Privacy, Permissions, and the Health App Ecosystem: A Stack Overflow Exploration

Mohammad Tahaei
mohammad.tahaei@bristol.ac.uk
Department of Computer Science
University of Bristol
United Kingdom

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

Awais Rashid
awais.rashid@bristol.ac.uk
Department of Computer Science
University of Bristol
United Kingdom

ABSTRACT

Health data is considered to be sensitive and personal; both governments and software platforms have enacted specific measures to protect it. Consumer apps that collect health data are becoming more popular, but raise new privacy concerns as they collect unnecessary data, share it with third parties, and track users. However, developers of these apps are not necessarily knowingly endangering users' privacy; some may simply face challenges working with health features.

To scope these challenges, we qualitatively analyzed 269 privacy-related posts on Stack Overflow by developers of health apps for Android- and iOS-based systems. We found that health-specific access control structures (e.g., enhanced requirements for permissions and authentication) underlie several privacy-related challenges developers face. The specific nature of problems often differed between the platforms, for example additional verification steps for Android developers, or confusing feedback about incorrectly formulated permission scopes for iOS. Developers also face problems introduced by third-party libraries. Official documentation plays a key part in understanding privacy requirements, but in some cases, may itself cause confusion.

We discuss implications of our findings and propose ways to improve developers' experience of working with health-related features—and consequently to improve the privacy of their apps' end users.

CCS CONCEPTS

• **Security and privacy → Software and application security**; **Human and societal aspects of security and privacy**; **Usability in security and privacy**; • **Human-centered computing → Human computer interaction (HCI)**; **HCI design and evaluation methods**; • **Software and its engineering**;

KEYWORDS

software developers, health apps, usable privacy, developer forums

EuroUSEC 2022, September 29–30, 2022, Karlsruhe, Germany

ACM ISBN 978-1-4503-9700-1/22/09…$15.00
https://doi.org/10.1145/3549015.3555669

ACM Reference Format:
Mohammad Tahaei, Julia Bernd, and Awais Rashid. 2022. Privacy, Permissions, and the Health App Ecosystem: A Stack Overflow Exploration. In *2022 European Symposium on Usable Security (EuroUSEC 2022), September 29–30, 2022, Karlsruhe, Germany*. ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3549015.3555669

1 INTRODUCTION

Mobile apps, fitness trackers, and sensors provide many users with insights into their health, and motivation to improve it. The data collected by these services is often considered sensitive, and many countries have specific regulations and limitations for working with it [e.g., 40, 75, 76]. However, health apps[1] still share data with third parties, track users, ask for unnecessary permissions, and use insecure modes for transferring data [e.g., 37, 60, 63, 74].

In general, app developers face a number of challenges with privacy features, including managing access control, writing privacy policies, understanding documentation for libraries, translating legal privacy requirements into technical requirements, and finding time to prioritize privacy in the first place [16, 19, 45, 58, 65, 69, 73, 77, 82]. While literature has explored some of these general issues from app developers' perspectives, developers who work with health data face additional complications, due to the potential for heightened user privacy concerns and to special regulations. It is not yet known how these additional complications affect health app developers' management of privacy challenges.

We therefore conducted an exploratory qualitative analysis of 269 privacy-related posts made by health app developers on Stack Overflow, a popular public forum for programming questions. Our research questions (RQs) were:

RQ1: What privacy-related challenges do app developers face when integrating health-related features?

RQ2: How do the challenges differ when developing health apps for different platforms?

RQ3: How do health app developers navigate those privacy challenges?

In addressing these questions, we contribute to research on supporting developers in performing privacy tasks—and thus improving privacy protection for the end users of those apps.

Our findings identify the major privacy challenges and confusions for Android and iOS health app developers, especially in dealing with health-specific requirements regarding access control and permissions; meeting enhanced requirements set by app stores and health frameworks (i.e., software libraries that provide

[1]Throughout, we use the term "health apps" fairly broadly, to refer to any apps with medical, health, and/or fitness purposes.

access to health sensors and data on mobile devices); and addressing unexpected permissions problems introduced by third-party components.

We observe that those platform requirements drive most privacy efforts—and at the same time are a source of many privacy confusions. The discussion compares those findings with prior work. In addition, we make recommendations about improving documentation to guide compliance with specialized platform requirements regarding health data, and about tools and information to help health app developers identify privacy implications of third-party components.

2 BACKGROUND: HEALTH FRAMEWORKS AND PERMISSIONS RULES FOR APPLE AND GOOGLE APPS

This section provides an overview of how health data is handled in the two major mobile operating systems.

Both Android (Google) and iOS (Apple) devices support app features that use health data such as heart rate, blood pressure, and step counts. This health data may be collected from sensors on the smartphone itself, or from separate devices, including wearable devices from the same companies or manufactured by third parties. Android and iOS each have parallel pared-down Operating Systems (OSes) for their own wearable devices, WearOS and WatchOS [8, 28], respectively, as do some other companies that make wearables. The wearable OSes can run their own apps, and users can also interact with them through companion apps on smartphones.

Each company has a proprietary framework for collecting, storing, and working with health-related sensor data. While Apple's HealthKit mainly works with on-device data stores, Google Fit's data stores are cloud-based, accessed via different APIs depending on OS and app type. In both frameworks, developers have to define a description for the permissions they want to use in their apps, including the purpose for accessing any health-related resources.

Android has two permissions for health data, restricted (for reading data) and sensitive (for writing data). They both require developers to pass a verification process; however, accessing restricted resources requires extra steps, including a security assessment by a third party [29, 31].

Apple has a generic review process for all apps [9] that checks for any violations of app development guidelines. These guidelines include specific requirements for health data, but, based on the documentation, there does not seem to be a separate developer verification step for health apps.

3 RELATED WORK

3.1 Privacy in Health Apps

Health apps vary from simple fitness apps that count the steps someone takes in a day to services that work with more sensitive information about physical and mental health, such as trackers for symptoms or medications [3, 26, 38, 47].

The number of mobile health apps has grown steadily in the past decade, increasing more sharply since the COVID-19 pandemic began [22, 44, 60, 63]. The prevalence of health apps creates a space for collecting data and tracking users [e.g. 48, 53, 54, 60, 74, 79]. These app behaviors may not be disclosed in privacy policies [39, 74], and some health apps do not have privacy policies at all [48, 54]. Such behaviors are even found in apps built by governments [37, 60]. Such data-collection overreach occurs despite specific regulations to protect health data, such as the Health Insurance Portability and Accountability Act (HIPAA) [76] in the U.S. or extra precautions in the General Data Protection Regulation (GDPR) [75] and the UK Data Protection Act [40].

Users' opinions about health app privacy are mixed [e.g., 35, 52, 55, 78, 85], and awareness of specific privacy practices and policies is low [81]. Some may assume the app would not give away their data without their knowledge [46, 81]. Others may have concerns about sharing their health data with apps, or about which third parties the app might share it with [e.g., 34, 50, 81, 85].

Yet despite these concerns, many studies show a lack of privacy safeguards in health apps [e.g., 20, 63, 74, 83]. Our study aims to improve the health app privacy ecosystem by examining how developers of these apps consider privacy, and how they can be better supported in integrating privacy features, which could consequently improve users' privacy.

3.2 Empirical Privacy Studies With Developers

There has been an increase in the number of privacy-related posts on Stack Overflow (from 10 to 234 posts between 2008 and 2018 [73]), suggesting that privacy is increasingly being discussed in developer communities.

One recurring challenge is translating privacy requirements, which can be filled with legal jargon, into technical requirements [e.g., 19, 33, 61, 64, 69]. Developers' understanding of privacy might be impacted by several other factors, such as their workplace and the software development platforms [e.g., 4, 12, 32, 70]. For example, developers in an interview study often used the language of security, prominent in their workplaces, to explain privacy topics, or discussed privacy indirectly via references to privacy policies [33].

