Are Bite-Size Data Safety Details a Healthy Diet for Android Telehealth App Users? Impacts of Privacy Nutrition Labels on Users' Privacy Perceptions

Alisa Frik
International Computer Science Institute
afrik@icsi.berkeley.edu

Subham Mitra
University of California, Berkeley
subham.mitra@berkeley.edu

Priyasha Chatterjee
Max Plank Institute for Security and Privacy
priyasha.chatterjee@mpi-sp.org

Julia Bernd
International Computer Science Institute
jbernd@icsi.berkeley.edu

Abstract

Mobile telehealth apps can provide valuable services, but they raise significant privacy and security concerns, as they collect health-related and other sensitive personal information. We conducted two surveys ($N = 1,256$ total) to examine US users' privacy expectations about Android telehealth and teletherapy apps' data practices and legal privacy protections for the data they collect, gaps between those expectations and actual practices and protections, and how privacy perceptions and behavioral intentions are affected by privacy disclosures. In Survey 1, we explored participants' privacy perceptions and intentions about 10 telehealth apps, first after reading just the general description from the Google Play Store, then after reading the Data Safety section (DSS). Survey 2 explored broader privacy expectations regarding telehealth apps, regulatory awareness, and preferred legal protections.

Findings indicate that participants perceived apps provided by independent developers as less likely to protect privacy than apps offered by healthcare providers. However, participants often had inaccurate privacy expectations and overestimated legal safeguards, potentially leading to uninformed privacy decisions. DSSs significantly affected participants' expectations about data practices and legal protections and their likelihood of using the app—but while DSSs often increased participants' *confidence* in their privacy expectations, they did not necessarily improve their *accuracy*.

Keywords

Privacy, Transparency, Health Apps, mHealth, HIPAA

1 Introduction

The swiftly-growing market of mobile apps that aim to help consumers manage their health (*mHealth* or *health apps*) encompasses a variety of applications, including remote medical and psychotherapy consultation, advice and information, medication adherence, mental health support, and contact tracing. These technologies come with significant benefits to users [29, 75, 95], but also privacy and security risks [45, 71, 73, 97, 117] that users of such apps worry about [7, 39, 53, 99, 103]. Previous research indicates that US health app users' limited understanding of privacy laws and app functionalities can result in privacy expectations that are not met [41, 66] and uninformed decisions that can be detrimental to users. It is therefore important to investigate disparities between users' privacy expectations and the actual privacy practices of health apps.

We focus on health apps for several reasons. Firstly, users consider medical data particularly sensitive [20, 68, 70, 77, 82]. Previous studies indicate that users often misunderstand and worry about health apps' data practices [19, 62, 63, 67, 76], yet fail to utilize privacy/security features to safeguard their health data [98]. Secondly, privacy and security concerns can impede the adoption of emerging mHealth services that are otherwise essential, as they offer increased access to and reduced costs for healthcare [7, 11, 80, 123]. Finally, misunderstanding of regulations like HIPAA might lead users to expect legal protections for their privacy when using apps, while in reality, many health apps and their operations may fall outside these legal protections, often providing less robust privacy safeguards than anticipated by the users [32, 33].

We focused on *telehealth* (including teletherapy) apps due to the particular risk of privacy confusion, given that some of them are subject to HIPAA and some are not (i.e. some are legally considered "covered entities" and some "non-covered"). This presents an opportunity to test potential differences in user perceptions between apps with different legal statuses. Moreover, telehealth and teletherapy apps are likely to collect especially sensitive information, potentially including identifiable medical records.

We ran two surveys in the US to answer these research questions:

- **RQ1:** What are participants' **privacy expectations about data practices** of teleheath apps, and are they different from actual observed data practices?
- **RQ2:** What are participants' **privacy attitudes and behavioral intentions** about teleheath apps?
- **RQ3:** What is the impact of telehealth apps' **Data Safety sections** on participants' **a)** privacy expectations, and **b)** privacy attitudes and behavioral intentions?
- **RQ4: What factors** affect participants' privacy attitudes and behavioral intentions regarding telehealth apps?
- **RQ5:** What are participants' **expectations and preferences about legal privacy protections** for data collected by telehealth apps?

Proceedings on Privacy Enhancing Technologies 2026(1), 366–392

https://doi.org/10.56553/popets-2026-0019

In **Survey 1** ($N = 855$), we showed participants a Google Play Store description of one of ten Android telehealth apps. We asked what they thought the apps' data practices were (RQ1), what privacy laws the data recipients are subject to (RQ5), how well the app would protect their privacy, how confident they were of understanding its data practices, and how likely they would be to download it (RQ2, RQ4). We then showed the app's Data Safety section and repeated the questions (RQ3). We also compared participants' expectations with data from app testing and with the relevant legal text, to assess whether expectations were accurate and whether the Data Safety sections impacted accuracy (RQ1, RQ3a, RQ5).

In **Survey 2** ($N = 401$), we delved deeper into participants' expectations about data practices and legal protections. We asked about participants' impressions of telehealth apps *in general* (rather than specific apps), and also asked what legal protections participants would *prefer* (RQ1, RQ5).

We found that many participants had incorrect or unrealistic expectations about data flows, and overestimated legal safeguards. In their current form, telehealth apps' Data Safety sections (AKA privacy nutrition labels) provide incomplete, vague, and sometimes confusing information, and by boosting overconfidence rather than privacy awareness, they can lead to uninformed privacy decisions and violate users' expectations. These insights inform suggested improvements to privacy disclosures, and recommendations for aligning legal protections with telehealth app users' expectations.

In sum, the main contributions of this research are:

- Quantified empirical evidence regarding the impact of privacy nutrition labels on the *accuracy* of users' expectations, their *confidence* in understanding data practices, their *beliefs about privacy protections and regulatory safeguards*, and their *decisions to install or use* a telehealth app.
- Data-driven recommendations to help to enhance transparency and support telehealth users in forming accurate expectations about data practices and legal protections, and making informed privacy decisions for *health data*.

2 Related Work

2.1 User Perceptions and Transparency Challenges in Health Apps

A number of studies have found that privacy and security concerns can hinder the adoption of mHealth technologies [7, 11, 56, 80, 123]. Users worry about data breaches, misuse, and targeted advertising [19, 39, 42, 76, 99]. These concerns are heightened when apps handle sensitive information that could lead to social stigma or discrimination, such as data related to mental health or HIV [20, 68, 82]. Interview participants were much more hesitant about sharing their mental health data via a telehealth app than sharing it directly with providers or researchers [92]. A literature review noted that older adults' privacy concerns about telehealth depend heavily on details of context, as does their willingness to adopt telehealth despite those concerns [80]. Despite these privacy risks, users may still share their health data if they perceive the health benefits as outweighing the potential threats [18, 21, 80]. Additionally, many users fail to utilize security features like authentication passcodes to safeguard their health data [98], due in part to usability barriers [3].

Prior research has indicated that data-sharing practices in health apps lack transparency, raising concerns and complicating users' ability to control data flows [7, 78]. For instance, mHealth users want to better understand what data is collected, with whom it is shared, and how it is used [3, 39]. User review analysis showed that participants often find permissions in mHealth apps irrelevant to the core functionality, or unclear about their purpose [37]. Participants in another study had inaccurate expectations about data permissions in mHealth apps [3]. Meanwhile, health apps' privacy policies, if they are even provided at all, are typically vague about these details while not addressing users' most pressing concerns [35, 74, 101], are lengthy and difficult to understand [3, 31, 37, 81, 87], and can be changed at any time by developers [35, 86]. Similar problems have been found in extensive prior research on privacy policies [e.g. 34, 65, 72]; it seems health apps are no exception, despite the sensitive data they collect.

Motivation for Our Study. Prior work highlights serious user privacy concerns and lack of transparency in health apps. Our study assesses the effectiveness of privacy nutrition labels in closing the transparency gap, identifies their shortcomings, and offers recommendations for improving user awareness of telehealth apps' data practices and legal privacy protections.

2.2 Privacy Nutrition Labels

To counter difficulties with comprehension of privacy policies, researchers have proposed a "privacy nutrition labels" framework to provide users with clear, standardized information about how their data is collected, used, and shared by digital platforms [47, 48], similar to how nutrition labels on food products inform consumers about the contents and health implications of what they are consuming. Researchers have conceptualized the application of privacy nutrition labels in mobile apps [49], websites [47, 90], as well as Internet-of-Things devices [13, 24–26]. This research has shown that standardized privacy nutrition labels have potential to improve user experience compared to more traditional transparency mechanisms like privacy policies, as well as users' discovery and comprehension of information about data practices, enabling comparison across technological devices and services with diverse data practices and impacting decisions to purchase, install, or use them.

Although the idea became popular in the research community in 2009 after the publication of a study by Kelley et al. [47], the concept was first implemented in app marketplaces in 2020 by Apple and 2022 by Google. In App Privacy sections of the app descriptions on Apple's App Store, users can see what data types the app is collecting, what it is used for, and whether it is linked to users or used to track them [5]. Data Safety sections in Google's PlayStore shows users what data types are collected or shared by the app, for what purposes that data is used, and what security practices are implemented [79]. These app privacy nutrition labels are populated with information self-reported by the developers. Prior work has shown that developers find it challenging to accurately report data practices, especially if the apps collect extensive amounts of user data, and often make mistakes, misinterpret terms, or face ambiguity when reporting data practices [9, 51, 57]. This can lead to labels that are inaccurate and misleading [51, 54, 55, 119], outdated [8, 58],

or inconsistent across platforms [50, 88], with app permissions [51] or privacy policies [46, 102].

In addition to developers, users also suffer from usability issues with mobile privacy nutrition labels. In interviews with iPhone users, many were unaware of Apple's privacy labels, were not satisfied with inability to control data flows via labels, and often misunderstood them, due to their confusing structure and confusing or unknown terms [120]. The vagueness of the language decreased user trust in the labels. Another interview study [60] discovered that many participants did not expand the details in privacy nutrition labels, were confused about the definitions of terms, found information to be vague and insufficient, and questioned the accuracy of the labels. Some participants in both studies [60, 120] had misconceptions that app marketplaces (rather than or in addition to app developers) created the privacy label. Privacy nutrition labels in both Apple and Google app marketplaces do not or only partially address users' privacy and security related questions and concerns [121]. Participants were missing key information about who their data is shared with, retention policies, permission lists, whether their data is sold, and how their data is secured.

Motivation for Our Study. Prior research on privacy labels is focused on technical measurement, while studies with *app users* are limited. While providing qualitative insights about usability [60, 120] and quantified insights on whether they address common privacy and security questions [121], to the best of our knowledge, no prior work has investigated and quantified the impact of privacy labels on the *accuracy* of users' expectations, their *confidence* in understanding data practices, and their *beliefs about privacy protections and regulatory safeguards*—nor their *decision to install or use* a health app. Finally, no prior work on privacy labels focused on *health apps* in specific.

2.3 Existing Legal Protections

The Health Insurance Portability and Accountability Act (HIPAA) [14] is a federal US law that sets a standard to protect medical records and other personal health information. HIPAA applies to certain individually identifiable health-related information ("protected health information," or PHI) handled by "covered entities" with proper user authorization, which include most healthcare providers, health plans, healthcare clearinghouses, and their "business associates." While HIPAA's requirements for handling PHI, including privacy and security measures, and breach notification requirements, apply to health apps developed and distributed by covered entities like healthcare providers or insurance companies, they do not apply to the many health apps offered by companies that are not covered entities (unless such sharing is explicitly mentioned in the privacy policies and Business Associate Agreements) [14]. For instance, an application developed by a healthcare provider for use in remote patient counseling would be covered by HIPAA [109].

However, a health app that contains information generated by the consumer, like a blood pressure tracking app or a period-tracking app, would not [33, 89, 105, 109]. Legal analyses have highlighted gaps in legal protections for health app data [89, 106, 116]. For example, HIPAA does not apply to health apps used by consumers to transmit their own PHI to covered entities, for example apps where doctors can list their services and offer appointments, or to apps that do not collect identifiable health information [33, 109]. Even if a health app both transmits PHI to and from covered entities, it is still exempt from HIPAA, if the app is understood to be using the PHI on behalf of the consumer instead of the entity [109, 110].

Other privacy regulations, like FDA guidance [30] and the FTC's breach notification requirements for providers that handle consumer-provided electronic health records [28], are similarly complex and limited. For example, apps that do not make false or misleading claims, are unlikely to cause significant harm, or provide more benefits than harm are not subject to FTC enforcement [28]. A patchwork of state-specific privacy laws that govern health data (e.g., CCPA, Illinois Biometric Information Privacy Act, Virginia's Genetic Data Privacy Law) further convolute the understanding of legal privacy protections [32]. These complexities in privacy regulations coverage may result in users of some health apps having incorrect beliefs about their data being protected by HIPAA.

Indeed, prior research has identified gaps in users' understanding of legal protections for mobile and online data and how they apply to them [40, 108], and in users' comprehension of consumer data flows [61, 83, 94], including health data tracking [41].

Motivation for Our Study. Prior work has not focused on accuracy of users' expectations about *health data*. Investigating these disconnects, and the sources of users' misunderstandings of legal protections, can help enhance transparency and support users in making informed privacy decisions about health data.

3 Methods

We began both surveys by providing definitions of *telehealth platforms* ("a mobile app, website, or web app that helps you find, make or attend virtual or in-person appointments with physical or mental health care providers"). At the end of both surveys, we assessed participants' privacy attitudes, opinions, and prior experiences with health apps, and other background that could help contextualize their responses. Survey questions we analyzed can be found in Appendix E for Survey 1 and Appendix F for Survey 2.

3.1 Survey 1

3.1.1 Survey Design In Survey 1, we asked participants to read the Google Play Store description of a particular telehealth app and answer questions about it. Each participant saw only one randomly-assigned app from a total pool of 10 Android apps, divided into two conditions. The pool included 5 apps provided by independent developers (for the *Independent* condition) and 5 apps associated with healthcare providers (for the *Provider* condition).

In the Independent condition, we asked participants to imagine they don't have a regular healthcare provider, so needed to find a service to help them get a doctor's appointment, and that they found an app provided by an independent developer (not associated with any particular insurance, healthcare system, or medical provider). In the Provider condition, we told participants that their healthcare provider told them to find and book an appointment using the provider's app.

After showing the participants a screenshot of the Play Store description for their assigned app, we asked multiple-choice questions about whether they had prior experience with this app, and Likert-scale questions about how likely they were to download it,

and how well they thought it would protect their privacy. We then asked multiple-choice questions about their expectations of what data the app could collect, for how long it would be stored, with whom it could be shared, for what purposes those recipients could use the data, whether those recipients would be required by law to comply with various privacy regulations, and a Likert-scale question about participants' level of confidence in their understanding of the apps' data practices based on the Play Store description.

We next asked participants to read a screenshot of the full Data Safety section (DSS) for that app from the Play Store. After showing the DSS, we asked them to answer the same set of questions as before. We also asked participants whose self-reported likelihood of downloading the app or perceived privacy protection had changed about the reasons for those changes.

When showing the app descriptions and the DSS, we did not allow them to advance the screen before 90 seconds elapsed. We recorded their total reading time, and asked them to self-report how carefully they read the information. We used screenshots instead of sending users to the actual Google Play Store to ensure internal validity by making sure all participants saw the same information, to control the amount of time they spent on each page, and to prevent them from accessing additional out-of-scope information (e.g., reviews or privacy policies). Screenshots of the app descriptions and DSSs were captured on 6 March 2024 and can be found in the supplementary materials at https://bit.ly/3WU5bFb; we also include two illustrative examples in Appendix §B.

3.1.2 App Selection We wanted to compare users' expectations not only before and after their exposure to DSSs, but also with the actual data practices of the apps. We used a dataset of telehealth data practices measured via dynamic traffic analysis between August 2022 and October 2023 [116], which used custom instrumentation developed to capture network traffic on Android phones [84, 91, 118]. The dataset tested Android apps that are free to download, though many would require payment or insurance to use the full set of features. Human testers followed an interaction protocol for finding a doctor and making an appointment, ending when they were asked to pay or confirm an appointment (which occurred at different points depending on the app) [116].

