is stored and the legal jurisdiction while considering international regulations and user concerns.*

5 RQ2 – Privacy Policy and Data Use Agreements Analysis

5.1 Data access and sharing

Our analysis of Privacy Policies and Data Use Agreements reveals that 92% of eHealth apps need device access permissions to function. Additionally, 86% access or collect more data than necessary, and 84% share user data with third parties, such as advertisers. Moreover, 95% of the free eHealth apps in our study feature ads. Only 27% provide users with a direct option to permanently delete their data. Each of these privacy issues is discussed in detail below.

Are user's data used out of the app scope or shared with third parties?

Cloud Storage and Infrastructure: 83% of eHealth apps use third-party cloud services for data storage and processing. This involves storing user data on external servers, potentially accessible by the cloud provider.
Shared for Features/Services Enhancement: 71%

share user data with third-party specialists or health platforms to enhance services, like providing detailed health insights or improving user experience.

Shared for Advertising or Marketing: 63% may share data with advertising platforms or for targeted marketing, especially in free eHealth apps.

Data Brokers and Third-Party Sale: 18% might sell user data to third-party brokers, who resell it to various industries, raising privacy concerns.

Shared for Research Purposes: 13% share de-identified or aggregated data with research institutions, with 27

Strictly Within App Scope: Only 7% of the apps strictly use data within the app scope, not sharing it externally or for unrelated purposes.

Does the app collect more data than it needs?

Data for Personalisation: 84% of eHealth apps collect various data to provide personalised health recommendations and insights, tailoring user experience and health advice.

Feature-based Collection: 38% of the apps gather information specifically related to their features or services, ensuring data collection is essential for operation based on the user's chosen features.

Minimum Data Collection: Only 14% strictly adhere to data minimisation, collecting only the necessary data to deliver their services effectively while respecting user privacy and limiting vulnerabilities.

Can users delete their data permanently?

No Direct Deletion: 53% of eHealth apps do not offer direct data deletion. Users can request deletion through customer support, which is then processed within a set period.

Third-Party Dependencies: 44% allow users to delete primary data from the app. For data shared with third parties, users might need to contact those entities for complete deletion.

Automated Data Lifecycle: 35% have automated policies for deleting data not used for a specific period, with an option for users to expedite this process.

Full User Control: 27% provide an option for users to permanently delete all their data, which is irreversible.

Data Anonymisation: 3% offer data anonymisation instead of deletion, masking personal identifiers while using the data for research.

Does the app request permissions to work properly?

Optional Permissions: 52% of eHealth apps request permissions for a better user experience, many of which are optional. Users can deny these and still use the primary app features.

Broad Permissions Required: 24% require a broad set of permissions with clear purposes. Users can decline permissions but may experience limited usage or be unable to use the app.

Essential Permissions Only: 17% indicate that only essential permissions are needed for core functionalities, accessing only necessary data and features for delivering health services.

Transparent Permission Policy: 7% provide detailed explanations of each permission, allowing users to make informed decisions.

Ads, in-app purchases or subscription?

Subscription Model: 53% of eHealth apps use a subscription model. The basic version is free, with premium features available through monthly or yearly subscriptions, and in-app purchases for specific functionalities.

One-time Purchase Model: 33% offer a one-time purchase option. These apps provide core features for free, with a single in-app purchase granting lifetime access to premium features.

Ad-supported Model: 14% operate on an ad-supported model, offering free usage but containing ads, with no subscriptions or in-app purchases.

Can users opt out of the data collection policy and still use the app?

No Opt-out: 31% of eHealth apps do not offer an opt-out from data collection, using the data to enhance user experience and health outcomes.

Conditional Opt-out: 28% allow opting out of certain data collection modules like location or biometrics, but require sharing other essential data for the app's primary functions.

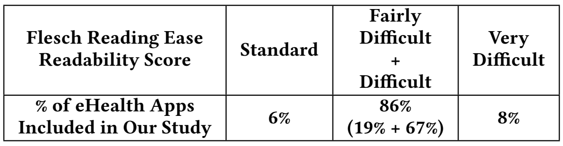
Complete Opt-out: Only 26% permit a complete opt-out from data collection while continuing to use the app and all its features, potentially affecting personalisation and accuracy of health recommendations.

Full Opt-out with Limited Functionality: 15% allow opting out from data collection policies but with limited access to personalised features, though core functionalities remain available.

5.2 Privacy Policy Complexity

Our analysis reveals that the readability of eHealth apps' privacy policies is generally complex. Table 2 shows that 67% of the privacy policies are classified as difficult, whereas only 6% are considered standard. 19% are fairly difficult, and 8% are very difficult. App creators are not legally required to simplify their policies, despite the emphasis on clarity in laws and regulations like GDPR or APA.