Studies of the iPhoneDevSDK and XDA forums [62] and the /r/androiddev subReddit [45] noted an emphasis on informing users by showing permissions dialogues—which are mobile OSes' primary point of access control for private data resources. Because of these structures, app stores and mobile operating systems like Apple and Google are key drivers of privacy in developer communities [7, 32, 62, 70]; this is discussed further in §6.1.

Regarding health apps specifically, research has explored developers' security challenges, including lack of knowledge about security requirements, not having the guidelines, and not engaging experts in the design process [5, 6]. While prior work studies general *privacy* challenges for developers [e.g., 16, 45, 61, 73, 77, 82] and *security* challenges for health apps [e.g., 5, 6, 51, 74], there has been no analysis that covers developers' privacy challenges working with sensitive health data. We leverage the methods and findings from these prior bodies of research to fill that gap.

3.3 Studying Developers Using Online Forums

Online forums, such as Stack Overflow, Reddit, and GitHub, have become a widely used resource for empirical studies of developers [23, 32, 36, 45, 62, 70, 73, 80, 84]. Such forums provide a rich source of data about about developers—who are often challenging

to recruit for empirical studies [24, 41, 72]—via artefacts such as sample code and written posts.

Studying Stack Overflow, for example, has provided insights into the privacy and security challenges of developers [23, 73, 84]. Researchers have also identified ways it can be a potential vector for security vulnerabilities, for example a lab study showing that code written using Stack Overflow as a resource is less secure than using official documentation or programming books [1, 2], or a study tracing insecure code in live Android apps to code snippets in Stack Overflow posts [25]. Such studies show the impact of this forum on privacy and security of developers' code and the app ecosystem.

Our study extends this literature to pinpoint developers' privacy challenges in working with health-related features—and meanwhile highlights the impact of research framing and choice of keywords on final datasets, and therefore on different studies' results.

4 METHOD

We created a dataset and qualitatively analyzed 269 health and privacy-related Stack Overflow posts to answer our research questions.

4.1 Study Ethics

We received ethics approval and oversight from our institute's ethics committee. The study is in line with Stack Overflow's terms of service and privacy policy. Contributed content is available under a Creative Commons license and Stack Overflow encourages academics to use its data for research [14, 15]. For attribution, we provide hyperlinks attached to post identifiers [13]. Because the dataset contains usernames, we are not able to share it directly with the community (per our institute's ethics guidelines); however, the queries used to collect it are included in Appendix A.

4.2 Dataset

Collection of initial dataset. We collected data in October 2021, using the Stack Exchange API [66] to query posts from the five-year period from 2016/July/01 to 2021/July/01. To find posts about health apps for Android and iOS, we queried for posts whose title or tags included a combination of {fitness, google fit, health, medical} with {android, ios, watchos, wearos}.[2] We focused on Android and iOS because they are by far the most widely used mobile OSes [67].

In total, we collected 1,055 unique posts, of which a slight majority were about iOS and WatchOS. This tilt seems unique to health apps; overall, the ratio of posts with *Android* or *WearOS* in the title or tags to posts with *iOS* or *WatchOS* was about 2:1 over the same time period (more in keeping with Android's larger market share [21]).

Selection of final dataset. From our initial set of 1,055 posts, we selected a final dataset of 269 posts mentioning privacy-related topics, including privacy, access permissions, authentication, and data security (example in Figure 1).

[2]We used *google fit* to make sure we collected posts referring to the Google Fit health-data framework that might not use our other terms in the title or tag, as results from *fit* alone were dominated by other meanings of the word. Posts that specifically referred to the HealthKit and Samsung Health frameworks were caught by the search term *health*, as we used the `LIKE` operator to retrieve substring matches.

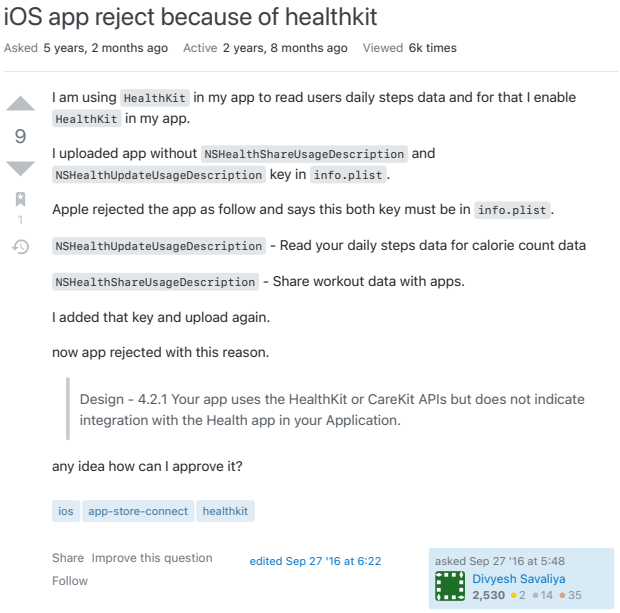

Figure 1: A sample question about permissions-related problems in an iOS health app [stackoverflow.com/questions/39716868]. The post asks about required descriptions in iOS for requesting access to a resource.

We chose to narrow down the dataset by hand, rather than by using query terms such as *privacy*, because our preliminary investigations found that posts about our target topics often did not use such terms in the titles nor tags. In addition, as we noted in §3.2, previous research has shown that the topic of privacy may come up indirectly; our inclusion criteria were based on those studies. We excluded posts about health apps for Android and iOS that were not about our target topics, as well as a handful that were caught by our query terms but were not about health apps or were not about our target OSes.

Selection was performed by the first two authors independently coding the same 5% of the data for inclusion or exclusion; interrater agreement for that initial test batch was 81%. They then split the data and each coded half of the rest, flagging any "maybes" to resolve through discussion. Posts were included if the target topics were mentioned in any part (i.e., question, answers, or comments). However, we excluded cases where the posters only mentioned the topic in passing, for example, in listing potential code errors they had already checked for.

Posts often referred to Android and WearOS together, or iOS with WatchOS. Grouping each family of OSes together, there were 496 unique posts about Android and WearOS and 569 unique posts about iOS and WatchOS (going by titles and tags) in the initial dataset. Of these, 26% and 24.6% were privacy-related, respectively, and thus were included in the final dataset. (See Table 3 in Appendix B for a breakdown by query term.)

4.3 Qualitative Analysis

The first two authors qualitatively coded the 269 privacy-related posts. Again, all parts of the posts were included (question, answers,

and comments). First, they independently analyzed an initial batch of 36 posts, using an inductive approach with open codes [49, 59], discussed their findings, and identified the major topics or theme groups. They then independently coded another batch of 36 posts, discussed, and built an initial codebook. The two coders continued coding all posts, jointly resolving disagreements, and adjusting the codebook based on the additional posts as well as input from the third author. Kupper-Hafner interrater agreement [43] for thematic coding across all posts was 60% (codes were not mutually exclusive, and posts could have multiple codes). At the same time, one of the coders also recorded which OS and health-data framework each poster was developing for.

5 FINDINGS

A quarter of all the posts we collected related to mobile health apps were about privacy (25.5%), indicating that privacy is a major source of difficulty in working with health features. As we noted in §4.2, the proportions of privacy-related posts relating to each of our target OSes (relative to the initial datasets for those OSes) were similar; neither OS seems to be presenting disproportionately more challenges as regards health and privacy features. However, as we will describe in detail below, the specific questions for each OS tended to be different.