We included both apps provided by independent developers and by healthcare providers themselves (clinics, hospital networks, or health insurance companies) because, for the most part, HIPAA classifies the former type as non-covered entities, and the latter as covered entities. The primary distinction between covered and non-covered entities is the nature of their interaction with PHI and their legal responsibilities under HIPAA.[1] We were curious if that distinction affects users' expectations of privacy. We also hypothesized that users may have different levels of trust and perceived freedom of choice between the independent and providers' apps. We included 5 apps per condition to test whether users' opinions differ significantly across apps within the Independent and Provider categories, or whether there are relatively generalizable patterns between the two groups.

Out of 68 telehealth apps then available in the traffic analysis dataset,[2] we selected the 10 shown in Table 1, which are equally split between covered and non-covered entities and diverse in number of downloads (between 10K and 1M) and in data collection and sharing practices. We excluded apps with fewer than 10K downloads, specialty-focused apps (e.g., dermatology), and those with recent negative press around privacy (e.g., GoodRX), to avoid biasing the results. All Provider apps and two Independent apps claimed HIPAA compliance in their privacy policy, while three Independent apps admitted HIPAA non-compliance or omitted that information. All Provider apps and three Independent apps provided a wide range of health services (we call these Generic apps), while two of the Independent apps specifically focused on mental health services.

3.2 Survey 2

Survey 2 explored participants' opinions and beliefs about legal privacy protections in telehealth apps *in general*, without showing information for any specific app. We asked about participants' expectations about sharing of personally identifiable data and medical data with various recipients, privacy policy update communications, recipients' obligations to comply with privacy regulations, and bounds on the data uses permitted by those regulations. Then we asked participants what restrictions they desired for sharing of data collected by telehealth apps, and what data types, recipients, and recipient purposes of use those restrictions should apply to.

3.3 Participant Recruitment and Ethics

We recruited participants for both surveys from the online platform Prolific in May 2024. Using Prolific's screening criteria, we selected a gender-balanced sample of US Android users over 18 years old. Prolific supplied additional demographic information. Participants from Survey 1 were blocked from responding to Survey 2.

We first conducted three cognitive walkthroughs with the user-testing service UserFeel, to test comprehension and flow. Initially, we had planned to run Surveys 1 and 2 as a single survey, but walkthrough interviews demonstrated it was too lengthy. To reduce fatigue and burden, and to avoid anchoring general perspectives we solicited in Survey 2 to the specific apps shown in Survey 1, we decided to split the surveys. We then conducted pilots with 50 participants for each, to estimate average times and as a final check for any potential errors. As we identified no mistakes and no need for further shortening, we include the pilot results in the analysis. We excluded all participants in either survey who failed one or both attention checks, or indicated that they no longer used an Android phone. Median times for included participants were 19 minutes for Survey 1 and 15.7 minutes for Survey 2. We compensated participants USD $5.25 and $3.93, respectively.

We obtained IRB approvals prior to conducting the research. All participants provided informed consent.

3.4 Analysis

Defining Accuracy of Expectations About Data Practices We assessed the accuracy of participants' expectations about the apps'

[1] *Covered entities* must comply with HIPAA privacy, security, and breach notification rules, ensuring the protection of PHI. *Non-covered entities* are not directly subject to HIPAA regulations, although they may incur obligations under HIPAA if they receive PHI indirectly through business associate agreements (BAA) with covered entities.

[2] Eventually, Webster et al. [116] found 409 Play Store apps that allowed users to make medical appointments, including 209 US-based apps. When we designed our study, they were still validating data and so far had only 68 US-based apps validated.

Table 1: Summary of information about apps used in Survey 1. (As of 5 December 2023.)

App name	Origin	Downloads (in thousands)[a]	App type	Self-reported HIPAA compliance	Developer
K Health | 24/7 Virtual Care	Provider	1,000	Generic	Yes	K Health, Inc.
Amwell: Doctor Visits 24/7	Provider	1,000	Generic	Yes	American Well Corp.
Doctor On Demand	Provider	1,000	Generic	Yes	Included Health, Inc.
PlushCare: Online Doctor	Provider	100	Generic	Yes	Accolade, Inc.
Galileo Health: Medical Care	Provider	50	Generic	Yes	Galileo, Inc.
Direct Health for Patients	Independent	100	Generic	Yes	Bender Medical Group, Inc.
ReGain - Couples Therapy	Independent	100	Therapy	Not mentioned	BetterHelp, Inc.
Teen Counseling	Independent	100	Therapy	Not mentioned	BetterHelp, Inc.
MEDIFI for Patients	Independent	50	Generic	Yes	Medifi
Forward - Primary Care For You	Independent	10	Generic	No	Forward

data practices by comparing their responses to the dynamic analysis dataset [116], which we used as ground truth. For the items for which ground truth was available,[3] we calculated the *false negative* rate based on each particular app's data practices as defined by the ground truth, by dividing the number of false negatives by the number of actual positives. False negative rates thus represent the proportions of cases when participants thought that a particular data type is not collected, that data is not shared with certain recipients, or that data is not used by recipients for certain purposes, but the ground truth showed that data is actually collected, shared, or used by recipients for that purpose.[4]

We focus on reporting and comparing false negatives because they reflect participants' most dangerous misconceptions that may violate their privacy expectations and most harm their privacy decision-making. These false negative rates represent a lower bound of unexpected data practices, as further app testing, beyond the paywall and appointment scheduling phase, might have revealed more extensive data collection and sharing practices not captured in the traffic analysis dataset. We do not report false negative rates for personal identifiers because the ground truth showed that they were not collected by any of the target apps.

Defining Accuracy of Expectations About Legal Protections We assessed the accuracy of participants' expectations about legal protections by comparing their responses to the actual applicability of privacy regulations. Section 5 of the FTC Act applies to all apps in our study, the GDPR does not apply because all participants were US residents and the apps are US-based, and COPPA does not apply because all the participants were adults (COPPA only applies if children themselves are using an app). Whether HIPAA and the FTC's Health Breach Notification Rule (HBNR) apply depends not only on the specific combination of app type, data recipient, and purpose, but also on other factors like BAAs and user consent. Here we are most interested in the *false positive* rates: the proportion of cases where participants thought data recipients are required by law to comply with a particular privacy regulation, but in reality they are not required to do so. To calculate false positive rates, we divided the number of false positives by the number of actual negatives. We focus on false positives because they reflect participants' most dangerous misconceptions about legal protections that actually do not exist. Because the FTC Act applies to all apps in our study, there could not be any false positives. We also did not calculate false positives for HIPAA and the FTC's HBNR because of the nuanced conditions for when they apply to telehealth apps outlined above.

Quantitative Analysis For measurement scales (e.g. privacy attitudes), we used mean values for each participant.

To account for non-normally distributed data, we used the non-parametric Wilcoxon Signed-Rank and McNemar tests to compare participants' responses before and after exposure to DSSs (and Fisher's exact test when there were less than 5 observations). We applied Bonferroni correction [96] to p-values in pairwise tests to account for multiple comparisons. For the regression analysis, we used Cumulative Link Mixed Models (CLMMs), suitable for non-independent data in multiple-measurement studies [16, 104]. For effect sizes, we report odds ratios (OR) that represent a measure of the change in the dependent variable occurring for a one-unit increase in the predictor variable, holding all other variables constant. Variance Inflation Factor (VIF) analysis confirmed absence of significant multicollinearity in all regression models [69, 114]. We used robust standard errors to mitigate heteroskedasticity revealed by the Breusch-Pagan test in two of the regression models [12].

Qualitative Analysis To analyze the open-ended responses, two coders independently developed initial codebooks based on themes that emerged in the responses. They met, discussed, and merged

[3] Ground truth was assessed for collection (i.e., data being sent to the app's servers) of all except two data types (video and audio recordings, which would not happen unless an actual appointment occurred). We assessed ground truth for two data recipients (third-party advertisers/trackers and third-party analytics companies). Ground truth about recipients' purposes of use could be reasonably inferred in three cases (providing medical treatment, processing payments, and analytics).

[4] As we collected screenshots specifically for this study, they do not match collection times for the ground truth dataset [116], raising the possibility that participants' expectations might have had different accuracy results if they had seen the earlier DSSs. We therefore checked historical app descriptions and DSS overviews using the Wayback Machine [**?**] and APKMirror [**?**], comparing information about the version used for ground truth (or the closest available version) with our screenshots. We found that two apps had changed their DSS overviews, with our screenshots listing more categories of data collected than the earlier versions. However, comparing this to the ground truth, this resulted in only one case where one data category (financial info) had been inaccurately omitted from the DSS overview for the ground truth version of one app but was added in the screenshot version, so the effect on false-negative results was likely quite minimal. Two apps did not yet have DSSs at the time of ground truth collection, and the other six did not show any changes in DSS overviews regarding data practices for which we calculated participants' accuracy.

the two codebooks. Then they coded the data using the final codebook, calculated the agreement rate, and discussed and resolved disagreements, eventually reaching a 100% agreement rate.

3.5 Limitations

Ecological Validity. To ensure relative similarity in the context of the role-playing task, we used hypothetical scenarios that may not represent users' actual insurance coverage, although we controlled for it in the regressions. In addition, to avoid potential updates in the app information during the study, and to avoid confounding factors related to the real-world variations in users' app store navigation patterns, we asked participants to read the screenshots of app descriptions and expanded views of DSSs instead of interacting with the actual Google Play store pages. Thus, our study has high internal validity, and illustrates the upper bound of participants' expectations about data practices in telehealth apps based on reading or at least skimming app descriptions and DSSs. Future work can explore how users' perspectives change when they naturally interact with the app store pages (including decisions on how to navigate app descriptions, collapsed DSS sections, user reviews, and privacy policy links), and when they are driven by the real-world user needs, preferences, and circumstances.

App Selection and Ground Truth Methods. To avoid user fatigue and keep the number of factors manageable, we limited the number and types of health apps that we included in the survey. In addition, we focused on Android apps because the ground truth dataset is specific to Android, and no similarly detailed datasets exist for iOS apps. Nevertheless, our results show interesting insights about differences in participants' privacy expectations between the Independent and Provider conditions, and that these expectations are relatively similar across apps within each condition. Future work can explore users' perspectives on other types of health apps, including iOS apps. Having chosen Android, we used Google Play Store descriptions as it is the largest Android marketplace outside China [6]. Future work could compare data safety formats used in different marketplaces. As noted in §3.4, we focus on *false negatives*—rather than *false positives*—because the ground truth methodology [116] did not capture data collection or sharing that would have occurred after the point of payment or appointment confirmation. We thus could not confidently determine false positives. Future work could include data practices beyond the paywall.

Interactions. To keep survey length manageable, we explored expectations about data types, recipients, and purposes in isolation. Future work could assess (e.g., with factorial vignettes) which data users expect to be shared with which recipients, for which purposes.

4 Results of Survey 1

4.1 Participants

We aimed to collect at least 770 responses for Survey 1, based on sample size calculations to achieve statistical power. We recruited 910 participants; after discarding 55 (as described in §3.3), we included the remaining 855 responses in the analysis.

We obtained a balanced sample in terms of gender, age (between 18 and 76 y.o., with average of 42), and education. Our sample was predominantly white (71%). The majority (76%) did not have education or work experience in computer science or information technology fields, but most used smartphone apps frequently (73%), and were employed full-time (76%) or part-time (24%).

The majority (88%) said they had used telehealth platforms on either laptop/desktop computers or smartphone/tablet at least once. Almost half (47%) said that their healthcare provider/doctor recommended the last telehealth platform they used, while 20% found it themselves, 19% followed an insurance company's recommendation, and 7% relied on a friend's recommendation. About 53% of participants had experienced a privacy or security violation in the past, but only 10% said it involved medical information. Only 9% of participants have no health insurance, while 2% don't know what insurance they have. Figure 8 in Appendix A provides a summary of participants' demographics and background.

After seeing an app description, 97% said they hadn't used the app before, 1.5% recalled using it, and the rest did not remember. Thus, our results predominantly reflect the opinions of participants viewing the app description and DSS for the first time, which is representative of most app store users' experiences when they look for an app to address their needs.

4.2 Findings

For brevity, we will refer to participants' responses after they read the app description (but before reading the DSS) as *ex-ante* and after they read the DSS as *ex-post.*

4.2.1 Expectations about Data Practices (RQ1 & RQ3a) This section examines participants' expectations (including false negatives) about data types collected by the telehealth apps (Table 2), recipients of that data (Table 3), purposes for which recipients will use the data (Table 4), and data retention periods (Table 5), and how those expectations changed after exposure to DSS. Expectations are also visualized in Appendix C, Figures 3–6. Note that "All of the above" responses are included in the expectations about individual data types and privacy regulations, and in the measures of false negatives and false positives.

While there were variations between individual apps in expectations about some of the individual data practices, we did not observe meaningful patterns in these variations. Therefore we focus on reporting aggregated results, as individual apps' data practices are out of scope for this research.

Data Types. The majority of participants expected telehealth apps to collect nearly all data types we asked about, except information about children (Table 2). (This is not surprising as the vignettes did not mention children, and participants may not have thought about what would happen if they tried to make an appointment for a child.) For most data types, participants had false negative rates below 30%. However, we found a false negative rate of between 33% and 54% for financial information, device identifiers and device information, and user interaction data, among cases where technical app analysis demonstrated those data types were collected. (Data about children had an even higher false negative rate, 62%; again, likely because the vignettes did not mention children.)

After exposure to DSSs, expectations about the collection of demographics, health data, signup credentials, insurance information, and physical attributes significantly decreased, and the false negative rates for these data types (except physical attributes) increased.

On the other hand, expectations about the collection of location, financial information, device identifiers and device information, user interactions, and personal identifiers significantly increased, while the false negative rates for these data types (except personal identifiers) decreased.

Recipients. Most participants thought that doctors and care provider employees would have access to collected information, and a majority thought insurance companies and payment processing services would as well (Table 3). In contrast, expectations regarding access by different third-party recipients were lower, but quite varied, ranging from analytics companies (40% ex-ante and 43% ex-post), to third parties outside the US (16% ex-ante and 18% ex-post). False negative rates were between 59% and 68% for third-party analytics companies' and third-party advertisers' access to the user data.

After exposure to DSSs, expectations that doctors and care providers, insurance companies, and pharmacies that provide medications to the user would access the data decreased significantly, while expectations that no one but the user would have access increased significantly. On the other hand, expectations that payment processing services, the app's developers, and government increased significantly. Exposure to the DSS did not change the rate of false negatives about recipients.

Recipients' Purposes of Use. Most commonly, participants believed that recipients would use telehealth app data for providing medical treatment, communicating with users, processing payments, complying with legal obligations, for analytics, or for security purposes (Table 4). Interestingly, about a third of all participants thought that it would be used for marketing and advertising or to sell to or share with third-party companies.

After exposure to DSSs, fewer participants expected their data to be used for providing medical treatment and selling or sharing with third-party companies, while more participants expected it to be used to comply with legal obligations, for analytics, and for security protections. Exposure to DSSs significantly decreased the rate of false negatives about the use of data for analytics (from 40% to 22%), but increased it for the purpose of providing medical treatment (from 11% to 17%). The rate of false negatives remained slightly below 30% for payment purposes both ex-ante and ex-post.

Data Retention. After exposure to DSSs, participants' expectations about data retention periods significantly changed (Table 5). The proportion of participants who thought that the data would be deleted only upon user request increased (33% ex-ante vs. 60% ex-post), while the expectations of deletion after a certain period of time (30% ex-ante vs. 15% ex-post) or after a goal is achieved (7% ex-ante vs. 4% ex-post), and the expectation that it will be kept indefinitely (29% ex-ante vs. 18% ex-post) significantly decreased.

4.2.2 Privacy Attitudes and Intentions (RQ2 & RQ3b) Here we focus our analysis on perceptions about how well the app protects user privacy *(Perceived Privacy*), confidence in understanding app's data practices (*Confidence*), and likelihood of downloading/using the app (*Likelihood*). We also tested differences between individual apps *within* the Independent and Provider conditions, but found that they were not significant (except slightly lower ex-ante Likelihood of using the two Therapy apps compared to the Generic apps), and thus we do not report app-specific analyses below.