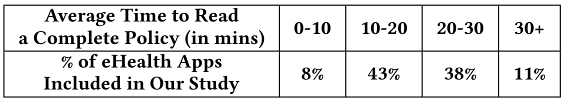
Table 2: eHealth Apps Privacy Policy Readability Analysis



Flesch Reading Ease Readability Score	Standard	Fairly Difficult + Difficult	Very Difficult
% of eHealth Apps Included in Our Study	6%	86% (19% + 67%)	8%

Table 3 indicates that most eHealth apps' privacy policies take over 15 minutes to read. 43% of the apps in our study have policies requiring 10–20 minutes to read fully. Meanwhile, 38% need 20–30 minutes. Only 8% can be read in less than 10 minutes, while 11% take more than 30 minutes. The combination of lengthy reading times and complex readability often results in users consenting to these policies without fully understanding them.

Table 3: Average Time to Read Privacy Policy



Average Time to Read a Complete Policy (in mins)	0-10	10-20	20-30	30+
% of eHealth Apps Included in Our Study	8%	43%	38%	11%

6 Discussion

Scam and Lack of Trust in eHealth App Reviews: Scam and trust issues are prominently raised in privacy-related user reviews, highlighting concerns like unapproved charges, misleading descriptions, fake reviews, unresponsive customer service, scam accounts, and issues with paid features.

Need for Simpler Privacy Policies in eHealth Apps: The least raised issue in reviews is policy-related, suggesting most users do not read privacy policies before app use. Users often raise issues in reviews that are covered in these policies, indicating the need for a simpler, quicker-to-read summary.

Excessive Data Collection by eHealth Apps: Many eHealth apps collect and share more data than necessary, unrelated to app functionality. Developers should limit data collection to what is essential for current app functions.

Improving User Awareness of eHealth App Privacy Policies: Given the complexity and length of most privacy policies, users often consent without fully understanding them. Developers should simplify these policies and provide clear summaries of key data captured and its purpose.

Need for Stricter Laws on eHealth App Privacy Policies: Current regulations like GDPR or APA do not specifically mandate the use of plain English in privacy policies. Our analysis suggests that readability and the time needed to read these policies call for improved regulations to enhance user protection.

7 Threats to Validity

Limited Information in Reviews: Many users give only a star rating or short comments, not fully expressing their opinions or detailing issues with the app. **Inaccurate Translation**: The accuracy of our translated reviews is not guaranteed, which could lead to misclassification. **Manual Policy Analysis**: The privacy and data usage policies of apps were manually analysed by one author and double-checked by another. However, these policies may not accurately represent the app's actual data management practices. **Automated Review Analysis**: We classified user reviews into 8 privacy subaspects using a large dataset of words and phrases, linking them to app star ratings. Some relevant keywords might be missing from our dataset, but it was created after manually inspecting over 23,000 reviews, including those for non-eHealth apps.

8 Related Work

The eHealth domain faces significant privacy challenges. Analysing user reviews is crucial for app developers and researchers, as recognised in various studies. For example, (Alqahtani and Orji, 2019; Stuck et al., 2017) used reviews to identify usability issues in mental health and medication apps, while (Bouras et al., 2020; Sahama et al., 2013) highlighted the importance of user trust and clear communication in eHealth apps. Our study goes further by examining 5.1 million user reviews across different eHealth app categories, providing detailed analysis of privacy concerns and identifying eight key issues.

Other works like (O'Loughlin et al., 2019; Sunyaev et al., 2015) have noted privacy policy issues across app categories. Our research specifically targets eHealth apps, acknowledging their often unclear policies. Aligning with studies such as (Robillard et al., 2019; Das et al., 2018) on policy readability, we find that eHealth app privacy policies are complex and typically require over 15 minutes to read, hindering user comprehension. The need for improved privacy communication has been addressed in various studies (Balebako and Cranor, 2014; O'Loughlin et al., 2019). Our contribution includes targeted recommendations for eHealth app developers and introducing a tool to summarise privacy policies, enhancing their accessibility for users.

9 Summary

We carried out a large-scale analysis of 276 commonly used eHealth apps. We found over 37,000 user reviews raised one or more data privacy concerns. We analysed their privacy policies and found over 90% to be difficult or very difficult to read on the Flesch reading ease scale, and nearly 50% take 20 or more minutes to read. We recommend several key areas for developers to address in their app privacy behaviours, privacy policy creation and app privacy behaviour disclosure summary to users. We propose a prototype tool to aid developers in determining their required eHealth app privacy behaviours and to summarise these clearly and succinctly to users to gain their informed consent.