5.1 Description of the Final Dataset

Table 1 shows the numbers and proportions of questions in the final dataset from posters developing for each of the target OSes and health frameworks.[3] In addition to smartphone apps, 51 posts out of 269 (19%) related at least in part to apps for specialized OSes for wearable sensor devices. For the most part, posters developing for iOS or WatchOS were using Apple's integrated HealthKit framework (including WatchKit) and posters developing for Android or WearOS were using Google Fit, but there were some exceptions that crossed platform lines. A few developers of Android and iOS apps were working with health data from other systems.

Privacy vs. access control. The vast majority of posts in our final dataset were about dealing with access control issues (e.g., permissions or authentication systems), rather than explicitly framed in terms of privacy concepts. Stack Overflow users **explicitly mentioned data privacy or sensitivity** in 8.6% of the posts in the final dataset (amounting to 2.2% out of all 1,055 health-related posts in the initial dataset):

> [A][4] Google Fit restricts write access for the data types in HealthDataTypes to only certain developers because health data is potentially sensitive. [stackoverflow.com/questions/44523685]

5.2 Themes and Changes Over Time

The number of posts in our final dataset relating to each major OS is fairly similar overall. As Figure 2 shows, the proportions of posts relating to each major OS changed noticeably across the five years in the dataset. The spike in posts about Android apps in 2020–21 may have been due to new policies, restrictions, and verification processes that were introduced for Google Fit in October 2020 and went into force in May 2021 [30]. The numbers of posts about Apple HealthKit are less variable. There is a slight dip in 2019–2021; if there have been fewer major changes to privacy processes than for Google, documentation may have been better able to catch up, and SO users may be more able to reuse solutions proposed in the past.

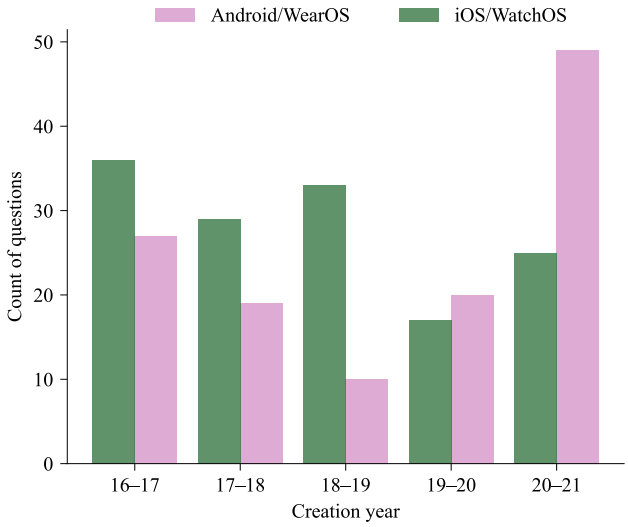

Figure 2: Count of health and privacy-related questions over the five-year period for each operating system (N = 265 posts; does not include posts about multiple OSes).

Table 2 shows the frequency of each of the themes we identified, grouped into major topics. The following subsections each discuss a group of themes in detail. Figure 3 breaks down the frequency of each theme over the five years of the dataset, for each major OS (does not include posts about multiple OSes).

5.2.1 Problems and inspirations for posting. The first group of themes concerns what problem or question inspired the poster to post on Stack Overflow. Unlike the other groups of themes, we applied these codes solely based on the initial question asked. The great majority of Stack Overflow posts about health app permissions or privacy (89.6%) were made because the asker was trying to figure out how to get **access to a protected resource**, such as reading health data either from a framework, a sensor on the smartphone, or another device, or writing to the framework data store.[5]

However, the specific focus of posts about data access tended to differ depending on which platform the developer was working with. For example, many of the posts from developers working with Apple HealthKit were concerned with how to get permissions requests and permissions justifications right. Such posts often focused on the interaction with the user via the permissions dialog.

[3] Except as otherwise noted, OS numbers in this section are based on the more accurate hand-coding of platforms, based on the entire post. They differ from those given in Table 3 (in Appendix B), which were based only on title and tags. In particular, posters asking about apps for WearOS or WatchOS often did not tag them nor mention the wearables-specific OS in the post title.

[4] When quoting, we use [Q] for questions, [A] for answers, and [C] for comments.

[5] We report numbers here to demonstrate the frequency with which each challenge is *mentioned* in our dataset; we do not assume that they represent the frequency with which those challenges *occur*.

Table 1: Posts about each operating system and health framework in the final dataset (N = 269).

Operating System	Posts
iOS (only)	108 (40.1%)
Android (only)	107 (39.8%)
WatchOS and iOS	32 (11.9%)
WearOS and Android	18 (6.7%)
Android and iOS	3 (1.1%)
Tizen and Android	1 (0.4%)

Health Framework	Posts
HealthKit	134 (49.8%)
Google Fit	120 (44.6%)
Samsung Health	6 (2.2%)
Other framework	2 (0.7%)
Google Fit and HealthKit	1 (0.4%)
Google Fit and Samsung Health	1 (0.4%)
Unspecified	1 (0.4%)
None (but unintended HealthKit; see §5.2.1)	4 (1.5%)

Table 2: Frequency of constructed themes. Occurrences were counted at the level of the whole post (N = 269). *Views*, *Answers*, *Comments*, and *Score* show the sum of values for all posts with that theme. Score is the difference between up votes and down votes.

Theme	Posts	Views	Answers	Comments	Score
Theme group: problems or inspirations for asking					
Need access to data or resource	241 (89.6%)	186,782	223	341	302
Error or crash	100 (37.2%)	97,682	102	150	140
App store submission or review problem	22 (8.2%)	17,936	27	47	44
Too much/unexpected data access	11 (4.1%)	9,600	8	14	10
Unintended attempts to access health data	4 (1.5%)	2,318	3	15	5
Theme group: causes or sources of problems					
App store requirements	35 (13.0%)	30,014	46	58	58
Third-party components	35 (13.0%)	18,564	31	63	35
Ethical considerations	14 (5.2%)	10,840	16	22	16
Legal requirements	5 (1.9%)	1,815	5	5	2
Theme group: proposed solutions					
Fix permissions/authentication	158 (58.7%)	159,013	195	275	236
Fix other code errors	64 (23.8%)	75,095	90	146	136
Not supported; bug; use an alternative option	61 (22.7%)	58,616	68	135	106
Follow health-specific requirements in app stores	26 (9.7%)	28,825	44	44	54
Theme group: attitudes and wishes					
Confusion about requirements/processes	73 (27.1%)	45,224	70	106	98
Need better documentation	51 (19.0%)	57,061	55	98	101
Clear feedback needed	27 (10.0%)	40,660	33	46	70
Frustration with existence of requirements/desire to bypass them	14 (5.2%)	8,572	16	20	8
Theme group: references to external sources					
Official documentation	132 (49.1%)	128,066	158	239	210
Other sources (e.g., how-tos and blogs)	80 (29.7%)	70,967	96	138	122
Theme group: mention of data privacy or sensitivity					
Mentioned explicitly	23 (8.6%)	16,145	32	32	32

A particular source of confusion in iOS was the feedback an app gets about whether the permissions request was successful. To protect users' privacy, Apple does not report to the app whether the user granted or denied a health permission request, only that the request was successfully made [10]. However, this runs contrary to developers' default assumption of what a returned value of "true" means for such an action:

> [Q] The method requestAuthorization(toShare:read:completion:) which asks for authorization always produces a true when the completion handler returns—success in my code below. Even when I decline everything in the simulator i get a true . . . . [A] You're misinterpreting what that success flag means. YES means that the permission screen was successfully shown and NO

> means that there was an error presenting the permissions screen [quote from official documentation]. [stackoverflow.com/questions/39233297]

With Google Fit, we found that many more posts were concerned with how to establish a connection to the framework involved. Establishing and managing an OAuth client requires extra effort; Google requires apps to be signed with the developer's private key and use a OAuth 2.0 client ID to access Google Fit [27]. Creating and managing certificates for this connection was a challenge.