Perceived Privacy in Telehealth Apps. More than half of the participants (61% ex-ante and 58% ex-post) thought that the app protected user privacy well. However, some thought the app protected it poorly (8% ex-ante and 22% ex-post). Participants who gave negative or neutral ex-ante scores explained in open-ended responses that they wanted the app description to have more information about data practices (45%) and privacy protections specifically (24%), and proof or guarantees of those protections being effective (25%). Those who gave negative or neutral ex-post scores said they wanted the telehealth apps to engage in less data collection/storage/use (23%), and for DSSs to provide details about data recipients (18%). Both ex-ante and ex-post, about 19% gave such scores due to a sense of resignation and general lack of trust that companies can effectively protect user privacy.

Perceived privacy protection levels significantly changed after exposure to the DSS ($p < 0.00001$). Specifically, they decreased for 30% and increased for 21% of participants. In open-ended responses, participants explained their increased perceptions of privacy protection mostly with improved transparency (26%)—and specifically with added details about recipients (17%), recipients' purposes of use (15%), and data types being collected (14%)—as well as reassurance that the app is not selling user data to third parties (12%). Decreased protection perception, in turn, was associated with the realization of excessive data collection (9%) and sharing (8%), or use of data for purposes that participants did not like (7%), including advertising and marketing (5%).

Confidence in Understanding Data Practices. Participants' confidence that they understand the app's data practices has changed after exposure to DSSs ($p < 0.00001$). Specifically, it decreased for 9% and increased for 58% of participants. Moreover, the proportion of participants who rated their confidence as low has decreased (49% ex-ante vs 17% ex-post, $p < 0.00001$), while the proportion of participants who rated their confidence as high has increased (21% ex-ante vs 45% ex-post, $p < 0.00001$).

Participants explained ex-ante low confidence predominantly by the lack (62%) or incompleteness (30%) of information about data practices. In contrast, after reading the DSSs, barely any participants explained their low confidence with the lack of any information about data practices (62% ex-ante vs. 5% ex-post, $p < 0.00001$), but rather with the incompleteness of information presented in DSSs (33%). Reasons that were not very common ex-ante were often mentioned as explanation of the low confidence ex-post, including the abundance of terminology/jargon (11% ex-ante and 29% ex-post), low clarity or vagueness (16% ex-ante and 29% ex-post), and description length (17% ex-ante and 20% ex-post).

Likelihood of Using the Telehealth App. About half the participants said they were unlikely to use the app (46% ex-ante and 51% ex-post), while about a third said they were likely to do it (35% ex-ante and 32% ex-post).

Based on open-ended responses, the main reasons for low Likelihood of using the app were utilitarian, such as perceptions that the app would not be helpful (e.g., would not provide accurate diagnoses) or relevant (especially for the therapy apps) (31% ex-ante and 30% ex-post). Many participants did not want to download the app because they already had another similar health app (21%

Table 2: Expectations about what types of user data are collected by telehealth apps.

Data type	Expectations			False negative rate		
	Ex-ante	Ex-post	p	Ex-ante	Ex-post	p
Contact info	94%	93%	0.3964	6%	7%	0.3964
Demographics	94%	85%	↓ **<0.0001**	6%	15%	↑ **<0.0001**
Health info	89%	81%	↓ **<0.0001**	10%	17%	↑ **<0.0001**
Signup credentials	86%	82%	↓ **0.0070**	14%	20%	↑ **0.0021**
Insurance info	82%	73%	↓ **<0.0001**	14%	23%	↑ **<0.0001**
Physical attributes	78%	71%	↓ **<0.0001**	19%	25%	0.3017
Location	75%	78%	↑ **0.0433**	27%	20%	↓ **0.0309**
Financial info	67%	79%	↑ **<0.0001**	33%	21%	↓ **<0.0001**
Device identifiers	58%	67%	↑ **<0.0001**	43%	34%	↓ **<0.0001**
Video recordings	57%	54%	0.0992			
Audio recordings	55%	54%	1			
Device info	54%	69%	↑ **<0.0001**	47%	32%	↓ **<0.0001**
User interactions	52%	66%	↑ **<0.0001**	54%	34%	↓ **<0.0001**
Personal identifiers	46%	52%	↑ **0.0014**	N/A	N/A	
Info about children	40%	37%	0.0969	62%	63%	0.9131
All of the above	17%	26%	↑ **<0.0001**			
Other	1%	1%	0.7893			
No data is collected	0%	0%	0.4795			

Table 3: Expectations about which recipients have access to user data collected by telehealth apps.

Recipients	Expectations			False negative rate		
	Ex-ante	Ex-post	p	Ex-ante	Ex-post	p
Doctors and care providers	91%	83%	↓ **<0.0001**			
Insurance companies	62%	55%	↓ **0.0002**			
Payment processing services	52%	59%	↑ **0.0009**			
Pharmacies that provide medications to the user	50%	46%	↓ **0.0253**			
Parent company of the care provider	41%	40%	0.5596			
3rd party analytics	40%	43%	0.1324	62%	59%	0.2000
Parent company of the app's developer	38%	41%	0.6085			
App's developers	34%	43%	↑ **<0.0001**			
3rd party advertisers	32%	31%	0.7372	68%	66%	0.3750
Pharmaceutical companies	30%	31%	0.4434			
Government	19%	25%	↑ **0.0001**			
3rd parties outside US	16%	18%	0.1491			
Informal caregivers	6%	6%	0.3865			
No one other than the user	2%	4%	↑ **0.0006**			
Other users	2%	2%	0.2812			
Other	2%	2%	0.0763			
General public	1%	2%	0.0665			

ex-ante and 15% ex-post), had insurance coverage and reimbursements concerns (18% ex-ante and 9% ex-post) or other cost-related concerns (13% ex-ante and 9% ex-post). Some participants were also skeptical of the virtual healthcare services as opposed to in-person doctor visits (18% ex-ante and 10% ex-post). While privacy concerns were not a common reason for low ex-ante Likelihood of using the app, worries about the extent of data collection (18%) and lack of adequate privacy and security protections (10%) were relatively more common reasons for low ex-post Likelihood.

Participants' Likelihood of using the app significantly changed after the exposure to DSSs ($p = 0.0001$). Specifically, it decreased for 18% and increased for 12% of participants. Participants attributed their change of mind predominantly to an improved understanding of the app's data practices (79%) and data protection levels (76%), the app's functionalities (43%), and the app's quality (35%).

4.2.3 Drivers of Privacy Attitudes and Intentions (RQ4) To understand the relationships between the main dependent variables (DVs)—Perceived Privacy, Confidence, and Likelihood—and participants' personal characteristics, attitudes, and experiences, we ran regression analysis. In this subsection, unless we explicitly mention *ex-ante* or *ex-post*, the finding applies to both variables.

We found significant positive relationships between the three main DVs. Participants with higher Perceived Privacy rated higher their Confidence in understanding the app's data practices and Likelihood of using the app. Participants with higher Confidence

Table 4: Expectations about which purposes recipients use data collected by telehealth apps for.

Purposes of use by recipients	Expectations			False negative rate		
	Ex-ante	Ex-post	p	Ex-ante	Ex-post	p
For providing medical treatment	89%	83%	↓ **0.0001**	11%	17%	↑ **<0.0001**
For communication purposes	73%	75%	0.4521			
For payment purposes	73%	72%	0.5384	27%	29%	0.5384
To comply with legal obligations	64%	68%	0.0292			
For analytics	62%	77%	↑ **<0.0001**	40%	22%	↓ **<0.0001**
For security protection	48%	66%	↑ **<0.0001**			
For marketing and advertising	40%	37%	0.1824			
To sell to or share it with third-party companies	31%	27%	0.0119			
For executing a merger/acquisition	11%	12%	0.6061			
Other	0%	1%	1.00			

Table 5: Expectations about the data retention periods for data collected by telehealth apps.

Retention period	Ex-ante	Ex-post	p-value
The data won't be stored at any point	1%	1%	0.4545
Delete immediately after the goal of use is achieved	7%	4%	↓ **0.0183**
Delete after a certain period of time (e.g., 3 months, 1 year, etc.)	30%	15%	↓ < **0.0001**
Keep until user requests deletion	33%	60%	↑ **<0.0001**
Keep indefinitely	30%	18%	↓ **<0.0001**
Other	1%	1%	0.7539

rated higher the Perceived Privacy and Likelihood of using the app. Similarly, higher Likelihood of using the app was associated with higher Perceived Privacy and Confidence in understanding the app's data practices. (See Tables 9–11 in Appendix D for details.)

Participants rated their Likelihood of use and the Perceived Privacy of the Independent telehealth apps lower than the Provider apps. This aligns with the observation that 57% thought that a Provider app would protect user privacy better, while only 11% of participants thought that an Independent app would do better.

Privacy attitudes and experiences significantly impacted the main DVs as well. Using the IUIPC sub-scale indices, higher levels of privacy concern about data collection were associated with lower Perceived Privacy and ex-ante Confidence; higher levels of concern about lack of control over personal data was associated with lower Likelihood of using the app; and greater privacy awareness was associated with higher Confidence, ex-ante Perceived Privacy, and ex-ante Likelihood of using the app. Prior experiences with privacy violations were associated with lower Confidence in understanding the app's data practices and lower ex-post Likelihood of using it.

Personal characteristics and experiences also had an effect on some of the DVs. Women rated ex-post Perceived Privacy protection levels 39% higher than men. Black participants rated ex-post Perceived Privacy 40% lower and ex-post Likelihood of using the app 81% higher than white participants. Participants with education or work experience in the information technology fields rated ex-ante Perceived Privacy 29% lower than participants without such experience. Greater experience with smartphones was associated with higher Likelihood of using the app. Participants who reported more frequent use of telehealth apps in general rated their Confidence and Likelihood of using the app higher than less frequent users and non-users of telehealth apps. Participants with health insurance had lower ex-ante Likelihood of using the telehealth apps in our study. This is not surprising, because many insurance providers in the US offer access to telehealth platforms as part of their services [112]. Participants who admitted that they read the app description in more detail had higher ex-ante Perceived Privacy levels, while those who said they read the DSSs in more detail had higher ex-post Confidence in understanding apps' practices.

4.2.4 Expectations about Regulatory Protections (RQ5) Table 6 summarizes participants' expectations about which privacy regulations the potential data recipients are required to comply with; the findings are also visualized in Figure 7 in Appendix C. After including "All of the above" responses in the responses for individual regulations, we found that about 90% of participants thought the recipients they selected are required by law to comply with HIPAA. These expectations were between 56% and 71% for other regulations we asked about. After exposure to DSSs, the number of participants who believed that the recipients they selected would be required to comply with the GDPR, the FTC Act, and/or FTC's HBNR, or who chose "All of the above", significantly increased. The rates of false positives were high (62-71%) for the GDPR and COPPA, and increased for the GDPR after reading DSSs.

When we asked about telehealth apps in general (not the specific app they'd seen earlier), 44% of participants thought the data they collect is protected by HIPAA in all circumstances (which is incorrect because HIPAA only protects covered entities). About a third did not know whether any circumstances would cause the waiving of HIPAA protections. Among the remaining 21% who mentioned various circumstances for HIPAA exemptions, many hypothesized that certain data types (e.g., those not related to health) (30%), anonymized (7%) or publicly available data (7%), or certain

recipients (10%), such as third-party companies (6%) or government and law enforcement agencies (9%), might not be covered by HIPAA. Some believed that the need to use telehealth app data in an emergency or life-threatening situation (9%), or the user's explicit consent (5%), could waive HIPAA protections. Finally, 3% thought that HIPAA does not apply if the app is based in or is provided to users in a location not governed by HIPAA (e.g., outside the US). Some noted that poor enforcement (13%) or apps' non-compliance with HIPAA requirements (8%) could also be a factor. No one suggested that HIPAA applicability could depend on whether the app is provided by a covered vs. a non-covered entity. Overall, many participants had low confidence in their understanding of the requirements for HIPAA compliance, with twice as many choosing *likely* yes or no responses, rather than *definitely* yes or no.

5 Results of Survey 2

5.1 Participants

We aimed to collect at least 385 responses for Survey 2. In total, 441 participants completed the survey. After excluding 40 responses (as described in §3.3), we analyzed the remaining 401.

We obtained a balanced sample in terms of gender, education, and age (between 19 and 71 y.o., average 41 y.o.) , Our participants were predominantly self-identify as white (66%). The majority were employed full-time (74%) or part-time (24%), while 12% were students. Most did not have education or work experience in computer science or IT (75%), and used smartphone apps frequently (73%).

Most participants (87%) had used telehealth platforms at least once. Almost 48% of participants experienced a privacy or security violation/incident in the past, of whom 13% said it involved medical information. Figure 8 in Appendix A provides a summary of demographics and background.

5.2 Findings

This section summarizes details of participants' responses about regulatory protections for *telehealth apps in general* (not the specific 10 Android apps tested in Survey 1).

Expectations about Regulatory Protections (RQ5) Participants' expectations of what telehealth apps are required to do by law if they want to share users' PHI with other entities or organizations differed depending on the intended purpose of use (see Table 7). Obtaining additional explicit consent was the most common answer for almost all of the purposes of use (except complying with legal obligations), chosen by 24–41% of participants. Limiting recipients' purpose of use or obtaining explicit consent in addition to limiting the purpose of use were second most common answers for all the purposes, except marketing/advertising and selling/sharing data with third parties (whereas 27% and 29% of participants thought that telehealth apps are not allowed to share user data for those purposes with other entities/organizations at all). A smaller proportion of participants, 19%, thought that telehealth apps are not required to do anything when sharing user data with other entities for the purposes of complying with legal obligations or for executing merger/acquisition. For other purposes of use, only a small proportion of participants (8–12%) thought that telehealth apps are not required to do anything when sharing user data.

Moreover, most participants expected telehealth apps to notify users about updates to their privacy policies, whereas 70% also expected to be required to provide consent to the changes, and 27% did not expect to be required to re-consent.

Preferences about Regulatory Protections Most participants said they prefer privacy regulations to require telehealth apps to obtain additional explicit user permission before sharing user data (60%), followed by limiting recipients' purposes of use (44%), and preventing telehealth apps from sharing the data at all (27%). Several participants suggested other restrictions, like not allowing sale of the data under any circumstances, or giving users full control over their data (2%), and 1% said that telehealth apps should not be required to do anything particular when sharing user data with other entities or organizations.

6 Discussion

6.1 Gaps in Expectations about Data Practices

While false negative rates were rather low for collection of most data types that users usually input themselves, they were higher for metadata. On the one hand, it is possible that data collection that happens in the background is more obscure to telehealth app users (see Lin et al. [59] for similar evidence not specific to health apps). On the other hand, based on their open-ended responses, participants may be less familiar with what information such data types as device identifiers, device information, and user interactions actually contain (in line with prior work on app privacy labels in general [60, 120]). False negatives were also high for financial information, perhaps because participants did not think through whether they might be charged for a medical appointment (especially given that the false negative rate was similar for Independent vs. Provider apps).

Participants' expectations about access by recipients beyond those directly involved in providing care or medications, or administering insurance claims and payments, were low. Less than half of participants expected user data to be shared with third parties, parent companies, and governments. Similarly, few participants expected user data to be shared with advertisers or used for advertising, and many have incorrect expectations about it. Thus, data sharing with third-parties and use of data for marketing violates the privacy expectations of many telehealth users.

Interestingly, although over 60% of participants expected user data to be used by recipients for analytics, only about 40% expected data recipients to be third-party analytics companies or the app's developers—the most likely entities to perform such analytics. In addition, only slightly over half of the participants expected data to be shared with payment processing services, although a substantially higher proportion expected the apps to collect financial information. **These insights signal that participants have incomplete mental models of data flows in telehealth apps, and do not always understand the involvement of third-party companies.**

6.2 Impact of Privacy Nutrition Labels

Exposure to Data Safety sections had both positive and negative impacts on participants' privacy expectations. On the one hand, DSSs decreased the rates of false negative expectations

Table 6: Expectations about privacy regulations with which recipients are required by law to comply.