ACKNOWLEDGEMENTS

Haggag and Grundy are supported by ARC Laureate Fellowship FL190100035.

REFERENCES

Alqahtani, F. and Orji, R. (2019). Usability issues in mental health applications. In *Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization*, pages 343–348.

Andow, B., Mahmud, S. Y., Wang, W., Whitaker, J., Enck, W., Reaves, B., Singh, K., and Xie, T. (2019). {PolicyLint}: investigating internal privacy policy contradictions on google play. In *28th USENIX security symposium (USENIX security 19)*, pages 585–602.

Arellano, A. M., Dai, W., Wang, S., Jiang, X., and Ohno-Machado, L. (2018). Privacy policy and technology in biomedical data science. *Annual review of biomedical data science*, 1:115–129.

Authors, A. (2021). Removed for anonymous peer review.

Authors, A. (2022). Removed for anonymous peer review.

Balebako, R. and Cranor, L. (2014). Improving app privacy: Nudging app developers to protect user privacy. *IEEE Security & Privacy*, 12(4):55–58.

Benjumea, J., Ropero, J., Rivera-Romero, O., Dorronzoro-Zubiete, E., Carrasco, A., et al. (2020). Privacy assessment in mobile health apps: scoping review. *JMIR mHealth and uHealth*, 8(7):e18868.

Bouras, M. A., Lu, Q., Zhang, F., Wan, Y., Zhang, T., and Ning, H. (2020). Distributed ledger technology for ehealth identity privacy: State of the art and future perspective. *Sensors*, 20(2):483.

Bradford, L., Aboy, M., and Liddell, K. (2020). Covid-19 contact tracing apps: a stress test for privacy, the gdpr, and data protection regimes. *Journal of Law and the Biosciences*, 7(1):lsaa034.

Braghin, C., Cimato, S., and Della Libera, A. (2018). Are mhealth apps secure? a case study. In *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, volume 2, pages 335–340. IEEE.

Brysbaert, M. (2019). How many words do we read per minute? a review and meta-analysis of reading rate. *Journal of Memory and Language*, 109:104047.

Chen, R., Fang, F., Norton, T., McDonald, A. M., and Sadeh, N. (2021). Fighting the fog: Evaluating the clarity of privacy disclosures in the age of ccpa. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, pages 73–102.

Choice (2022). Drowning in privacy policies: Choice calls for reform.

Das, G., Cheung, C., Nebeker, C., Bietz, M., Bloss, C., et al. (2018). Privacy policies for apps targeted toward youth: descriptive analysis of readability. *JMIR mHealth and uHealth*, 6(1):e7626.

Dehling, T., Gao, F., Schneider, S., Sunyaev, A., et al. (2015). Exploring the far side of mobile health: information security and privacy of mobile health apps on ios and android. *JMIR mHealth and uHealth*, 3(1):e3672.

Glenn, T. and Monteith, S. (2014). Privacy in the digital world: medical and health data outside of hipaa protections. *Current psychiatry reports*, 16(11):494.

Harkous, H., Fawaz, K., Lebret, R., Schaub, F., Shin, K. G., and Aberer, K. (2018). Polisis: Automated analysis and presentation of privacy policies using deep learning. pages 531–548.

Hinds, J., Williams, E. J., and Joinson, A. N. (2020). "it wouldn't happen to me": Privacy concerns and perspectives following the cambridge analytica scandal. *International Journal of Human-Computer Studies*, 143:102498.

Hu, M. (2020). Cambridge analytica's black box. *Big Data & Society*, 7(2):2053951720938091.

Huckvale, K., Prieto, J. T., Tilney, M., Benghozi, P.-J., and Car, J. (2015). Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. *BMC medicine*, 13(1):1–13.

Huebner, J., Frey, R. M., Ammendola, C., Fleisch, E., and Ilic, A. (2018). What people like in mobile finance apps: An analysis of user reviews. pages 293–304.

Ibdah, D., Lachtar, N., Raparthi, S. M., and Bacha, A. (2021). "why should i read the privacy policy, i just need the service": A study on attitudes and perceptions toward privacy policies. *IEEE access*, 9:166465–166487.

Jensen, C. and Potts, C. (2004). Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pages 471–478.

Khan, S., Hoque, A., et al. (2016). Digital health data: a comprehensive review of privacy and security risks and some recommendations. *Computer Science Journal of Moldova*, 71(2):273–292.