Another frequent inspiration for posting was seeking the cause of **an error or crash** (37.2%). Askers often copy-pasted the error message or took a screenshot and asked for help or an explanation:

> [Q] Once I disable unable to reconnect. if try upload data to google fit I'm getting [this] error. *There was a problem reading the data. com.google.android.gms.common.api.ApiException: 4: The user must be signed in to make this API call.* [stackoverflow.com/questions/49106474]

Errors and crashes often occurred because the app did not have permission to access a resource or was unable to authenticate correctly to the API; 95% of the time, this theme co-occured with *need resource access*. Accordingly, the types of errors differed depending on the platform in similar ways to resource access problems. One common cause of crashes in iOS was forgetting to include usage descriptions (i.e., to explain to users why a permission is needed). The HealthKit documentation includes a prominent warning about this [11]; however, it is not clear why it triggers a crash rather than an error or notification. In Google Fit, troubles with OAuth certificates sometimes caused errors.

Some questions (8.2%) were prompted by **a submission or a review problem** in the app stores. Problems included uncertainties about submission instructions for health apps, automatic rejections of submissions that did not adhere to requirements (see §5.2.2), and apps being rejected after review by the store:

> [Q] I'm having trouble getting my app approved, and to be honest, I'm having trouble understanding what Apple are on about in this case. My app only uses HealthKit to create, pause, and finish a workout. It does not read any data [quote from app store feedback] The problem appears to be with my watchOS app not asking for permission to use the Health app. [stackoverflow.com/questions/42568105]

A few posts (1.5%) asked about a specific type of submission problem in the Apple App Store that was triggered by **non-health apps** that accidentally had a HealthKit call or a health permission listed. In three out of the four cases, the HealthKit references were in third-party libraries, and were difficult for the developer to find and remove:

> [Q] My xamarin.ios build has been rejected from the app center due to reference of HEALTHKIT framework. I can't set linker to SDK framework only because of some 3rd party liberary. Also, I have uploaded a nee build with mtouch parameter "–linkskip=HealthKit", still my app got rejected 2nd time. Can anyone please guide me what more cahnges need to be done to remove the reference of HEALTHKIT framework from the application. [stackoverflow.com/questions/55442764]

A few questions (4.1%) were inspired by posters discovering (or thinking they had discovered) that their health app had access to a health resource they did not intend it to, i.e., having **too much access**. In some cases, the developers were trying to find a way to revoke access because it was causing a problem in their authentication process. In other cases, they simply noticed it and were confused or concerned:

> [Q] The problem I have is that when I revoke access of my app from the user's account web page the Play Services client library still lets me use silentSignIn without a problem. So my question is—is this the proper way to get user's authorization to access their data? Is there a better or more accurate way? [stackoverflow.com/questions/49938922]

5.2.2 Causes or sources of issues. This group of themes identifies to whom or what the poster—or a commenter or answerer—explicitly attributed the cause(s) or source(s) of their problem or challenge. We captured all such sources, whether they came up as part of the problem description or were identified by someone offering a potential solution. We tried to rely only on explicit statements rather than drawing inferences based on our own knowledge, as we were interested in who or what developers themselves see as the active players in their context.

When talking about why they were having an issue, posters very often referred to **framework requirements or limitations**, i.e., requirements imposed by the relevant health-data frameworks (mostly Apple HealthKit or Google Fit) or by the OSes, or limitations on what could be done within those frameworks:

> [A] You should simply request authorization to read/write samples of the HKWorkout sample type. There are not fine-grained authorization controls for each individual activity type, such as HKWorkoutActivityTypeEquestrianSports, in HealthKit. [stackoverflow.com/questions/41251169]

We did not code for this theme separately and attempt to quantify it, in part because it was frequently difficult to tell whether a poster intended to specifically attribute framework requirements as the cause of their issue or was only providing context. However, it is worth noting that framework requirements or limitations were mentioned, or at least indirectly evoked, almost any time posters asked about problems accessing resources, as well as being frequently mentioned or evoked in discussions of other types of problems:

> [Q]Is it still the case that a user cannot grant HealthKit access on the watch alone even though Watch Series 3 now can be completely untethered via LTE? [stackoverflow.com/questions/47127864]

Another source of problems or constraints were **app store requirements** (13%). Posters had sometimes recognized these constraints during development, when they were blocked from *accessing a needed resource*, but often did not recognize them until they encountered a *submission or review problem*. Requirements included specifications for what should be in the code, including

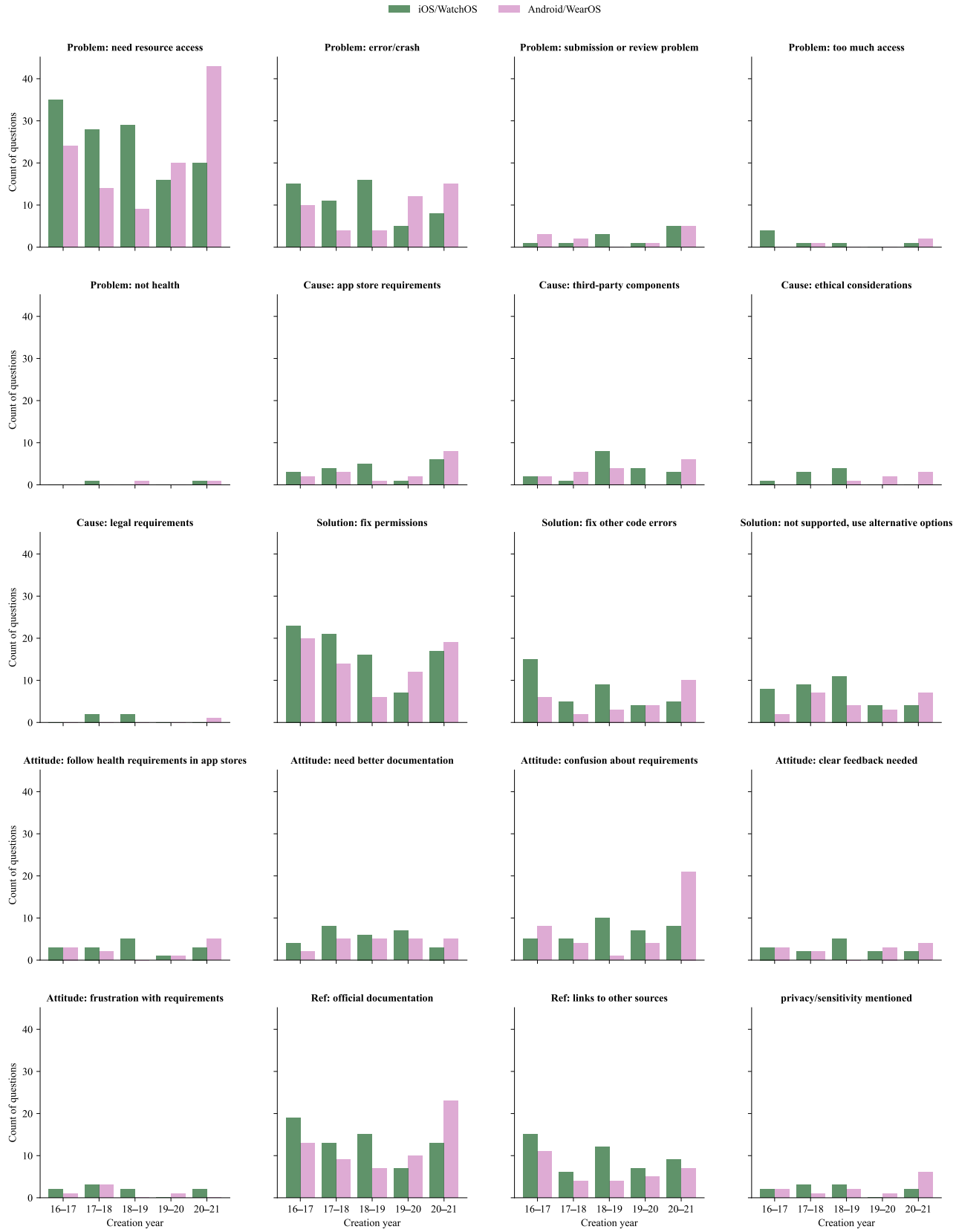

Figure 3: Count of health and privacy-related questions per theme with the two major operating systems ($N = 265$ posts).

correctly formatted permissions strings and (for some apps) encryption, as well as other types of requirements like disclosing health data collection and use in the app description, or developer verification:

> [Q] Everything works fine when installing the app from Android Studio or via side-loading. However, once I signed the APK and posted it on Play Store, the Fit History API part stopped working. . . . I have a hunch that when publishing an app on Play Store I need to do something special with regards to the fact that my app uses Fit History API. [stackoverflow.com/questions/49696997]

In particular, many recent posts were inspired by Google's new verification process specifically for health apps (see §2).