Regulations	Expectations			False positive rate		
	Ex-ante	Ex-post	p	Ex-ante	Ex-post	p
HIPAA	90%	89%	0.0648			
GDPR	67%	71%	↑ **0.0021**	67%	71%	↑ **0.0030**
COPPA	63%	64%	0.1956	62%	64%	0.2314
FTC Act	56%	62%	↑ **< 0.0001**			
FTC's HBNR	59%	64%	↑ **0.0003**			
All of the above	40%	48%	↑ **< 0.0001**			
Other	2%	1%	0.2207			
None	4%	5%	↑ **0.0164**			

Table 7: Expectations about what telehealth apps are required to do if they want to share users' personally-identifiable health information (PHI) with other entities or organizations.

Purpose of use by recipients	Obtain additional explicit permission	Limit purpose (require the entity to only use PHI for this purpose)	Both obtain additional explicit permission and limit purpose	Telehealth apps are not allowed to share PHI with any entity at all	Telehealth apps are not required to do anything when they share
For providing medical treatment	36%	21%	28%	6%	8%
For payment purposes	30%	25%	24%	13%	8%
For analytics (incl. to support technical functionality, or to improve the app)	28%	23%	23%	15%	11%
For marketing and advertising	36%	10%	19%	27%	8%
To comply with legal obligations	24%	27%	24%	6%	20%
For executing a merger/acquisition	26%	17%	22%	16%	19%
For security protection	32%	20%	25%	13%	9%
For communications with users	36%	20%	22%	9%	11%
To sell to or share it with third-party companies	41%	7%	17%	29%	6%

about metadata collection, and data use for analytics. Initially, users' privacy expectations revolved primarily around data types, recipients, purposes, and regulations directly related to healthcare. However, DSSs increased participants' expectations about more general-purpose or less obvious data practices and applicable regulations, like collection of financial information and metadata, and data use by payment services, developers, and governments, e.g., for complying with legal obligations (and not just HIPAA), for analytics, or for security protection.

On the other hand, DSSs *increased* rates of false negatives for some data types that users usually input themselves, as well as data being used for the purpose of providing medical treatment, and increased the rates of false positives for protection under the GDPR. We hypothesize this decrease in accuracy may be due in part to confusion between data collected and data shared, and in part to inaccuracies in or omissions from DSSs (see §2.2 for an overview of similar issues not specific to health apps).

DSSs also boosted participants' Confidence in understanding apps' data practices, despite the significant increase in false negatives for some of those data practices. In other words, **DSSs promoted overconfidence among many participants, even when they did not increase the accuracy of their expectations**. In open-ended responses, many noted that the app descriptions rarely contained any information about privacy at all. In contrast, although participants negatively judged DSSs for excessive length, vagueness, and jargon, few described DSSs as lacking privacy information. Thus, although imperfectly delivered, privacy disclosures in DSSs did boost participants' Confidence, compared to having no or very minimal information from app descriptions only.

Moreover, we found that greater Confidence was associated with greater Perceived Privacy and Likelihood of using the app. This means that the current design of the DSS may at the same time promote incorrect privacy expectations and boost a false sense of Confidence, thus encouraging users to install telehealth apps that will likely violate those expectations.

The direct impact of DSSs on Perceived Privacy protection levels and Likelihood of using the app was also mixed, and depended on the specifics of the data practices that the DSSs presented. For some participants, the improved transparency and the reassurance that the app is not sharing data with or selling it to third parties improved Perceived Privacy and Likelihood of using the app. For other participants, DSSs revealed a greater extent of data collection, sharing, and use than they expected, which reduced their Perceived Privacy and Likelihood of using the app. Moreover, DSSs may have shifted participants' focus from utilitarian reasoning based on reading app descriptions towards more privacy-aware reasoning for deciding whether to install and use a telehealth app. Specifically, privacy concerns were less common reasons for low initial Likelihood to use telehealth apps, compared to insurance coverage, reimbursement and cost concerns, or skepticism about

virtual care. In contrast, many participants attributed changes in their Likelihood of using telehealth apps to privacy-related reasons after reading the DSSs. This is in line with prior work in non–health specific contexts showing that saliently presenting privacy information increased not only participants' awareness of data practices [22], but also the impact of this information on their decisions and behaviors [1, 2, 43, 107, 115].

Despite greater transparency about data practices compared to app descriptions, **many participants still viewed telehealth apps' DSSs as lacking details about data recipients, purposes of use, and types of data collected, and using unclear terminology and jargon.** This echoes prior findings that privacy nutrition labels across app domains do not address users' privacy and security questions and concerns, or do so only partially [60, 120, 121].

6.3 Design Recommendations

As DSSs did have some effect in shifting participants' focus from utilitarian to more privacy-aware reasoning, we recommend displaying such privacy information more prominently in the app stores. However, our findings about participants' expectations highlight gaps in their understanding of telehealth apps' data practices, even after seeing the DSSs, suggesting improvements are needed.

For DSSs to increase not just confidence, but also accuracy of expectations, they should more clearly differentiate between data *collection* and *sharing* (e.g. via visualizations or icons), fix inaccuracies, address vagueness in wording, and decrease confusing terminology. In particular, DSSs should move beyond broad categories and **offer more specific and contextually-relevant examples of the types of data collected within each category**. For instance, currently, DSSs simply say that payment information is collected or shared for a vague "app functionality" purpose, leaving the user to guess whether this means paying for appointments or medications or something else, and do not mention recipients. Telehealth apps should clarify what financial information is collected, what it is used for, and who it is shared with. Similarly, instead of the vague label "Health Information," telehealth apps could specify whether, e.g., medication lists, appointment history, audio or video recordings of appointments, or therapy notes are collected or shared.

Disclosures should also clarify what kinds of "analytics" and "personalization" the apps use data for, and whether it involves third party companies, as this was a common source of confusion among our participants. Relately, disclosures should better explain the meaning of terms for metadata, such as device identifiers, along with *contextual* explanations of what it is used for and why it is shared. For example, "Location data is used to match you with doctors in your area" is more informative than just "Location" that is used for "App functionality." Such contextual justifications have been shown to improve transparency, increase trust, and mitigate user concerns and decision-making fatigue for a variety of app types [36, 38, 49, 59].

It is especially important to **inform users about whether less-expected recipients, such as third-party or parent companies, advertisers, or government entities, get access to the data**, as without this information most participants (often incorrectly) assumed that only recipients directly involved in healthcare, insurance claims, and payment processing access user data. Such less-expectable information should be highlighted more saliently (e.g., in a brighter color, or with a warning icon), and included in the short *summary* about Data Safety in Google Play (before users click on "See details"). Brief, clear summaries are particularly useful in the telehealth context, where a sense of urgency about getting medical attention may cause users to make especially fast app assessments and decisions.

These details could be implemented as **interactive progressive disclosures to further reduce user fatigue and information overload**, which can lead to poor decisions, as well-documented in usable privacy/security literature [e.g., 15, 100, 113]. Prior work has shown that information about data practices can be overlooked when presented only before an app is downloaded [120], and is more likely to be noticed and remembered when shown after download [10]. Thus, to increase effectiveness, pre-installation labels could be combined with just-in-time [27, 93] and contextual [23, 93] permissions and notices. Progressive disclosure could reduce the cognitive burden arising from integrating notices with choices, which has been identified in prior non–health specific work [15, 17].

In addition, telehealth apps could **allow users to easily access and export their data** (as is independently important for health records). Easy access would allow users to update their beliefs, and compare privacy disclosures with the evidence of actual data collected. App stores could add a reporting functionality to allow users to report inaccuracies in DSSs (based on the exported data file, requested permissions, or direct experiences with the app). Regulators that enforce legal privacy protections could also collect users' feedback about inaccuracies in disclosures and violations of privacy expectations, via similar reporting features or online forms.

6.4 Comparisons of Participants' Expectations for Legal Protections with Reality

The way HIPAA defines covered entities differs from how participants conceptualize them. Because telehealth apps collect health information, almost all participants in our study assumed that HIPAA would apply to both Independent and Provider apps, while in reality there are nuanced circumstances defining covered entities. These gaps indicate that HIPAA's definitions of covered and non-covered entities do not align with users' expectations and may lead to incorrect assumptions about the regulatory protections against potential privacy violations that these recipients may cause to telehealth app users.

Meanwhile, participants expected higher levels of privacy protection in Provider apps than Independent apps. Healthcare providers are seen as experts in health-related matters and as bound by professional ethics and regulations, which may enhance their credibility [85]. Established healthcare brands have built reputations that can influence perceptions of their apps [52, 122]. Smaller Independent developers may thus find it harder to gain trust.

People who do not have health insurance—and are thus more likely to use Independent apps—are already more likely to be economically disadvantaged. If greater privacy concerns about Independent apps reduce willingness to use them, it could widen social disparities by limiting access to potentially more affordable virtual healthcare—but those who do use Independent apps will not have the same regulatory privacy protections as users of Provider apps.

Participants had some misconceptions about HIPAA exemptions. In contrast with their confusion about whether Independent apps are covered entities (and thus whether HIPAA protections apply), in some cases, participants thought HIPAA provides *less* coverage than it actually does. For instance, some suggested third party companies do not have to comply with HIPAA, while in reality business associates are required to comply if the app itself is a covered entity. Some incorrectly thought HIPAA would not apply to government-run healthcare entities.

Participants incorrectly expected notification of changes. While most participants thought telehealth apps are required to notify users about changes in privacy policies and obtain new consent, no federal laws explicitly mandate such notification or re-consent.

There is a gap between expected and desired legal privacy protections. While 60% of participants *wanted* telehealth apps to obtain informed user consent prior to sharing PHI with other entities, only 41% of participants thought that consent is *currently required* when sharing with or selling data to the third parties, 36% thought that consent is required when sharing data for marketing and advertising, and even fewer participants expected it for other purposes. Similarly, while 44% of participants would like the telehealth app to require data recipients to limit use of PHI to a specific purpose, only 27% of participants believed that telehealth apps currently do so.

6.5 Policy Recommendations

The gaps between users' expectations and preferences about legal protections and reality should be narrowed.

In the short term, it is important to **improve users' awareness and understanding of legal privacy protections for telehealth apps**. For example, privacy disclosures and FAQs (in app stores and on app websites, as well as in privacy policies) can directly address common misconceptions and clarify which local privacy regulations the specific telehealth app and data recipients are required to comply with, and what privacy protections these regulations ensure. Offering such information in multiple languages and formats (e.g., tables, images, audio, video) will improve accessibility for users with a variety of needs and levels of technical skill. For instance, for US users, *app stores* could mandate disclosure of whether the telehealth apps they host are covered or non-covered entities according to HIPAA, what other federal or state regulations may apply, and what the legal boundaries of their privacy protections are. *Telehealth apps* could undergo voluntary privacy risk and compliance assessments facilitated by third-party auditors, certification programs, or app stores. Use of clear standardized visual trust signals such as icons or badges to represent verification of, e.g., HIPAA compliance (for Provider apps) or other protections for health data (for Independent apps) could facilitate public awareness about privacy protections, increase credibility, and encourage telehealth apps to meet data- and risk-management standards. In-app feedback mechanisms could allow users to signal confusion or discomfort, prompting tailored educational outreach via email or in the app.

Healthcare providers can also emphasize the distinction between the legal protections their patients will get with the Provider app compared to an Independent telehealth app, to help patients understand the risks and benefits of using these apps. *Policymakers* can require developers to update their privacy disclosures (including DSSs) regularly to reflect any changes in their data practices and ensure that users have access to the most current information. In partnership with healthcare providers, insurers, and advocacy groups, government agencies can disseminate factual information, e.g., through infographics, FAQs, webinars, and community events, correcting myths about HIPAA protections and summarizing likely data practices of different types of telehealth apps.

In the long term, policymakers can **align legal protections for telehealth apps with users' expectations by expanding legal requirements** so that all telehealth apps collecting health data (not just those affiliated with providers) have to follow privacy standards similar to HIPAA, regardless of business agreements and purpose of data sharing/use. For example, policymakers should require not only HIPAA-covered apps but also Independent apps, to obtain substantive informed consent before collecting PHI. In addition, participants did not expect many of the healthcare operations uses that HIPAA *currently* allows. Thus, policymakers should consider expanding legal protections beyond PHI, as in recent guidance from HHS noting that even the name of an app can give away information about someone's health status [111].

Additionally, based on our findings about preferences, we recommend policymakers **require active user consent for major privacy policy changes** rather than assuming implicit acceptance, **implement standardized update notifications** across telehealth apps, including a summary of key changes, and **set mandatory data retention limits**. Further, policymakers could create a federal registry of telehealth apps to facilitate monitoring of these apps' data practices and adherence to regulated privacy protections.

Finally, development of clearer privacy regulations for telehealth apps will require collaboration between policymakers, healthcare organizations, consumer advocacy groups, and other key stakeholders. Ideally, such collaborations should be *international*, as many telehealth apps operate globally.

7 Conclusion

This research contributes quantitative evidence about how telehealth app users and non-users reason about data flows in those apps; how their beliefs about data flows and legal privacy protections affect their perception of the apps; and how Data Safety sections affect the nature and accuracy of their beliefs.

We found that participants' expectations about telehealth apps' data collection, sharing, and retention practices, and about recipients' use of data, were changed by reading DSSs (rather than just app descriptions), but that such changes often resulted in *less accurate* expectations. However, reading DSSs tended to lead to participants feeling more confident in their expectations (again, whether correct or not)—but had mixed effects on perceptions about how well the app protected their data and how likely they were to use it.

Participants' expectations about what legal privacy protections apply to the activities of telehealth apps and data recipients were also affected by DSSs, generally leading to higher expectation of protection. However, this was not always correct, and we noted a particular gap where many participants expected HIPAA rules to apply to a much broader set of entities than they actually do.

Acknowledgments

This research was supported by the U.S. National Science Foundation (award CNS-2055772) and the U.S. National Security Agency (contract H98230-18-D-0006).

Mitra Bokaei Hosseini, Mobin Javed, Michael Tschantz, and Primal Wijesekera contributed substantially to the design of the study. Mohsin Khan, Nicole Martinez-Martin, Alex Thomas, and our colleagues at the Berkeley Lab for Usable and Experimental Security also provided input and feedback. Naima Abrar, Shahzaib Ali, Maryam Arshad, Sumair Ijaz Hashmi, and Sheharyar Khalid conducted preliminary proof-of-concept studies. Reviewers for SOUPS and PoPETS gave feedback that helped to improve the paper.

Special thanks are due to Primal Wijesekera, Liam Webster, Nicole Martinez-Martin, and Anniyat Karymsak for sharing their ground truth data, and their expertise in interpreting it.

References

[1] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie F. Cranor, Saranga Komanduri, and et. al. 2017. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)* 50, 3 (2017), 1–41.

[2] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6221 (2015), 509–514.

[3] Bakheet Aljedaani, Aakash Ahmad, Mansooreh Zahedi, and M. Ali Babar. 2023. End-users' knowledge and perception about security of clinical mobile health apps: A case study with two Saudi Arabian mHealth providers. *Journal of Systems and Software* 195 (2023), 111519.

[44]]APKMirror APKMirror. [n. d.]. http://www.apkmirror.com Website.

[5] Apple Developer Support. 2023. App privacy details on the App Store. https://developer.apple.com/app-store/app-privacy-details/.

[6] Artem Dogtiev. 2025. App Stores List. Business of Apps. https://www.businessofapps.com/guide/app-stores-list/

[7] Audie A Atienza, Christina Zarcadoolas, Wendy Vaughon, Penelope Hughes, Vaishali Patel, Wen-Ying Sylvia Chou, and Joy Pritts. 2015. Consumer attitudes and perceptions on mHealth privacy and security: findings from a mixed-methods study. *Journal of Health Communication* 20, 6 (2015), 673–679.

[8] David G Balash, Mir Masood Ali, Xiaoyuan Wu, Chris Kanich, and Adam J Aviv. 2022. Longitudinal analysis of privacy labels in the apple app store. *arXiv preprint arXiv:2206.02658* (2022).