Liu, S., Zhao, B., Guo, R., Meng, G., Zhang, F., and Zhang, M. (2021). Have you been properly notified? automatic compliance analysis of privacy policy text with gdpr article 13. pages 2154–2164.

Mulder, T. (2019). Health apps, their privacy policies and the gdpr. *European Journal of Law and Technology*.

Okoyomon, E., Samarin, N., Wijesekera, P., Elazari Bar On, A., Vallina-Rodriguez, N., Reyes, I., Feal, Á., Egelman, S., et al. (2019). On the ridiculousness of notice and consent: Contradictions in app privacy policies.

O'Loughlin, K., Neary, M., Adkins, E. C., and Schueller, S. M. (2019). Reviewing the data security and privacy policies of mobile apps for depression. *Internet interventions*, 15:110–115.

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., and Patsakis, C. (2018). Security and privacy analysis of mobile health applications: the alarming state of practice. *Ieee Access*, 6:9390–9403.

Parker, L., Halter, V., Karliychuk, T., and Grundy, Q. (2019). How private is your mental health app data? an empirical study of mental health app privacy policies and practices. *Int. Journal. Law and Psychiatry*, 64:198–204.

Powell, A., Singh, P., Torous, J., et al. (2018). The complexity of mental health app privacy policies: a potential barrier to privacy. *JMIR mHealth and uHealth*, 6(7):e9871.

Ravichander, A., Black, A. W., Wilson, S., Norton, T., and Sadeh, N. (2019). Question answering for privacy policies: Combining computational and legal perspectives. *arXiv preprint arXiv:1911.00841*.

Robillard, J. M., Feng, T. L., Sporn, A. B., Lai, J.-A., Lo, C., Ta, M., and Nadler, R. (2019). Availability, readability, and content of privacy policies and terms of agreements of mental health apps. *Internet interventions*, 17:100243.

Rowland, S. P., Fitzgerald, J. E., Holme, T., Powell, J., and McGregor, A. (2020). What is the clinical value of mhealth for patients? *NPJ digital medicine*, 3(1):4.

Sahama, T., Simpson, L., and Lane, B. (2013). Security and privacy in ehealth: Is it possible? In *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)*, pages 249–253. IEEE.

Spadero, D. C. (1983). Assessing readability of patient information materials. *Pediatric Nursing*, 9(4):274–278.

Stuck, R. E., Chong, A. W., Tracy, L. M., and Rogers, W. A. (2017). Medication management apps: usable by older adults? In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 61, pages 1141–1144. SAGE Publications Sage CA: Los Angeles, CA.

Sunyaev, A., Dehling, T., Taylor, P. L., and Mandl, K. D. (2015). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association*, 22(e1):e28–e33.

Tahaei, M., Bernd, J., and Rashid, A. (2022). Privacy, permissions, and the health app ecosystem: A stack overflow exploration. In *Proceedings of the 2022 European Symposium on Usable Security*, pages 117–130.

Tangari, G., Ikram, M., Ijaz, K., Kaafar, M. A., and Berkovsky, S. (2021). Mobile health and privacy: cross sectional study. *bmj*, 373.

Times, N. Y. (2019). We read 150 privacy policies. they were an incomprehensible disaster.

Translate, G. (2021). Python client library.

ur Rehman, I. (2019). Facebook-cambridge analytica data harvesting: What you need to know. *Library Philosophy and Practice*, pages 1–11.

Wagner, I., He, Y., Rosenberg, D., and Janicke, H. (2016). User interface design for privacy awareness in ehealth technologies. In *2016 13th IEEE annual consumer communications & networking conference (CCNC)*, pages 38–43. IEEE.

Zhou, L., Bao, J., Watzlaf, V., Parmanto, B., et al. (2019). Barriers to and facilitators of the use of mobile health apps from a security perspective: mixed-methods study. *JMIR mHealth and uHealth*, 7(4):e11223.

Zimmeck, S., Goldstein, R., and Baraka, D. (2021). Privacyflash pro: Automating privacy policy generation for mobile apps. In *NDSS*, volume 2, page 4.

Zimmeck, S., Wang, Z., Zou, L., Iyengar, R., Liu, B., Schaub, F., Wilson, S., Sadeh, N., Bellovin, S., and Reidenberg, J. (2016). Automated analysis of privacy requirements for mobile apps.

Zimmeck, S., Wang, Z., Zou, L., Iyengar, R., Liu, B., Schaub, F., Wilson, S., Sadeh, N. M., Bellovin, S. M., and Reidenberg, J. R. (2017). Automated analysis of privacy requirements for mobile apps.