Users sometimes explicitly cited **ethical considerations** and values-based explanations for why health data is or should be considered worthy of protection or special treatment, or how users should be respected (5.2%):

> [C] Apple unfortunately won't allow you to get the Apple ID for the user, as this would be a privacy concern if any app could access that information. [stackoverflow.com/questions/64049847]

In particular, ethical explanations most frequently cooccured with *explicit mentions of privacy or data sensitivity*; however, under *ethical considerations*, we picked out posts where Stack Overflow users gave more detailed reasoning about ethics as a source of limitations. The two themes did not always overlap; for example, permissions might be described as a transparency mechanism without being explicitly framed in terms of privacy:

> [A] Android 10 introduces the android.permission.ACTIVITY_RECOGNITION runtime permission. . . . This is designed to give users visibility of how device sensor data is used in Settings. [stackoverflow.com/questions/59189266]

Requirements introduced by **laws and regulations**, including legal obligation via privacy policies, were mentioned in a few posts (1.9%):

> [A] And in some regions (such as the USA, and I suspect even more strongly within the EU), health privacy is considered a relatively important & legally required thing. So your app's users have to officially acknowledge and permit your app to read HealthKit data. [stackoverflow.com/questions/48493980]

For the most part, including in the examples above, ethical and legal considerations were cited as *secondary causes* explaining the requirements of the framework or platform in question, often as context for a quote from official documentation. However, in some cases, they were mentioned as explanations in themselves:

> [A] This is really a question for a lawyer and something you need to consider in terms of various privacy laws around the world as well as your own potential liability. I don't believe that Apple forbids it as long as the user grants you permission. [stackoverflow.com/questions/66286031]

The situation is similar for *explicit mentions of privacy or sensitivity*.

Relatedly, it is worth noting that these explicit mentions of ethical or legal considerations, or of the privacy or sensitivity of data, were more often brought up in a comment or an answer than raised in the original question. In only 14% of the posts citing ethical considerations and 20% citing legal considerations, and in only 22% of posts explicitly mentioning privacy or sensitivity, did those themes come up in the original question. In all of the other cases, the original poster asked a question about access control or submission problems, and the privacy, ethical, or legal context for those structures was introduced by someone else.

Third-party components, such as wearables and sensor devices, data sources, tools, and frameworks or libraries—including other health frameworks such as Samsung or Garmin Health—were attributed as the cause of a problem as often as app store requirements (13%). This highlights the impact of such components on developers' workflows:

> [Q] I use react-native-google-fit [bridge] package to get the steps data about the user. In my case this package works fine in some devices but in some others cant get any data or response from the google-fit API . . . . I implemented bugnsag to track the steps and the process stucks when I call google-fit API to get step samples. [stackoverflow.com/questions/63613349]

For the most part, developers who mentioned problems with third-party components were largely having trouble syncing data (intentionally) or sorting out authentication between the various elements. But as we noted in §5.2.1, third-party tools and libraries could also introduce unexpected data calls or permissions requests.

5.2.3 Proposed solutions. We also examined the solutions or resolutions proposed in both answers and comments (including solutions mentioned by the original poster, if they added a comment or answer to their own question). We looked at both accepted, successful solutions and solutions that were downvoted or that the original poster said were unsuccessful or irrelevant, as all of these provide insight into how developers think about the problems at hand.

A majority of solutions suggested ways that the poster could **fix permissions or authentication** requests (58.7%). Suggested fixes included adding a permission request to code, fixing the syntax of a permission or authentication request (especially by adding a purpose description), and taking some action to reset permissions status (e.g., by reinstalling):

> [A] There are two Info.plist files that need NSHealthShareUsageDescription and NSHealthUpdateUsageDescription. One in the project file and one in the watch extension file. I had only done one of these. The strings for these also need to be a reasonable length and cannot be just a couple of words. [stackoverflow.com/questions/60081551]

Both Apple and Google require such a purpose description, as well as an explanation in the permissions dialog about the intended use of the data.

Some of the solutions provided specific advice about how to **follow health-specific requirements in app stores** (9.7%) (see §5.2.2). Advice might include registering as a health app developer (or registering test users) with the app store, or disclosing the use

of health data (via upload checkboxes, app descriptions, and/or permissions lists):

> [A] This is Private Policy for my app which uses HealthKit: [link]. It is fine for Apple Review team. You should also write that your app uses HealthKit in app's description in ItunesConnect (e.g 'HealthKit displays the amount of steps you need to make today'). [stackoverflow.com/questions/39688057]

Many suggested solutions (23.8%) involved fixing other aspects of the app unrelated to privacy, permissions, or authentication. **Fixing other code issues** might include updating versions, e.g., of a library, or fixing the syntax of non-permissions-related code, as well as removing references to health data in non-health apps:

> [A] This is a concurrency problem, not a HealthKit problem. . . . . You have to wait for the answer of requestAuthorization before you continue reading birthday and biologicalSex. [stackoverflow.com/questions/40396194]

Some answers and (especially) comments suggested that there was **no supported solution** for the asker's problem (22.7%). In some cases, the operating system or health framework is not designed to allow the desired app behavior:

> [Q] Does HealthKit report to the cloud that can be accessed with an API? Or does it need to be an app that accesses the HealthKit data locally? [A] There is no cloud API, you would have to create an app that reads the HelathKit data and reports it to your backend. [stackoverflow.com/questions/60175535]

In other cases, there was an unresolved bug in the system:

> [C] I think there is an open bug report regarding reading HealthDataTypes, try following that report to be updated. [stackoverflow.com/questions/46110711].

In some cases, answers or comments suggested workarounds or third-party alternatives for unsupported features/bugs.

5.2.4 Developers' Attitudes and Wishes. Some posters explicitly expressed their feelings or attitudes about the issue they were having, or their wishes for changes that they thought would make their situation better.[6]

Posters complained about unhelpful documentation or expressed a **need for better documentation** (19%). Problems included documentation being difficult to find or understand, missing key information or examples, or relying on sample code that did not work:

> I need my app to read step count from Google Fit. I'm using health 3.05 package. For now I copied the example code to see if it works and unfortunately it's not. Of course I did every step from this packge readme. [stackoverflow.com/questions/67432179].

Others complained about unclear runtime error messages, crashes with no error messages, or unclear app store rejection notices, and expressed a **need for clear feedback** (10%):

> [C] The first line of the guideline I quoted in my answer (the guideline you were rejected on) says apps must "indicate that integration in their app description." Although I agree that Apple could certainly have been clearer in their rejection notice. [stackoverflow.com/questions/39716868].

As we noted in §5.2.1, even successfully completed operations could produce confusing feedback.