[9] Rebecca Balebako and Lorrie Cranor. 2014. Improving app privacy: Nudging app developers to protect user privacy. *IEEE Security & Privacy* 12, 4 (2014), 55–58.

[10] Rebecca Balebako, Florian Schaub, Idris Adjerid, Alessandro Acquisti, and Lorrie Cranor. 2015. The impact of timing on the salience of smartphone app privacy notices. In *Proceedings of the 5th ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Ddevices*. 63–74.

[11] Soumitra S Bhuyan, Hyunmin Kim, Oluwaseyi O Isehunwa, Naveen Kumar, Jay Bhatt, David K Wyant, Satish Kedia, Cyril F Chang, and Dipankar Dasgupta. 2017. Privacy and security issues in mobile health: Current research and future directions. *Health policy and technology* 6, 2 (2017), 188–191.

[12] Trevor S Breusch and Adrian R Pagan. 1979. A simple test for heteroscedasticity and random coefficient variation. *Econometrica: Journal of the Econometric Society* (1979), 1287–1294.

[13] Peter Caven, Zitao Zhang, Jacob Abbott, Xinyao Ma, and L Jean Camp. 2024. Comparing the Use and Usefulness of Four IoT Security Labels. In *Proceedings of the CHI Conf. on Human Factors in Comp. Systems*. 1–31.

[14] Centers for Medicare & Medicaid Services. 1996. The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

[15] Hanbyul Choi, Jonghwa Park, and Yoonhyuk Jung. 2018. The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior* 81 (2018), 42–51.

[16] Rune Haubo B Christensen. 2015. A Tutorial on fitting Cumulative Link Models with the ordinal Package. www.cran.r-project.org/package=ordinal.

[17] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie F. Cranor, and Norman Sadeh. 2020. Informing the design of a personalized privacy assistant for the internet of things. In *Proceedings of the CHI Conference on Human Factors in Comp. Systems*. 1–13.

[18] Cristina Nieves Perdomo Delgado and Luis Carlos Paschoarelli. 2020. Implementation of a Remote Control Application for Elderly People in Brazil: Analysis of the Factors Involved in the use of a Technological Innovation related to Telecare. *Disability, CBR & Inclusive Development* 31, 2 (November 2020), 148–156.

[19] Laura Dennison, Leanne Morrison, Gemma Conway, and Lucy Yardley. 2013. Opportunities and challenges for smartphone applications in supporting health behavior change: qualitative study. *JMIR* 15, 4 (2013), e86.

[20] Daniel Di Matteo, Alexa Fine, Kathryn Fotinos, Jonathan Rose, and Martin Katzman. 2018. Patient willingness to consent to mobile phone data collection for mental health apps: structured questionnaire. *JMIR mental health* 5, 3 (2018), e56.

[21] Linda Dimitropoulos, Vaishali Patel, Scott A Scheffler, and Steve Posnack. 2011. Public attitudes toward health information exchange: perceived benefits and concerns. *The American Journal of Managed Care* 17, 12 Spec No. (2011), SP111–6.

[22] Nico Ebert, Kurt Alexander Ackermann, and Björn Scheppler. 2021. Bolder is better: Raising user awareness through salient and concise privacy notices. In *Proceedings of the CHI Conf. on Human Factors in Computing Systems*. 1–12.

[23] Serge Egelman, Janice Tsai, Lorrie F. Cranor, and Alessandro Acquisti. 2009. Timing is everything? The effects of timing and placement of online privacy indicators. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 319–328.

[24] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie F. Cranor, and Hanan Hibshi. 2020. Ask the experts: What should be on an IoT privacy and security label?. In *IEEE Security & Privacy*. 447–464.

[25] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie F. Cranor. 2021. An informative security and privacy "nutrition" label for internet of things devices. *IEEE Security & Privacy* 20, 2 (2021), 31–39.

[26] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie F. Cranor. 2021. Which privacy and security attributes most impact consumers' risk perception and willingness to purchase IoT devices?. In *IEEE Security & Privacy*. 519–536.

[27] Federal Trade Commission. 2013. Mobile Privacy Disclosure: Building trust through transparency. (2013).

[28] Federal Trade Commission. 2016. Mobile Health Apps Interactive Tool. https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool.

[29] Joseph Firth, John Torous, Jennifer Nicholas, Rebekah Carney, Abhishek Pratap, Simon Rosenbaum, and Jerome Sarris. 2017. The efficacy of smartphone-based mental health interventions for depressive symptoms: a meta-analysis of randomized controlled trials. *World Psychiatry* 16, 3 (2017), 287–298.

[30] Food and Drug Administration. 2019. Guidance Document: Policy for Device Software Functions and Mobile Medical Applications. https://www.fda.gov/media/80958/download.

[31] Leah R. Fowler, Charlotte Gillard, and Stephanie R. Morain. 2020. Readability and Accessibility of Terms of Service and Privacy Policies for Menstruation-Tracking Smartphone Applications. *Health Promotion Practice* 21, 5 (September 2020), 679–683.

[32] Vivian Genaro Motti and Shlomo Berkovsky. 2022. Healthcare Privacy. In *Modern Socio-Technical Perspectives on Privacy*. Springer International Publishing.

[33] Tasha Glenn and Scott Monteith. 2014. Privacy in the Digital World: Medical and Health Data Outside of HIPAA Protections. *Current Psychiatry Reports* 16, 11 (Sept. 2014), 494. https://doi.org/10.1007/s11920-014-0494-4

[34] Mark A Graber, Donna M D Alessandro, and Jill Johnson-West. 2002. Reading level of privacy policies on internet health web sites. *Journal of Family Practice* 51, 7 (2002), 642–642.

[35] Sophie Grimme, Susanna Marie Spoerl, Frederike Jung, and Marion Koelle. 2025. Hidden in Plain Sight: A Structured Analysis of Privacy Policies in the Context of Body-worn 'FemTech' Technologies. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 105, 19 pages. https://doi.org/10.1145/3706598.3713702

[36] Jie Gu, Yunjie Calvin Xu, Heng Xu, Cheng Zhang, and Hong Ling. 2017. Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems* 94 (2017), 19–28.

[37] Omar Haggag, John Grundy, and Mohamed Abdelrazak. 2024. An Analysis of Privacy Issues and Policies of eHealth Apps. In *Proceedings of the International Conference on Evaluation of Novel Approaches to Software Engineering*.

[38] David Harborth and Alisa Frik. 2021. Evaluating and redefining smartphone permissions with contextualized justifications for mobile augmented reality apps. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 513–534.

[39] Leonie Hendrikoff, Lana Kambeitz-Ilankovic, Rüdiger Pryss, Fanny Senner, Peter Falkai, Oliver Pogarell, Alkomiet Hasan, and Henning Peters. 2019. Prospective acceptance of distinct mobile mental health features in psychiatric patients and mental health professionals. *Journal of Psychiatric Research* 109 (2019), 126–132.

[40] Chris Jay Hoofnagle and Jennifer M Urban. 2014. Alan Westin's Privacy Homo Economicus. *Wake Forest Law Review* 49 (2014), 261.

[41] Chris Jay Hoofnagle, Jennifer M Urban, and Su Li. 2012. Privacy and Modern Advertising: Most US Internet Users Want "Do Not Track" to Stop Collection of Data About their Online Activities. In *Proceedings of Amsterdam Privacy Conference*.

[42] Anna Ida Hudig and Jatinder Singh. 2025. Intimate Data Sharing: Enhancing Transparency and Control in Fertility Tracking. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 1184, 24 pages. https://doi.org/10.1145/3706598.3714089

[43] Thomas Hughes-Roberts and Elahe Kani-Zabihi. 2014. On-line privacy behavior: Using user interfaces for salient factors. *Journal of Computer and Communications* 2, 4 (2014), 220–231.

[44]]Wayback Internet Archive. [n. d.]. The Wayback Machine. http://web.archive.org Website.

[45] Leonardo Horn Iwaya, Aakash Ahmad, and M. Ali Babar. 2020. Security and Privacy for mHealth and uHealth Systems: A Systematic Mapping Study. *IEEE Access* 8 (2020), 150081–150112.

[46] Akshath Jain, David Rodriguez, Jose M Del Alamo, and Norman Sadeh. 2023. ATLAS: Automatically detecting discrepancies between privacy policies and privacy labels. In *2023 IEEE European Symposium on Security and Privacy Workshops*. 94–107.

[47] Patrick G. Kelley, Joanna Bresee, Lorrie F. Cranor, and Robert W Reeder. 2009. A" nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. 1–12.

[48] Patrick G. Kelley, Lucian Cesca, Joanna Bresee, and Lorrie F. Cranor. 2010. Standardizing privacy notices: an online study of the nutrition label approach. In *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*. 1573–1582.

[49] Patrick G. Kelley, Lorrie F. Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*. 3393–3402.

[50] Rishabh Khandelwal, Asmit Nayak, Paul Chung, and Kassem Fawaz. 2023. Comparing Privacy Labels of Applications in Android and iOS. In *Proceedings of the 22nd Workshop on Privacy in the Electronic Society*. 61–73.

[51] Rishabh Khandelwal, Asmit Nayak, Paul Chung, Kassem Fawaz, Antonio Bianchi, et al. 2024. Unpacking privacy labels: A measurement and developer perspective on google's data safety section. In *33rd USENIX Security Symposium*. 2831–2848.

[52] Sayed Hamid Khodadad Hosseini and Leila Behboudi. 2017. Brand trust and image: effects on customer satisfaction. *International Journal of Health Care Quality Assurance* 30, 7 (2017), 580–590.

[53] Agnieszka Kitkowska, Farzaneh Karegar, and Erik Wästlund. 2023. Share or Protect: Understanding the Interplay of Trust, Privacy Concerns, and Data Sharing Purposes in Health and Well-Being Apps. In *Proceedings of the 15th Biannual Conference of the Italian SIGCHI Chapter*. 1–14.

[54] Simon Koch, Malte Wessels, Benjamin Altpeter, Madita Olvermann, and Martin Johns. 2022. Keeping privacy labels honest. *Proceedings on Privacy Enhancing Technologies* (2022).

[55] Konrad Kollnig, Anastasia Shuba, Max Van Kleek, Reuben Binns, and Nigel Shadbolt. 2022. Goodbye tracking? Impact of iOS app tracking transparency and privacy labels. In *Proceedings of the ACM Conf. on Fairness, Accountability, and Transparency*. 508–520.

[56] Paul Krebs and Dustin T Duncan. 2015. Health app use among US mobile phone owners: a national survey. *JMIR mHealth and uHealth* 3, 4 (2015), e101.

[57] Tianshi Li, Kayla Reiman, Yuvraj Agarwal, Lorrie F. Cranor, and Jason I Hong. 2022. Understanding challenges for developers to create accurate privacy nutrition labels. In *Proceedings of the CHI Conf. on Human Factors in Comp. Systems*. 1–24.

[58] Yucheng Li, Deyuan Chen, Tianshi Li, Yuvraj Agarwal, Lorrie F. Cranor, and Jason I Hong. 2022. Understanding iOS privacy nutrition labels: An exploratory large-scale analysis of App Store data. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*. 1–7.

[59] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the ACM Conference on Ubiquitous Computing*. 501–510.

[60] Yanzi Lin, Jaideep Juneja, Eleanor Birrell, and Lorrie Cranor. 2023. Data Safety vs. App Privacy: Comparing the Usability of Android and iOS Privacy Labels. *arXiv preprint arXiv:2312.03918* (2023).

[61] Byron Lowens, Vivian Genaro Motti, and Kelly Caine. 2017. Wearable privacy: Skeletons in the data closet. In *IEEE International Conference on Healthcare Informatics*. 295–304.

[62] Deborah Lupton. 2021. "Sharing Is Caring:" Australian Self-Trackers' Concepts and Practices of Personal Data Sharing and Privacy. *Frontiers in Digital Health* 3 (2021), 649275.

[63] Deborah Lupton and Sarah Pedersen. 2016. An Australian survey of women's use of pregnancy and parenting apps. *Women and Birth* 29, 4 (Aug. 2016), 368–375.

[64] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.

[65] Aleecia M McDonald and Lorrie F. Cranor. 2008. The cost of reading privacy policies. *ISJLP* 4 (2008), 543.

[66] Maryam Mehrnezhad and Teresa Almedia. 2021. Caring for Intimate Data in Fertility Technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–11.

[67] Maryam Mehrnezhad and Teresa Almeida. 2023. "My sex-related data is more sensitive than my financial data and I want the same level of security and privacy": User Risk Perceptions and Protective Actions in Female-oriented Technologies. In *Proceedings of the European Symposium on Usable Security*. 1–14.

[68] Kathryn E Muessig, Emily C Pike, Beth Fowler, Sara LeGrand, Jeffrey T Parsons, Sheana S Bull, Patrick A Wilson, David A Wohl, and Lisa B Hightow-Weidman. 2013. Putting prevention in their pockets: developing mobile phone-based HIV interventions for black men who have sex with men. *AIDS Patient Care and STDs* 27, 4 (2013), 211–222.

[69] John Neter, Michael H Kutner, Christopher J Nachtsheim, William Wasserman, et al. 1996. Applied linear statistical models. (1996).

[70] Jennifer Nicholas, Katie Shilton, Stephen M. Schueller, Elizabeth L. Gray, Mary J. Kwasny, and David C. Mohr. 2019. The Role of Data Type and Recipient in Individuals' Perspectives on Sharing Passively Collected Smartphone Data for Mental Health: Cross-Sectional Questionnaire Study. *JMIR mHealth and uHealth* 7, 4 (April 2019), e12578.

[71] Leysan Nurgalieva, David O'Callaghan, and Gavin Doherty. 2020. Security and Privacy of mHealth Applications: A Scoping Review. *IEEE Access* 8 (2020), 104247–104268.

[72] Jonathan A Obar and Anne Oeldorf-Hirsch. 2020. The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society* 23, 1 (2020), 128–147.

[73] Achilleas Papageorgiou, Michael Strigkos, Eugenia Politou, Efthimios Alepis, Agusti Solanas, and Constantinos Patsakis. 2018. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access* 6 (2018), 9390–9403.

[74] Lisa Parker, Vanessa Halter, Tanya Karliychuk, and Quinn Grundy. 2019. How private is your mental health app data? An empirical study of mental health app privacy policies and practices. *International Journal of Law and Psychiatry* 64 (May 2019), 198–204.

[75] Bambang Parmanto, Gede Pramana, Daihua Xie Yu, Andrea D Fairman, Brad E Dicianno, and Michael P McCue. 2013. iMHere: A novel mHealth system for supporting self-care in management of complex and chronic conditions. *JMIR mHealth and uHealth* 1, 2 (2013), e10.

[76] Wei Peng, Shaheen Kanthawala, Shupei Yuan, and Syed Ali Hussain. 2016. A qualitative study of user perceptions of mobile health apps. *BMC Public Health* 16, 1 (2016), 1–11.

[77] Stacey Pereira, Jill Oliver Robinson, Hayley A. Peoples, Amanda M. Gutierrez, Mary A. Majumder, Amy L. McGuire, and Mark A. Rothstein. 2017. Do privacy and security regulations need a status update? Perspectives from an intergenerational survey. *PLOS ONE* 12, 9 (Sept. 2017), e0184525.

[78] Miloslava Plachkinova, Steven Andrés, and Samir Chatterjee. 2015. A taxonomy of mhealth apps–Security and privacy concerns. In *48th Hawaii International Conference on System Sciences*. 3187–3196.

[79] Play Console Help. 2023. Provide information for Google Play's Data safety section. https://support.google.com/googleplay/android-developer/answer/10787469?hl=en.

[80] Javad Pool, Saeed Akhlaghpour, Farhad Fatehi, and Leonard C. Gray. 2022. Data privacy concerns and use of telehealth in the aged care context: An integrative review and research agenda. *International Journal of Medical Informatics* 160 (April 2022), 104707.