Askers and answerers sometimes expressed their **confusion about requirements or processes** (27.1%).[7] Situations prompting such expressions included not knowing how to accomplish a task within the framework, not knowing why code was not achieving the expected results (including code from suggested solutions), or not knowing why a particular configuration behaves in a specific way:

> [Q] The watch face authenticates and receive fit data. Without actual OAuth Client and a Client ID! I thought there was some kind of caching in action. But now it's several hours and it keeps working. Does anybody have any idea WHY? How is this possible? [stackoverflow.com/questions/42228885].

A few posts (5.2%) expressed **frustration with the existence of requirements or a desire to bypass those requirements**,[8] e.g., HealthKit's or Google Fit's permissions structures:

> [C] It seems like permissions overload to require this as a permission when the user has to grant location access for this to be useful anyway. [stackoverflow.com/questions/45437669].

Sometimes, this attitude might result from the differences between how the two major frameworks handle health data:

> [Q] Are there any third party which provide data of apple health kit data using there end points like google fit provide us via rest api's [link to documentation] [stackoverflow.com/questions/60482930].

5.2.5 References to other resources. Stack Overflow users often provided links to or quotes from external resources. Those resources included **official documentation** (in 49.1% of posts) such as Apple, Android, HealthKit, or Google Fit web resources, libraries, and tutorials with sample code, or similar resources for third-party tools. References to **other sources** (29.7%) included online tutorials, blogs, example GitHub repositories, and other Stack Overflow posts.

Stack Overflow can in itself function as an aid to understanding such documentation. In some cases, when question-askers included quotes from documentation they were trying to follow, they asked their fellow Stack Overflow users to help explain it. In answers and comments, users sometimes explained parts of documentation that they perceived the asker had misunderstood, as well as pointing out documentation the asker might not have seen.

[6] Feelings and attitudes can be more difficult to reliably identify in text. The two coders tried to rely only on explicit cues, and interrater agreement scores for this group of codes were similar to the rest.

[7] It is likely that many people who decide to ask a question on Stack Overflow are feeling confused. This theme picks out those who express their feeling of confusion explicitly in the public forum.

[8] This theme captures negative attitudes towards the requirements or limitations existing in the first place (or demonstrating a desire to get around them), as opposed to negative attitudes about the difficulty of implementation, which are captured under *confusion about requirements*.

6 DISCUSSION

Above, we described the themes we constructed through our qualitative analysis of 269 Stack Overflow posts about privacy and permissions in health apps for Android or iOS. In the following, we discuss the implications of our findings and suggest future research avenues.

6.1 Who Triggers Privacy Discussions?

In our sample, posters did not tend to explicitly frame questions in terms of data privacy, nor in terms of legal regulations or ethical considerations when dealing with sensitive data. For the most part, where those themes came up at all, they were introduced by those answering or commenting, rather than motivating an initial question—and were most often introduced in the process of explaining platform and framework requirements.

Since their interaction is with the platforms and their requirements, developers' motivation is generally to satisfy the requirements so they can distribute their app. For example, the introduction of additional restrictions and verification processes for Google Fit apps prompted an increase in questions on that topic.

These findings are in line with prior work on health app security; for example, a study with 97 health app developers showed that their primary reasons for considering security measures were to avoid legal issues and financial losses [5]. More broadly, this study adds to a body of work showing that software development platforms play a critical role in developers' motivation to implement privacy features [7, 32, 62, 73]. For health apps, this role may be played by the health frameworks that provide the data rather than the OSes or app stores, but the motivational structure is similar.

While we did not observe many questions explicitly discussing legal issues, regulations can still impact developers' workflows, workloads, and privacy concerns. For example, the change in the number of questions over the course of 2016–2019 may be related to how GDPR was reflected in platforms' changing policies and processes for data handling.

Many studies show apps are often noncompliant with privacy regulations [56, 57], including health apps [63, 74, 83]. Prior work outlines how privacy regulations in general can encourage attention to privacy among technology developers—but also the challenges they may face in implementing them [7, 18, 82]. For example, mobile app developers find it challenging to find relevant information hosted by on ad networks' platforms about the privacy regulations that pertain to ad services, and to integrate regulation-compliant ads [71]. However, we believe that regulations may act as a catalyst for conversations about privacy within technical communities.

6.2 Design Implications for Privacy-Related Documentation and Review Tools on Health Features

Improving platforms' documentation on health-specific requirements. Few Stack Overflow posters questioned the *necessity* for enhanced permissions structures for health data; most seemed to accept it as a given. However, many posters expressed confusion about what the requirements *are*, and often complained of a lack of clarity from the platforms about *how* to comply with their privacy requirements. While Apple and Google provide plenty of documentation about their health frameworks, developers seem to still have trouble interpreting it or finding answers to their questions.

We find that, while there are many resources about developing with HealthKit and Google Fit—such as online tutorials, videos, and blogs—official documentation (see §5.2.5) is still the most cited resource in our dataset. This highlights how much developers rely on official documentation; it impacts millions of developers—and therefore millions more users. Improving the quality of documentation has the potential to impact how developers treat their users' privacy; as we described in §6.1, platforms are often the main drivers of developers' understanding of privacy.

Developing review tools to detect health data use. One of the recurring complaints we saw among Stack Overflow users (including developers of non-health apps) was having an app rejected because they had some health permission listed in their app that they did not intend to, or because of other problems stemming from third-party components [cf. 7, 17, 77]. One solution could be integrating automatic checks for health data into programming tools or before submitting an app to an app store. Platforms could benefit from fewer flags for app reviews, and developers could save time by not having to go through the app submission process multiple times.

Improving privacy documentation for third-party tools. A larger-scale solution would be to provide incentives and channels for third parties to better document and communicate the privacy implications to developers who integrate their components [cf. 68, 77]. One potential direction is to start with privacy "nutrition labels" [e.g., 42], borrowing from research on labels for end users, but accounting for the different needs and understanding of developers.

6.3 Capturing the Broad Framing of Privacy Discussions in Developer Forums

To capture all the ways that privacy considerations play out in systems that health app developers interact with, we found that we needed a different approach than previous research. For example, to analyze how developers themselves conceptualize privacy, Tahaei et al. [73] collected Stack Overflow posts that had "privacy" in their title or tags. In contrast, for this study, we instead began with posts about health apps for Android and iOS, then hand-picked the 269 posts that had a privacy angle. This approach captured broad aspects of app structure that are motivated by privacy or that have privacy consequences (namely, permissions, authentication, encryption, and data security)—whether or not "privacy" is mentioned. If we had focused only on threads where the discussion specifically mentioned privacy *per se*, we would have had only 23 posts in our final dataset—and if we had only included posts where "privacy" was in the title or tags, we would have had only *one* post left (a post on privacy policies). Our broad rubric allowed us to collect a dataset large enough—and comprehensive enough—to provide rich insights into health app developers' privacy challenges.

6.4 Limitations

Our study may suffer from selection bias, due to our choice of keywords for the initial dataset and the fact that we only queried on titles and tags (an approach similar to other privacy and security

research on developer forums [e.g., 45, 73, 84]). An alternative approach might sample random posts, and identify relevant posts by manually coding them; however, this approach would be very time-consuming relative to the number of relevant posts it would find.

Among the themes we identified and analyzed in the final dataset, some were more concrete and easily relatable to the posters' explicit statements, while others relied more on subjective interpretation of the posters' intent. Two authors coded each post to improve reliability and reduce bias.

Our sample covers developers who were inspired to post in a help forum, meaning almost entirely people who currently had a programming problem they wanted to solve. While this fits our RQs—finding out what the challenges are—it gives a limited view on how health app developers think about privacy more broadly.

In addition, though Stack Overflow is one of the largest Q&A websites for developers, our findings may not be generalizable to all health-app developers and developer forums.

6.5 Future Work

In addition to exploring the potential tools and standards suggested in §6.2, future research on this topic could: (1) identify a broader set of challenges (beyond those that could be addressed via Stack Overflow) by conducting interviews or surveys with health-app developers; (2) compare how privacy is addressed in documentation for health-specific vs. general software development platforms and data frameworks, and suggest improvements; and (3) further examine the interaction between health privacy regulations and regulation-driven platform requirements or software features in changing health app developers' privacy practices and workflows.

7 CONCLUSION

Health-specific requirements imposed by Apple and Google have introduced new challenges and complications for developers—for example, Apple's requirement for specific explanations of health data use in app descriptions, or Google's new submission procedure with an extra step for apps that use health data. Developers also face issues caused by unexpected data collection and sharing practices of third parties, which may violate the health-specific requirements.

The privacy efforts of most developers in our dataset were driven largely by the requirements and limitations imposed by health frameworks, platforms, and app stores. However, many developers found it challenging to figure out how to comply. There were many complaints about unclear, difficult-to-find, or non-working official documentation, highlighting the value of platforms' providing usable documentation about privacy features.

In sum, we found that platforms' requirements and documentation significantly impact how health app developers engage with and address privacy challenges in dealing with health data. While platforms' extra privacy measures to protect health data are laudable, we find that the ways they are implemented can turn into an additional burden on developers. We believe those extra measures need to be easier for developers to work with. A first step could be to address how privacy is covered in the documentation of health data frameworks, health-tracking devices, and app marketplaces. Improvements in coverage, framing, and organization of documentation have the potential to substantively improve developers' understanding of how to accomplish privacy tasks, and of the privacy implications of their choices about app structure. Increasing such support for health app developers could in turn have an impact in improving privacy protections in the health data ecosystem.

ACKNOWLEDGMENTS

This work is partly supported by the UK Engineering and Physical Sciences Research Council (grants "Why Johnny doesn't write secure software? Secure software development by the masses" EP/P011799/2 and EP/V011189/1), the U.S. National Science Foundation (grant CNS-2055772), and the U.S. National Security Agency (contract H98230-18-D-0006).

REFERENCES

[1] Yasemin Acar, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L Mazurek, and Christian Stransky. 2016. You Get Where You're Looking for: The Impact of Information Sources on Code Security. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 289–305. https://doi.org/10.1109/SP.2016.25

[2] Yasemin Acar, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L. Mazurek, and Christian Stransky. 2017. How Internet Resources Might Be Helping You Develop Faster but Less Securely. *IEEE Security and Privacy* 15, 2 (apr 2017), 50–60. https://doi.org/10.1109/MSP.2017.24

[3] Urs-Vito Albrecht, Oliver Pramann, and Ute von Jan. 2015. Medical Apps - The Road To Trust. *European Journal for Biomedical Informatics* 11, 03 (2015). https://doi.org/10.24105/ejbi.2015.11.3.3

[4] Abdulrahman Alhazmi and Nalin Asanka Gamagedara Arachchilage. 2021. I'm all ears! Listening to software developers on putting GDPR principles into software development practice. *Personal and Ubiquitous Computing* 25, 5 (Oct. 2021), 879–892. https://doi.org/10.1007/s00779-021-01544-1

[5] Bakheet Aljedaani, Aakash Ahmad, Mansooreh Zahedi, and M. Ali Babar. 2020. An Empirical Study on Developing Secure Mobile Health Apps: The Developers' Perspective. In *2020 27th Asia-Pacific Software Engineering Conference (APSEC)*. IEEE Computer Society, Los Alamitos, CA, USA, 208–217. https://doi.org/10.1109/APSEC51365.2020.00029

[6] Bakheet Aljedaani and M Ali Babar. 2021. Challenges With Developing Secure Mobile Health Applications: Systematic Review. *JMIR Mhealth Uhealth* 9, 6 (21 6 2021). https://doi.org/10.2196/15654

[7] Noura Alomar and Serge Egelman. 2022. Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps. *Proceedings on Privacy Enhancing Technologies* 2022, 4 (2022). https://doi.org/10.2478/popets-2022-0108

[8] Apple. 2021. *About the HealthKit Framework | Apple Developer Documentation*. Retrieved Dec 2021 from https://developer.apple.com/documentation/healthkit/about_the_healthkit_framework

[9] Apple. 2021. *App Review*. Retrieved Dec 2021 from https://developer.apple.com/app-store/review/

[10] Apple. 2021. *Authorizing Access to Health Data | Apple Developer Documentation*. Retrieved Dec 2021 from https://developer.apple.com/documentation/healthkit/authorizing_access_to_health_data

[11] Apple. 2021. *Protecting User Privacy*. Retrieved Dec 2021 from https://developer.apple.com/documentation/healthkit/protecting_user_privacy

[12] Renana Arizon-Peretz, Irit Hadar, Gil Luria, and Sofia Sherman. 2021. Understanding developers' privacy and security mindsets via climate theory. *Empirical Software Engineering* 26, 6 (Nov. 2021), 123. https://doi.org/10.1007/s10664-021-09995-z

[13] Jeff Atwood. 2009. *Attribution Required*. Stack Overflow. Retrieved Dec 2021 from https://stackoverflow.blog/2009/06/25/attribution-required/

[14] Jeff Atwood. 2009. *Stack Overflow Creative Commons Data Dump*. Stack Overflow. Retrieved Dec 2021 from https://stackoverflow.blog/2009/06/04/stack-overflow-creative-commons-data-dump/

[15] Jeff Atwood. 2010. *Academic Papers Using Stack Overflow Data*. Stack Overflow. Retrieved Dec 2021 from https://stackoverflow.blog/2010/05/31/academic-papers-using-stack-overflow-data/

[16] Oshrat Ayalon, Eran Toch, Irit Hadar, and Michael Birnhack. 2017. How Developers Make Design Decisions about Users' Privacy: The Place of Professional Communities and Organizational Climate. In *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (Portland, Oregon, USA) *(CSCW '17 Companion)*. Association for Computing Machinery, New York, NY, USA, 135–138. https://doi.org/10.1145/3022198.3026326

[17] Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason I Hong, and Lorrie Cranor. 2014. The privacy and security behaviors of smartphone app developers. In *Workshop on Usable Security (USEC'14)*. Internet Society. https://doi.org/10.14722/usec.2014.23006

[18] Kenneth A Bamberger and Deirdre K Mulligan. 2015. *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. MIT Press. https://mitpress.mit.edu/books/privacy-ground

[19] Kathrin Bednar, Sarah Spiekermann, and Marc Langheinrich. 2019. Engineering Privacy by Design: Are engineers ready to live up to the challenge? *The Information Society* 35, 3 (2019), 122–142. https://doi.org/10.1080/01972243.2019.1583296

[20] Jerry Beilinson. 2020. Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds. *Consumer Reports* (2020). https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats-a1100919965/ Blog post. Accessed: 9 June 2022.