[81] Adam Powell, Preeti Singh, and John Torous. 2018. The complexity of mental health app privacy policies: a potential barrier to privacy. *JMIR mHealth and uHealth* 6, 7 (2018), e158.

[82] Judith G Proudfoot, Gordon B Parker, Dusan Hadzi Pavlovic, Vijaya Manicavasagar, Einat Adler, and Alexis E Whitton. 2010. Community attitudes to the appropriation of mobile phones for monitoring and managing depression, anxiety, and stress. *JMIR* 12, 5 (2010), e64.

[83] Ashwini Rao, Florian Schaub, Norman Sadeh, Alessandro Acquisti, and Ruogu Kang. 2016. Expecting the unexpected: Understanding mismatched privacy expectations online. In *12th Symp. on Usable Privacy and Security*. 77–96.

[84] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. 2018. "Won't somebody think of the children?" Examining COPPA compliance at scale. *Proceedings on Privacy Enhancing Technologies* 2018, 3 (2018), 63–83.

[85] Frank A Riddick. 2003. The code of medical ethics of the American Medical Association. *Ochsner Journal* 5, 2 (2003), 6–10.

[86] Jessica L Roberts and Jim Hawkins. 2020. When health tech companies change their terms of service. *Science* 367 (2020), 745.

[87] Julie M Robillard, Tanya L Feng, Arlo B Sporn, Jen-Ai Lai, Cody Lo, Monica Ta, and Roland Nadler. 2019. Availability, readability, and content of privacy policies and terms of agreements of mental health apps. *Internet Interventions*

17 (2019), 100243.
[88] David Rodriguez, Akshath Jain, Jose M Del Alamo, and Norman Sadeh. 2023. Comparing privacy label disclosures of apps published in both the App Store and Google Play Stores. In *IEEE European Symposium on Security and Privacy Workshops*. 150–157.
[89] Celia Rosas. 2019. The future is femtech: Privacy and data security issues surrounding femtech applications. *Hastings Business Law Journal* 15 (2019), 319.
[90] Mortaza S. Bargh, Maud van de Mosselaar, Paul Rutten, and Sunil Choenni. 2022. On using privacy labels for visualizing the privacy practice of SMEs: challenges and research directions. In *Proceedings of the 23rd Intl. Conf. on Digital Gov. Res.* 166–175.
[91] Nikita Samarin, Shayna Kothari, Zaina Siyed, Oscar Bjorkman, Reena Yuan, Primal Wijesekera, Noura Alomar, Jordan Fischer, Chris Hoofnagle, and Serge Egelman. 2023. Lessons in VCR Repair: Compliance of Android App Developers with the California Consumer Privacy Act (CCPA). *Proceedings on Privacy Enhancing Technologies (PoPETs)* 2023, 3 (2023), 103–121. https://doi.org/10.56553/popets-2023-0072
[92] Emily N. Satinsky, Corine Driessens, David Crepaz-Keay, and Antonis Kousoulis. 2018. Mental health service users' perceptions of data sharing and data protection: a qualitative report. *Journal of Innovation in Health Informatics* 25, 4 (2018), 239–242.
[93] Florian Schaub, Bastian Könings, and Michael Weber. 2015. Context-adaptive privacy: Leveraging context awareness to support privacy decision making. *IEEE Pervasive Computing* 14, 1 (2015), 34–43.
[94] Awanthika R Senarath and Nalin Asanka Gamagedara Arachchilage. 2018. Understanding user privacy expectations: A software developer's perspective. *Telematics and Informatics* 35, 7 (2018), 1845–1862.
[95] Emily Seto, Kevin J Leonard, Joseph A Cafazzo, Jan Barnsley, Caterina Masino, and Heather J Ross. 2012. Perceptions and experiences of heart failure patients and clinicians on the use of mobile phone-based telemonitoring. *Journal of Med. Internet Res.* 14, 1 (2012), 25.
[96] Juliet Popper Shaffer. 1995. Multiple hypothesis testing. *Annual Review of Psychology* 46, 1 (1995), 561–584.
[97] Lucy Simko, Jack Chang, Maggie Jiang, Ryan Calo, Franziska Roesner, and Tadayoshi Kohno. 2022. COVID-19 contact tracing and privacy: A longitudinal study of public opinion. *Digital Threats: Research and Practice* 3, 3 (2022), 1–36.
[98] Katherine A Smith, Leming Zhou, and Valerie JM Watzlaf. 2017. User authentication in smartphones for telehealth. *Intl. Journal of Telerehabilitation* 9, 2 (2017), 3.
[99] Qiurong Song, Yanlai Wu, Rie Helene (Lindy) Hernandez, Yao Li, Yubo Kou, and Xinning Gui. 2025. Understanding Users' Perception of Personally Identifiable Information. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 240, 24 pages. https://doi.org/10.1145/3706598.3713783
[100] Brian Stanton, Mary F Theofanos, Sandra Spickard Prettyman, and Susanne Furman. 2016. Security fatigue. *It Professional* 18, 5 (2016), 26–32.
[101] Thomas Starks, Kshitij Patil, and Aqueasha Martin-Hammond. 2024. Exploring Users' Perspectives of Mobile Health Privacy and Autonomy. In *Pervasive Computing Technologies for Healthcare*. 70–91.
[102] Anne Stopper and Jen Caltrider. 2023. See No Evil: Loopholes in Google's Data Safety Labels Keep Companies in the Clear and Consumers in the Dark. Mozilla report.
[103] Gioacchino Tangari, Muhammad Ikram, Kiran Ijaz, Mohamed Ali Kaafar, and Shlomo Berkovsky. 2021. Mobile health and privacy: cross sectional study. *BMJ* 373 (June 2021), n1248.
[104] Jack E Taylor, Guillaume A Rousselet, Christoph Scheepers, and Sara C Sereno. 2023. Rating norms should be calculated from cumulative link mixed effects models. *Behavior Research Methods* 55, 5 (2023), 2175–2196.
[105] Kim Theodos and Scott Sittig. 2020. Health information privacy laws in the digital age: HIPAA doesn't apply. *Perspectives in health information management* 18, Winter (2020), 1l.
[106] Stacey A Tovino. 2019. Going Rogue: Mobile Research Applications and the Right to Privacy. *Notre Dame Law Review* 95 (2019), 155.
[107] Janice Y Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. The effect of online privacy information on purchasing behavior: An experimental study. *Info. Systems Research* 22, 2 (2011), 254–268.
[108] Jennifer M Urban, Chris Jay Hoofnagle, and Su Li. 2012. Mobile phones and privacy. *UC Berkeley Public Law Research Paper* 2103405 (2012).
[109] US Dept. of Health & Human Services. 2016. Health App Use Scenarios & HIPAA. https://www.hhs.gov/sites/default/files/ocr-health-app-developer-scenarios-2-2016.pdf.
[110] US Dept. of Health & Human Services. 2020. The Access Right, Health Apps, & APIs. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html.
[111] US Dept. of Health & Human Services. 2022. Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html
[112] US Dept. of Health & Human Services. 2025. Private insurance coverage for telehealth. https://telehealth.hhs.gov/providers/billing-and-reimbursement/private-insurance-coverage-for-telehealth.
[113] Karl Van Der Schyff, Greg Foster, Karen Renaud, and Stephen Flowerday. 2023. Online privacy fatigue: A scoping review and research agenda. *Future Internet* 15, 5 (2023), 164.
[114] Kristina P Vatcheva, MinJae Lee, Joseph B McCormick, and Mohammad H Rahbar. 2016. Multicollinearity in regression analyses conducted in epidemiologic studies. *Epidemiology* 6, 2 (2016).
[115] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie F. Cranor, Alain Forget, and Norman Sadeh. 2014. A field trial of privacy nudges for Facebook. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 2367–2376.
[116] Liam Webster, Mohsin Khan, Anniyat Karymsak, Nicole Martinez, and Primal Wijesekera. 2025. Understanding your Health Data, Apps, & US Regulations – Demystifying The Android Telehealth Ecosystem. Presented at the ACM Symposium on Computer Science and Law, Munich, Germany, March 25–27, 2025.
[117] Haohuang Wen, Qingchuan Zhao, Zhiqiang Lin, Dong Xuan, and Ness Shroff. 2020. A study of the privacy of COVID-19 contact tracing apps. In *Intl. Conf. on Security and Privacy in Communication Networks*.
[118] Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, and Konstantin Beznosov. 2015. Android permissions remystified: A field study on contextual integrity. In *24th USENIX Security Symposium (USENIX Security 15)*. 499–514.
[119] Yue Xiao, Zhengyi Li, Yue Qin, Xiaolong Bai, Jiale Guan, Xiaojing Liao, and Luyi Xing. 2023. Lalaine: Measuring and Characterizing Non-Compliance of Apple Privacy Labels. In *32nd USENIX Security Symposium*. 1091–1108.
[120] Shikun Zhang, Yuanyuan Feng, Yaxing Yao, Lorrie F. Cranor, and Norman Sadeh. 2022. How usable are iOS app privacy labels? *Proceedings on Privacy Enhancing Technologies* (2022).
[121] Shikun Zhang and Norman Sadeh. 2023. Do privacy labels answer users' privacy questions?. In *Workshop on Usable Security and Privacy*.
[122] Sijing Zheng, Siu Fu Hui, and Zhilin Yang. 2017. Hospital trust or doctor trust? A fuzzy analysis of trust in the health care setting. *J. of Bus. Res.* 78 (2017), 217–225.
[123] Leming Zhou, Jie Bao, Valerie Watzlaf, and Bambang Parmanto. 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 (2019), e11223.

A Participants

Table 8: Summary of participants' background.

	Survey 1	Survey 2
Gender		
Men	50%	50%
Women	48%	47%
Non-binary	2%	2%
Prefer not to say	1%	0%
Race or ethnicity		
White	71%	66%
Asian	6%	8%
Black	13%	15%
Mixed	7%	8%
Other	2%	3%
Prefer not to say	0%	0%
Highest level of education completed		
No formal qualifications	0%	0%
Secondary education	2%	3%
High school diploma	21%	22%
Technical/community college	24%	22%
Undergraduate degree	38%	36%
Graduate degree	12%	16%
Doctorate degree	3%	2%
Don't know / Not applicable	0%	0%
Smartphone experience		
I rarely use my smartphone for anything other than calling and texting	1%	2%
I occasionally use a few different apps on my smartphone	15%	14%
I often use a lot of different apps on my smartphone	73%	70%
I understand the technical details of how my smartphone works and can create apps myself	12%	14%
Used telehealth platforms on desktop/laptop		
Never	23%	24%
Less than once a year	20%	20%
Once or several times a year	37%	39%
Once or several times a month	16%	12%
Once or several times a week	4%	4%
Once or several times a day	0%	2%
Used telehealth platforms on smartphone/tablet		
Never	23%	25%
Less than once a year	18%	20%
Once or several times a year	38%	33%
Once or several times a month	16%	13%
Once or several times a week	4%	6%
Once or several times a day	1%	2%
Total number of participants	855	401

B Example Screenshots of an App from the Study

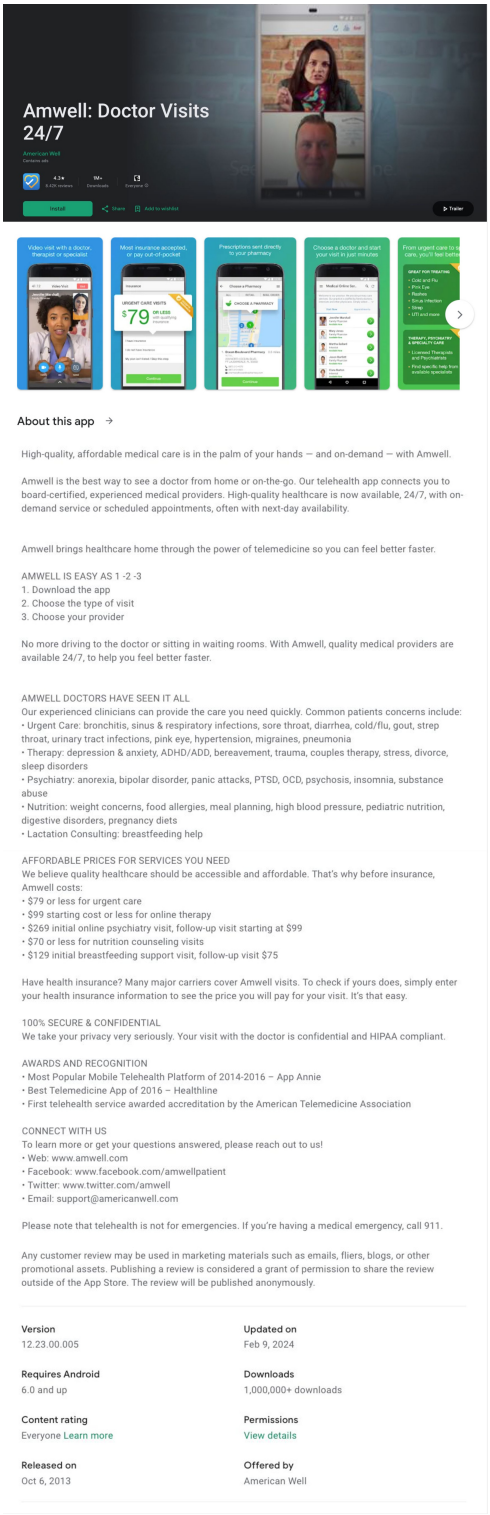

Figure 1: App description.

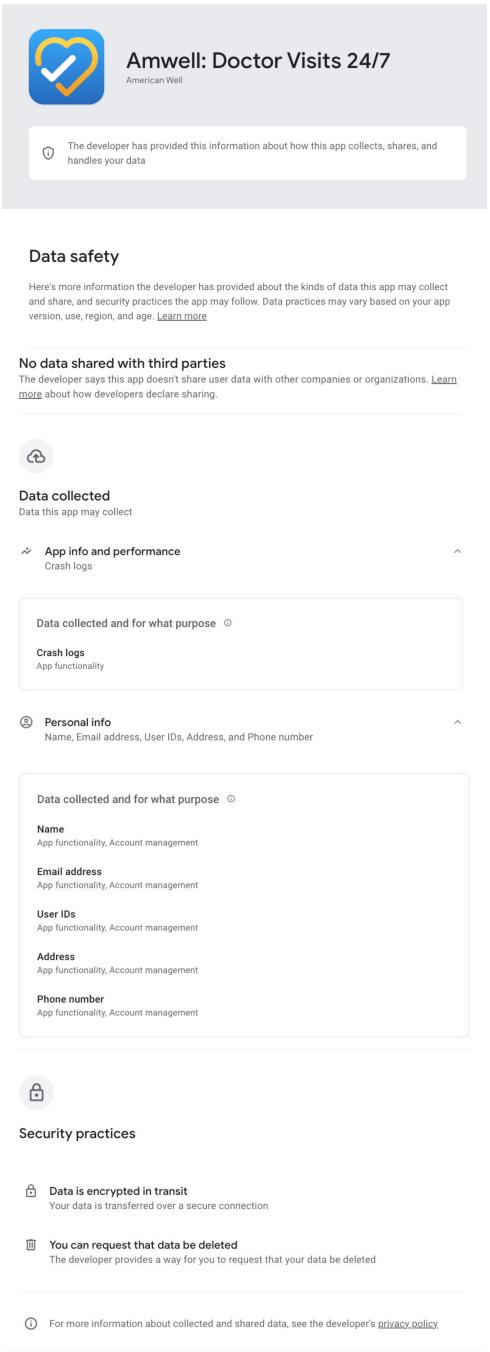

Figure 2: Data Safety section.

C Visualization of Responses from Survey 1

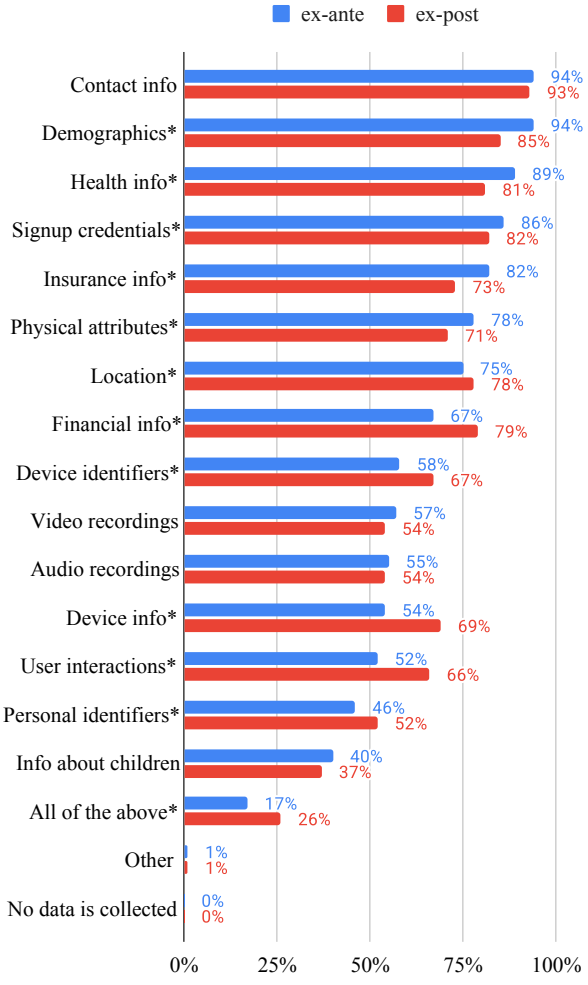

Figure 3: Expectations about what types of user Data are collected by telehealth apps. Asterisks indicate significant differences between ex-ante and ex-post expectations.

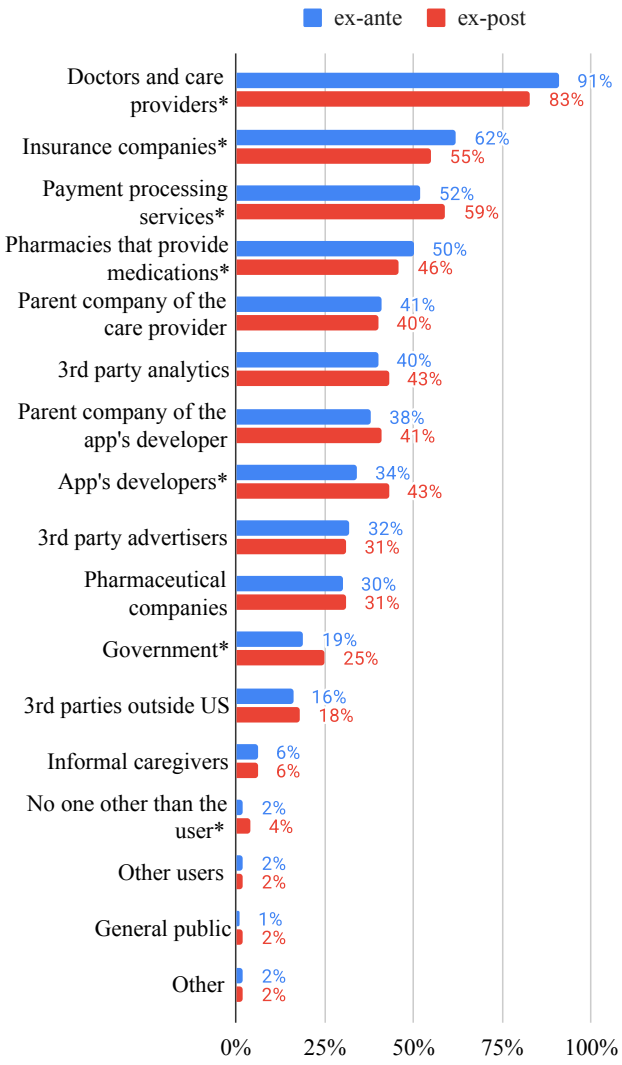

Figure 4: Expectations about Recipients having access to user data collected by telehealth apps. Asterisks indicate significant differences between ex-ante and ex-post expectations.

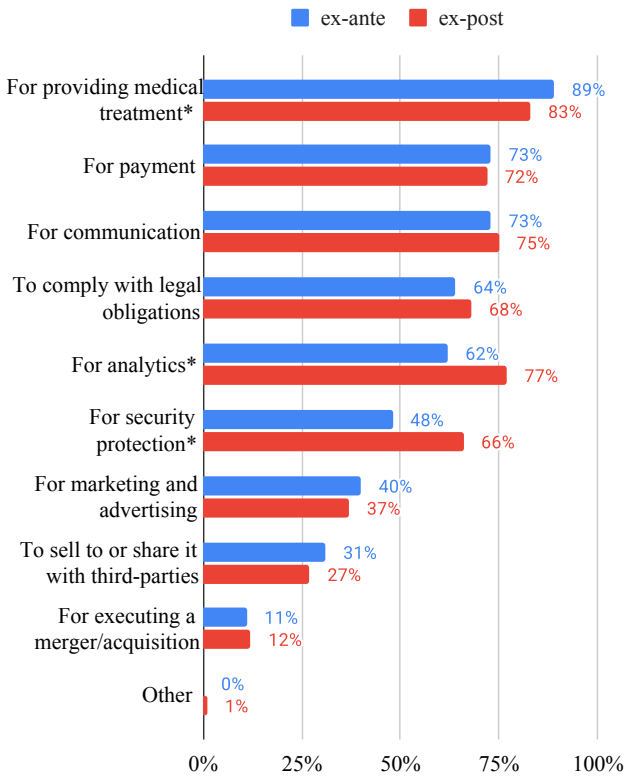

Figure 5: Expectations about which purposes recipients use data collected by telehealth apps for. Asterisks indicate significant differences between ex-ante and ex-post expectations.

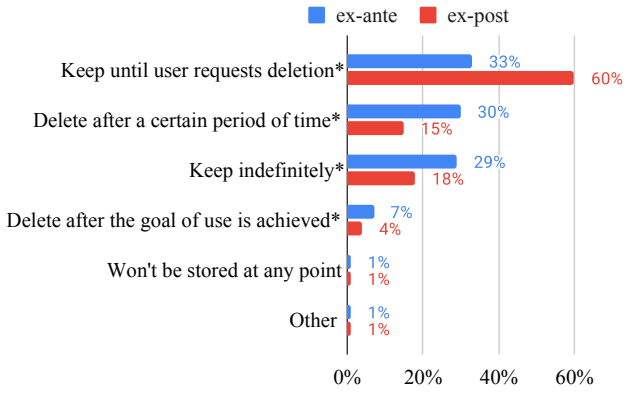

Figure 6: Expectations about how long telehealth apps keep the data they collected. Asterisks indicate significant differences between ex-ante and ex-post expectations.

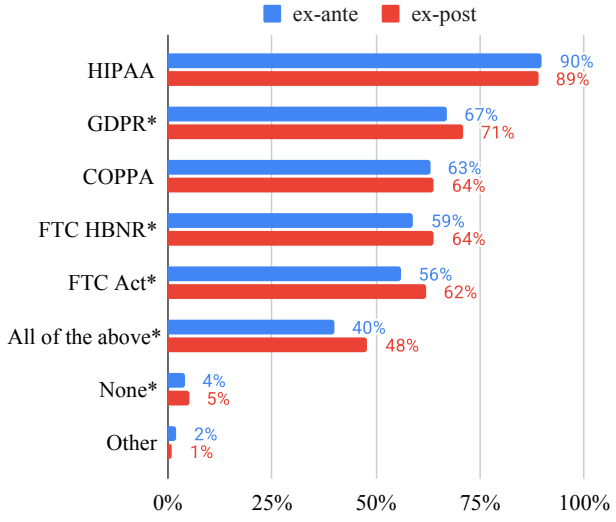

Figure 7: Expectations about privacy regulations with which recipients are required to comply. Asterisks indicate significant differences between ex-ante and ex-post expectations

D Regression Analysis (Survey 1)

Table 9: Factors affecting the Perceived Privacy protection level.

	Predictors	Dependent variable: Perceived Privacy					
		Ex-ante			Ex-post		
		β	OR	p	β	OR	p
Main effects	**App type (base: Provider apps)**						
	Independent apps	-0.2919	0.7469	**0.0317**	-0.2850	0.7520	**0.0340**
	Confidence	0.5248	1.6901	**<0.0001**	0.5832	1.7917	**<0.0001**
	Likelihood of use	0.3203	1.3775	**<0.0001**	0.7249	2.0645	**<0.0001**
	Reading extent	0.4548	1.5758	**0.0001**	0.0344	1.0350	0.7768
Privacy beliefs	**IUIPC (Control)**	0.0440	1.0450	0.7315	0.1068	1.1127	0.4149
	IUIPC (Awareness)	0.5033	1.6542	**0.0036**	0.1860	1.2044	0.2899
	IUIPC (Collection)	-0.5504	0.5767	**<0.0001**	-0.5784	0.5608	**<0.0001**
	Prior privacy violation (base: No)						
	Yes	-0.2340	0.7914	0.1019	-0.2472	0.7810	0.0803
	Prior medical privacy violation (base: No)						
	Yes	-0.1034	0.9018	0.6486	-0.2909	0.7476	0.1893
Demographics	**Age**	0.0093	1.0094	0.1095	-0.0026	0.9974	0.6515
	Gender (base: Male)						
	Female	0.1314	1.1404	0.3482	0.3287	1.3892	**0.0187**
	Non-binary	0.6453	1.9065	0.2228	0.1570	1.1700	0.7498
	Education	-0.0456	0.9554	0.4686	-0.0375	0.9632	0.5455
	Ethnicity (base: White)						
	Asian	-0.3516	0.7035	0.2227	-0.1036	0.9016	0.7136
	Black	0.0442	1.0452	0.8217	-0.5049	0.6035	**0.0114**
	Mixed	-0.1995	0.8192	0.4402	-0.2686	0.7645	0.2727
Background	**Experience in a technical field (base: No)**						
	Yes	-0.3400	0.7118	**0.0382**	-0.1013	0.9037	0.5318
	Smartphone experience	0.0907	1.0950	0.5022	0.0316	1.0321	0.8094
	Frequency of telehealth use (on desktop)	-0.1037	0.9015	0.1432	-0.0376	0.9631	0.5969
	Frequency of telehealth use (on smartphone/tablet)	0.0561	1.0577	0.4318	0.0249	1.0252	0.7258

End of table

Table 10: Factors affecting Confidence in understanding the app's data practices.

	Predictors	Dependent variable: Confidence					
		Ex-ante			Ex-post		
		β	OR	p	β	OR	p
Main effects	**App type (base: Provider apps)**						
	Independent apps	0.2021	1.2240	0.1276	-0.1232	0.8841	0.3582
	Likelihood of use	0.2797	1.3227	**<0.0001**	0.1476	1.1590	**0.0150**
	Perceived Privacy	0.5908	1.8053	**<0.0001**	0.4766	1.6106	**<0.0001**
	Reading extent	-0.2180	0.8042	0.0572	0.5528	1.7382	**<0.0001**
Privacy beliefs	**IUIPC (Control)**	-0.0487	0.9525	0.6911	0.0552	1.0567	0.6629
	IUIPC (Awareness)	0.3512	1.4207	**0.0318**	0.6739	1.9620	**0.0001**
	IUIPC (Collection)	-0.2529	0.7765	**0.0118**	-0.1487	0.8618	0.1475
	Prior privacy violation (base: No)						
	Yes	-0.6224	0.5367	**<0.0001**	-0.3134	0.7310	**0.0260**
	Prior medical privacy violation (base: No)						
	Yes	0.0226	1.0229	0.9182	0.2325	1.2617	0.2904
Demographics	**Age**	0.0030	1.0030	0.5833	-0.0076	0.9924	0.1862
	Gender (base: Male)						
	Female	-0.1068	0.8987	0.4294	-0.1392	0.8701	0.3131
	Non-binary	-0.6474	0.5234	0.2188	-0.5696	0.5657	0.2588
	Education	0.0158	1.0160	0.7934	0.0183	1.0184	0.7644
	Ethnicity (base: White)						
	Asian	-0.2315	0.7933	0.4223	-0.0982	0.9065	0.7275
	Black	0.0805	1.0838	0.6657	0.5912	1.8062	**0.0029**
	Mixed	-0.2688	0.7643	0.2904	0.1670	1.1818	0.4956
Background	**Experience in a technical field (base: No)**						
	Yes	0.1057	1.1115	0.5067	0.0764	1.0794	0.6402
	Smartphone experience	0.1235	1.1315	0.3294	0.1346	1.1440	0.3061
	Frequency of telehealth use (on desktop)	0.0760	1.0790	0.2760	-0.0367	0.9640	0.5965
	Frequency of telehealth use (on smartphone/tablet)	0.2098	1.2335	**0.0029**	0.2485	1.2821	**0.0004**

End of table

Table 11: Factors affecting the Likelihood of downloading and using the app.

	Predictors	Dependent variable: Likelihood of use					
		Ex-ante			Ex-post		
		β	OR	p	β	OR	p
Main effects	**App type (base: Provider apps)**						
	Independent apps	-0.6887	0.5022	**<0.0001**	-0.2791	0.7565	**0.0465**
	Confidence	0.3118	1.3659	**<0.0001**	0.2221	1.2487	**0.0054**
	Perceived Privacy	0.5269	1.6936	**<0.0001**	0.8427	2.3226	**<0.0001**
	Reading extent	0.2092	1.2327	0.0805	0.0975	1.1024	0.4455
Privacy beliefs	**IUIPC (Control)**	-0.4325	0.6489	**0.0012**	-0.3515	0.7036	**0.0082**
	IUIPC (Awareness)	0.4546	1.5756	**0.0092**	0.2714	1.3118	0.1248
	IUIPC (Collection)	-0.0831	0.9203	0.4331	-0.1278	0.8800	0.2232
	Prior privacy violation (base: No)						
	Yes	-0.1833	0.8325	0.2048	-0.2949	0.7446	**0.0424**
	Prior medical privacy violation (base: No)						
	Yes	-0.2244	0.7990	0.3316	0.1125	1.1190	0.6288
Demographics	**Age**	0.0031	1.0031	0.6043	0.0100	1.0101	0.1041
	Gender (base: Male)						
	Female	0.0194	1.0196	0.8917	-0.1264	0.8813	0.3835
	Non-binary	0.5220	1.6853	0.3405	0.5270	1.6938	0.3059
	Education	-0.1254	0.8821	0.0508	-0.0966	0.9079	0.1290
	Ethnicity (base: White)						
	Asian	0.0548	1.0564	0.8448	-0.1540	0.8573	0.5868
	Black	0.0806	1.0839	0.6969	0.0486	1.0498	0.8127
	Mixed	-0.1722	0.8418	0.5269	-0.0649	0.9372	0.8090
Background	**Experience in a technical field (base: No)**						
	Yes	0.1157	1.1226	0.4911	-0.1985	0.8200	0.2385
	Smartphone experience	0.3153	1.3707	**0.0231**	0.3452	1.4123	**0.0118**
	Frequency of telehealth use (on desktop)	0.1035	1.1091	0.1556	0.0992	1.1043	0.1848
	Frequency of telehealth use (on smartphone/tablet)	0.2606	1.2977	**0.0003**	0.2787	1.3214	**0.0002**
	Insurance plan (base: No insurance)						
	PPO-type plan	-0.5470	0.5787	**0.0204**	-0.3168	0.7284	0.1863
	HMO-type plan	-0.5472	0.5786	**0.0242**	-0.3581	0.6990	0.1479

End of table

E Survey 1

[The full survey instrument, including questions that were not relevant for the analysis, can be found in supplementary materials at https://bit.ly/3CGK02q.]

Welcome to the survey about mobile health apps (also often called telehealth apps) that help people connect with doctors. In this survey we will show you information about different mobile telehealth apps and ask your opinions about them. Some of those questions will be about your expectations; there are no right or wrong answers; we really just want to learn about your opinions. Although some of the information or scenarios in the survey will be hypothetical, please try to answer as closely as you can to what your response in real life would have been.

[consent form]

[health app experience] A telehealth platform is a mobile app, website, or web app that helps you find, make and attend virtual or in-person appointments with physical or mental health care providers. On average, how often do you use such telehealth platforms, for making appointments or for other services? *[In random order:]*

- Accessing telehealth platforms from a desktop computer/laptop
- Using telehealth apps on a smartphone or tablet/iPad

[Grid of response options] 1 - Never, 2 - Less than once a year, 3 - Once or several times a year, 4 - Once or several times a month, 5 - Once or several times a week, 6 - Once or several times a day

[telehealth apps] What telehealth platforms have you used in the past?

[telehealth provider] *[If 'Never' is not selected]* How did you find the last telehealth app you used? 1 - I found it myself, 2 - My friend recommended it, 3 - My insurance company or HMO recommended it, 4 - A healthcare provider/clinic/doctor (not an HMO) recommended it, 5 - I don't remember, 6 - Other (please specify)

[Participants are randomly assigned to either Independent or Provider condition]

Stage 1: App Description

[For Independent condition] Imagine that you are not feeling well and you decide to seek medical help. You don't have a regular healthcare provider, so you search for a service to help you find and book an appointment with a doctor. You find the app shown below. This app is provided by an independent developer, not associated with any particular insurance, healthcare system, or medical provider.

[For Provider condition] Imagine that you are not feeling well and you decide to seek medical help. Your healthcare provider says that you can find and book an appointment with a doctor using their app shown below.

Please read the app description below carefully, because the rest of the survey will be about it. Then answer the questions about this app. (You won't be able to advance to the next page before reading the information below, so please take your time to read it.)

[Screenshot of the app description.]

[Record time that participants spent on the app description screen. Set a timer that delays showing the 'Next' button by 90 seconds, to encourage reading the full app description.]

[self-reported reading of the app description] How much of the information on the previous screen did you read? (Please answer honestly; your answer won't affect your compensation for the survey). 1 - I did not read any of it, 2 - I read only titles/headlines, 3 - I skimmed it, 4 - I read most of it, 5 - I read all of it

[prior usage of the app] Have you used this app before? 1 - No, 2 - Yes, 3 - I don't remember

[attention check question 1] When you answer this question, could you please select never as a response option? 1 - Never, 2 - Rarely, 4 - Sometimes, 5 - Often, 6 - Always

Initial evaluation

[likelihood to download the app] *[If selected Yes for prior usage]* How likely are you to use this app? (*[If answered No or I don't remember for prior usage]* How likely are you to download and use this app?) 1 - Very unlikely, 2 - Somewhat unlikely, 3 - Neutral, 4 - Somewhat likely, 5 - Very likely

[reason for not willing to use] *[If Somewhat or Very Unlikely is selected]* Why are you not likely to [piped: use/download and use] this app?

[privacy perception] How well do you think this app protects user privacy? 1 - Very poorly, 2 - Somewhat poorly, 3 - Neither poorly, nor well, 4 - Somewhat well, 5 - Very well

[desired changes in privacy] *[If Somewhat well or Very well are NOT selected]* What would need to change in the [app description *(in Stage 1)* /additional information about the app *(in Stage 2)*] for you to think that the app protects user privacy well?

[expectations of data collection] In general, what information do you expect this app to collect about users? Choose ALL that apply. *[In random order]* 1 - Financial information (credit card details, bank credentials, etc.), 2 - Medical and health information (current and past health conditions, symptoms, diagnoses, lab results; prescriptions and medications; health monitoring data, such as heart rate, step count, activity level; doctors' session details and notes; physician name and specialty; medical record number), 3 - Contact information (name, email, phone number, mailing address), 4 - Location (exact location, neighborhood, city), 5 - Demographics (age, date of birth, gender, ethnicity, education, occupation, etc.), 6 - Personal identifiers (driver license, SSN, passport, etc.), 7 - Device information (device manufacturer, device model, screen size, operating system, web browser, etc.), 8 - Device identifiers (IP address, serial number or IMEI/MEID, advertising ID, etc.), 9 - User activities and interactions (including buttons and links the user clicked, anything the user searched in the app, pages visited, time spent on pages, etc.), 10 - Signup credentials (username, password, account number), 11 - Insurance information, 12 - Video recording of a

session/appointment, 13 - Audio recording of a session/appointment, 14 - Physical attributes (height, weight, etc.), 15 - Information about children, 16 - Other (please specify), 17 - All of the above *[exclusive answer, not randomized]*, 18 - No data will be collected *[exclusive answer, not randomized]*

[If selected 'No data', skip the questions about Recipients, Purposes, and Storage. Otherwise, ask the questions below.]

[expectations of data sharing/access] In general, who do you think will have access to the collected information? Choose ALL that apply. *[In random order]* 1 - No one, other than the user themself *[exclusive answer, not randomized]*, 2 - Doctors or care provider employees, 3 - Pharmacies that provide medications to the user, 4 - Parent company of the care provider, 5 - Insurance companies, 6 - Employees of the company that developed the app, 7 - Parent company of the app developer, 8 - Government entities, 9 - Pharmaceutical companies that do research and make medications, 10 - Third-party advertisers and trackers, 11 - Third-party analytics companies (that analyze app performance), 12 - Third-parties outside of the US, 13 - Payment processing services (credit card companies, etc.), 14 - Informal caregivers (e.g. friends, family), 15 - Other users of the app, 16 - The general public, 17 - Other (please specify) *[not randomized option]*

[expectations of data use] In general, for what purposes do you expect the recipients you selected in the previous question to use the collected information? Choose ALL that apply. *[In random order]* 1 - For providing medical treatment (and other primary services related to healthcare, e.g. scheduling and reminding about appointments, etc.), 2 - For payment purposes, 3 - For marketing and advertising, 4 - For analytics, to support technical functionality of the app, understand how users interact with the app (what users click, search, etc.), or to improve the app, 5 - To comply with legal obligations (e.g. regulations, government data requests, fulfill a law enforcement request or court order), 6 - For executing a merger/acquisition with another company, 7 - For security protection (e.g. fraud detection and prevention, protecting users' data, etc.), 8 - For communication purposes (e.g. to contact users to resolve issues, respond to user queries, etc.), 9 - To sell to or share it with other companies, 9 - Other (please specify) *[not randomized option]*

[expectations of data storage] In general, how long do you expect this app to store the data it collects? 1 - The data won't be stored at any point, 2 - Delete data immediately after the goal of use is achieved (e.g. after meeting with the doctor) or legal obligations are met, 3 - Delete after a certain period of time (for example, 3 months, 1 year, etc.), 4 - Keep until user requests deletion of the data, 5 - Keep indefinitely, 6 - Other (please specify)

[ease of understanding] Based on the [app description *(in Stage 1)* / additional information about the app that *(in Stage 2)*] you read, how confident are you that you understand the app's data practices (what information the app collects, how it uses it, who has access to it, how long it is stored)? 1 - Very low confidence, 2 - Medium-low confidence, 3 - Medium confidence, 4 - Medium-high confidence, 5 - Very high confidence

[reason for low confidence in understanding - app description] *[If Very or Medium-Low Confidence is selected]* Please explain why you do not feel confident you understand the app's data practices, based on the [app description *(in Stage 1)* / additional information about the app that *(in Stage 2)*] you read. Choose ALL that apply. **[In random order]** 1 - I didn't find any information about data practices, 2 - Too much terminology/jargon, 3 - Unclear/vague wording, 4 - Description was too long to read in detail or absorb, 5 - Information about data practices was incomplete, 6 - Other (please specify)

[expectations of recipients' compliance] Now think of the recipients that you assumed earlier would have access to your information collected by the app. Do you think these recipients are required by law to comply with any of the following privacy regulations? Choose ALL that apply. *[In random order]* 1 - General Data Protection Regulation (GDPR), 2 - Health Insurance Portability and Accountability Act (HIPAA), 3 - FTC's Health Breach Notification Rule, 4 - Children's Online Privacy Protection Act (COPPA), 5 - Federal Trade Commission Act (FTC Act), 6 - Other (please specify) *[not randomized]*, 7 - All of those regulations *[exclusive answer, not randomized]*, 8 - None of those regulations *[exclusive answer, not randomized]*

Stage 2: Data Safety section

Now, imagine that you noticed additional information about this app. Please read this information below carefully. Then answer the questions about it. (You won't be able to advance to the next page before reading the information below, so please take your time to read it.)

[Screenshot of the Data Safety section.]

[Record time that participants spent on the screen. Set a timer that delays showing the 'Next' button by 90 seconds.]

[self-reported reading of the data safety sections] How much of the information on the previous screen did you read? (Please answer honestly; your answer won't affect your compensation for the survey). 1 - I did not read any of it, 2 - I read only titles/headlines, 3 - I skimmed it, 4 - I read most of it, 5 - I read all of it

Now that you have had a chance to read additional information, we will ask your opinions about the app again. Although some of your opinions may have changed, we don't necessarily expect that to happen, so please don't feel like they need to be different.

Final evaluation *[Repeat the Initial Evaluation questions but with the wording for Stage 2]*

[self-reported change in the likelihood to download the app] How likely are you to [download / download and use] this app now, after reading more information about it? *[In random order]* 1 - More likely than before, 2 - Less likely than before, 3 - Same as before

[reasons for changed willingness to download] *[If final likelihood to download is different from the initial]* What influenced your willingness to download or use the app? Choose ALL that apply. *[In random order]* 1 - I better understood the app's functionalities, 2 - I better understood the app's data practices, 3 - I better understood the app's data protection level, 4 - I better understood the app's quality, 5 - Other (please explain)

[final privacy perception] How well do you think this app protects user privacy now, after learning more about the app? *[In random order]* 1 - Better than I thought before, 2 - Worse than I thought before, 3 - Same as I thought before

[reasons for changed privacy perceptions] *[If final privacy perception is different from the initial]* What influenced your perception of how well the app protects user privacy?

Exit survey

[attention check question 2] After reading the description of this question, could you please choose sometimes as your answer? 1 - Never, 2 - Rarely, 3 - Sometimes, 4 - Often, 5 - Always

Now let's talk about telehealth apps **in general** (not about the specific apps we just asked you about).

[privacy perceptions of insurance-provided vs independent apps] Which type of telehealth app do you think is more likely to do a better job of protecting users' privacy? 1- An app provided by an insurance company or healthcare system/provider is more likely to protect privacy better, 2 - An app from an independent developer/service (not associated with any insurance company or healthcare system/provider) is more likely to protect privacy better, 3 - Both are equally likely to protect privacy to about the same degree

[insurance] Do you have medical insurance? 1 - I have a PPO, POS, or a similar plan (you choose from a wide variety of doctors), 2 - I have an HMO plan (you choose among doctors that are part of a specific healthcare system), 3 - Other insurance plan (please specify), 4 - I don't have any insurance, 5 - I don't know

[requirement for HIPAA compliance] In general, are there any circumstances where you think data collected by telehealth apps is NOT protected by the Health Insurance Portability and Accountability Act (HIPAA)? 1 - Definitely no, 2 - Likely no, 3 - I don't know, 4 - Likely yes, 5 - Definitely yes

[circumstances for no HIPAA protection] *[If Likely or Definitely yes]* In your opinion, under what circumstances will the data collected by telehealth apps NOT be protected by HIPAA?

[mobile OS] What is the operating system on your personal smartphone? 1 - Android, 2 - iOS (on iPhone), 3 - Other (please specify), 4 - I don't know

[tech experience] Do you have education or work experience in any of the information technology fields (such as Computer Science, Software Engineering, App Development, etc.)? 1 - Yes, 2 - No

[smartphone experience] What best describes your level of technical experience with smartphones? 1 (Novice user) – I rarely use my smartphone for anything other than calling and texting, 2 (Regular user) – I occasionally use a few different apps on my smartphone, 3 (Power user) – I often use a lot of different apps on my smartphone, 4 (Expert user) – I understand the technical details of how my smartphone works and can create apps myself

[privacy attitudes] *[IUIPC validated scale[64]. In random order.]*

[experience with prior privacy/security violations] Have you ever experienced an information privacy or security violation/incident? 1 - No, 2 - Yes

[timing of violation] *[If Yes is selected]* When did you experience an information privacy or security violation/incident? 1 - Less than a month ago, 2 - 1-6 months ago 3 - 6-12 months ago, 4 - More than a year ago

[description of violation] *[If Yes is selected]* Please briefly describe the privacy or security violation/incident you experienced.

[experience with prior privacy violations in medical privacy space] Have you ever experienced a medical information privacy or security violation/incident? 1 - No, 2 - Yes

[timing of medical violation] *[If Yes is selected]* When did you experience a medical information privacy or security violation/incident? 1 - Less than a month ago, 2 - 1-6 months ago, 3 - 6-12 months ago, 4 - More than a year ago

[description of medical violation] Please briefly describe the medical privacy or security violation/incident you experienced.

[comments (optional)] Do you have any comments about the study?

[goodbye screen]

F Survey 2

[The full survey instrument, including questions that were not relevant for the analysis, can be found in supplementary materials at https://bit.ly/42LcW3J.]

Welcome to the survey about mobile health apps (also often called telehealth apps) that help people connect with doctors. In this survey we will show you information about different mobile telehealth apps and ask your opinions about them. Some of those questions will be about your expectations; there are no right or wrong answers; we really just want to learn about your opinions.

Although some of the information or scenarios in the survey will be hypothetical, please try to answer as closely as you can to what your response in real life would have been.

[consent form]

[health app experience] A telehealth platform is a mobile app, website, or web app that helps you find, make and attend virtual or in-person appointments with physical or mental health care providers. On average, how often do you use such telehealth platforms, for making appointments or for other services? *[In random order:]*

- Accessing telehealth platforms from a desktop computer/laptop
- Using telehealth apps on a smartphone or tablet/iPad

[Grid of response options] 1 - Never, 2 - Less than once a year, 3 - Once or several times a year, 4 - Once or several times a month, 5 - Once or several times a week, 6 - Once or several times a day

[telehealth apps] What telehealth platforms have you used in the past?

[attention check question 1] When you answer this question, could you please select never as a response option? 1 - Never, 2 - Rarely, 4 - Sometimes, 5 - Often, 6 - Always

[privacy policy update communication] In general, do you expect telehealth apps to communicate to users about updates to their privacy policies in the future? 1 - No, I expect to check for updates myself, 2 - Yes, I expect the app to communicate the changes but not to require me to consent to the changes, 3 - Yes, I expect the app to communicate the changes and to require me to consent to the changes, 4 - Other (please provide details)

Next, we will ask you some questions about what privacy regulations currently say about telehealth apps. It is ok if you are not sure about your answers, we just want to know about your expectations.

For the purpose of the questions on this page, let us clarify that we define personally-identifiable health information as health or medical information that is stored alongside the information that can identify you.

[current regulatory protection] According to your understanding of health privacy regulations, if a telehealth app wants to share your personally-identifiable health information with another entity/organization for the following purposes, what is the app required to do?

[Grid, with Action (as columns):] 1 - Obtain additional explicit permission from you before sharing, 2 - Require that entity/organization to agree they will ONLY use the data for this purpose, 3 - Both obtain additional explicit permission from you and require that entity/organization to agree they will ONLY use the data for this purpose, 4 - They are not allowed to share with any other entity/organization at all, 5 - They are not required to do anything when they share

[Purposes (as rows) in randomized order, as in Survey 1]

[attention check question 2] After reading the description of this question, could you please choose sometimes as your answer? 1 - Never, 2 - Rarely, 3 - Sometimes, 4 - Often, 5 -Always

Now, instead of focusing on the current regulation, we will ask you some questions about what privacy regulations should be protecting (regardless of whether you think they already do that or not). It is ok if you are not sure about your answers, we just want to know your opinions.

[desired restrictions] How would you prefer privacy regulations to restrict the sharing of data collected by telehealth apps? Choose ALL that apply. 1 - Require the app to obtain additional explicit user permission before sharing, 2 - Require the receiving entity/organization third party to agree they will ONLY use the data for specified purposes, 3 - Prevent the telehealth apps from sharing the data *[exclusive answer]*, 4 - Other (your answer), 5 - They should not be required to do anything when they share *[exclusive answer]*