[21] Martyn Casserly. 2019. *iPhone vs Android market share*. Retrieved July 2022 from https://www.macworld.com/article/673487/iphone-vs-android-market-share.html

[22] Swathikan Chidambaram, Simon Erridge, James Kinross, and Sanjay Purkayastha. 2020. Observational study of UK mobile health apps for COVID-19. *The Lancet Digital Health* 2, 8 (2020), e388–e390. https://doi.org/10.1016/S2589-7500(20)30144-8

[23] Roland Croft, Yongzheng Xie, Mansooreh Zahedi, M. Ali Babar, and Christoph Treude. 2021. An empirical study of developers' discussions about security challenges of different programming languages. *Empirical Software Engineering* 27, 1 (Dec. 2021), 27. https://doi.org/10.1007/s10664-021-10054-w

[24] Robert Feldt, Thomas Zimmermann, Gunnar R. Bergersen, Davide Falessi, Andreas Jedlitschka, Natalia Juristo, Jürgen Münch, Markku Oivo, Per Runeson, Martin Shepperd, Dag I. K. Sjøberg, and Burak Turhan. 2018. Four commentaries on the use of students and professionals in empirical software engineering experiments. *Empirical Software Engineering* 23, 6 (Dec. 2018), 3801–3820. https://doi.org/10.1007/s10664-018-9655-0

[25] Felix Fischer, Konstantin Böttinger, Huang Xiao, Christian Stransky, Yasemin Acar, Michael Backes, and Sascha Fahl. 2017. Stack Overflow Considered Harmful? The Impact of Copy Paste on Android Application Security. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 121–136. https://doi.org/10.1109/SP.2017.31

[26] 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

[27] Google. 2021. *Get an OAuth 2.0 Client ID*. Retrieved Dec 2021 from https://developers.google.com/fit/android/get-api-key

[28] Google. 2021. *Health Platform API | Android Developers*. Retrieved Dec 2021 from https://developer.android.com/training/wearables/health-services/health-platform

[29] Google. 2021. *OAuth API verification FAQs*. Retrieved Dec 2021 from https://support.google.com/cloud/answer/9110914

[30] Google. 2021. *Release Notes | Google Fit | Google Developers*. Retrieved Dec 2021 from https://developers.google.cn/fit/android/releases?hl=it

[31] Google. 2021. *Verify your app for use with Google Fit API*. Retrieved Dec 2021 from https://developers.google.com/fit/verification

[32] Daniel Greene and Katie Shilton. 2018. Platform privacies: Governance, collaboration, and the different meanings of "privacy" in iOS and Android development. *New Media & Society* 20, 4 (2018), 1640–1657. https://doi.org/10.1177/1461444817702397

[33] Irit Hadar, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. 2018. Privacy by designers: Software developers' privacy mindset. *Empirical Software Engineering* 23, 1 (Feb. 2018), 259–289. https://doi.org/10.1007/s10664-017-9517-1

[34] Eszter Hargittai, Elissa M. Redmiles, Jessica Vitak, and Michael Zimmer. 2020. Americans' willingness to adopt a covid-19 tracking app. *First Monday* 25, 11 (Oct. 2020), online. https://doi.org/10.5210/fm.v25i11.11095

[35] Maximilian Häring, Eva Gerlitz, Christian Tiefenau, Matthew Smith, Dominik Wermke, Sascha Fahl, and Yasemin Acar. 2021. Never ever or no matter what: Investigating Adoption Intentions and Misconceptions about the Corona-Warn-App in Germany. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, 77–98. https://www.usenix.org/conference/soups2021/presentation/acar

[36] Hideaki Hata, Nicole Novielli, Sebastian Baltes, Raula Gaikovina Kula, and Christoph Treude. 2021. GitHub Discussions: An exploratory study of early adoption. *Empirical Software Engineering* 27, 1 (Oct. 2021), 3. https://doi.org/10.1007/s10664-021-10058-6

[37] Majid Hatamian, Samuel Wairimu, Nurul Momen, and Lothar Fritsch. 2021. A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps. *Empirical Software Engineering* 26, 3 (March 2021), 36. https://doi.org/10.1007/s10664-020-09934-4

[38] Hsiao-Ying Huang and Masooda Bashir. 2017. Users' Adoption of Mental Health Apps: Examining the Impact of Information Cues. *JMIR Mhealth Uhealth* 5, 6 (28 06 2017), e83. https://doi.org/10.2196/mhealth.6827

[39] Kit Huckvale, John Torous, and Mark E. Larsen. 2019. Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation. *JAMA Network Open* 2, 4 (April 2019), e192542. https://doi.org/10.1001/jamanetworkopen.2019.2542

[40] Information Commissioner's Office. 2021. *Health data | ICO*. Retrieved Dec 2021 from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/health-data/

[41] Harjot Kaur, Sabrina Amft, Daniel Votipka, Yasemin Acar, and Sascha Fahl. 2022. Where to Recruit for Security Development Studies From: Comparing Six Software Developer Samples. In *Proceedings of the 2022 USENIX Security Symposium - SEC'22*.

[42] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "Nutrition Label" for Privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS)* (Mountain View, California, USA) *(SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 4, 12 pages. https://doi.org/10.1145/1572532.1572538

[43] Lawrence L. Kupper and Kerry B. Hafner. 1989. On Assessing Interrater Agreement for Multiple Attribute Responses. *Biometrics* 45, 3 (1989), 957–967. http://www.jstor.org/stable/2531695

[44] Simon Leigh, Rob Daly, Sebastian Stevens, Luka Lapajne, Charlotte Clayton, Tim Andrews, and Liz Ashall-Payne. 2021. Web-based internet searches for digital health products in the United Kingdom before and during the COVID-19 pandemic: a time-series analysis using app libraries from the Organisation for the Review of Care and Health Applications (ORCHA). *BMJ Open* 11, 10 (2021). https://doi.org/10.1136/bmjopen-2021-053891

[45] Tianshi Li, Elizabeth Louie, Laura Dabbish, and Jason I. Hong. 2021. How Developers Talk About Personal Data and What It Means for User Privacy: A Case Study of a Developer Forum on Reddit. *Proceedings of the ACM on Human-Compututer Interaction* 4, CSCW3 (Jan. 2021), 28 pages. https://doi.org/10.1145/3432919

[46] Deborah Lupton. 2021. "Sharing Is Caring:" Australian Self-Trackers' Concepts and Practices of Personal Data Sharing and Privacy. *Frontiers in Digital Health* 3 (2021). https://doi.org/10.3389/fdgth.2021.649275

[47] Borja Martínez-Pérez, Isabel de la Torre-Díez, and Miguel López-Coronado. 2013. Mobile Health Applications for the Most Prevalent Conditions by the World Health Organization: Review and Analysis. *J Med Internet Res* 15, 6 (14 06 2013), e120. https://doi.org/10.2196/jmir.2600

[48] Maryam Mehrnezhad and Teresa Almeida. 2021. Caring for Intimate Data in Fertility Technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, Yokohama Japan, 1–11. https://doi.org/10.1145/3411764.3445132

[49] Matthew Miles and Michael Huberman. 1994. *Qualitative Data Analysis: A Methods Sourcebook*. Sage.

[50] 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). https://doi.org/10.2196/12578

[51] Leysan Nurgalieva, David O'Callaghan, and Gavin Doherty. 2020. Security and Privacy of mHealth Applications: A Scoping Review. *IEEE Access* 8 (2020), 104247–104268. https://doi.org/10.1109/ACCESS.2020.2999934

[52] Leysan Nurgalieva, Seamus Ryan, and Gavin Doherty. 2021. Attitudes towards COVID-19 contact tracing apps: a cross-national survey. *IEEE Access* (2021). https://doi.org/10.1109/ACCESS.2021.3136649

[53] 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. https://doi.org/10.1109/ACCESS.2018.2799522

[54] 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. https://doi.org/10.1016/j.ijlp.2019.04.002

[55] 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). https://doi.org/10.1016/j.ijmedinf.2022.104707

[56] Joel Reardon, Álvaro Feal, Primal Wijesekera, Amit Elazari Bar On, Narseo Vallina-Rodriguez, and Serge Egelman. 2019. 50 Ways to Leak Your Data: An Exploration of Apps'Circumvention of the Android Permissions System. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 603–620. https://www.usenix.org/conference/usenixsecurity19/presentation/reardon

[57] 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. https://doi.org/10.1515/popets-2018-0021

[58] Rivka Ribak. 2019. Translating privacy: developer cultures in the global world of practice. *Information, Communication & Society* 22, 6 (2019), 838–853. https://doi.org/10.1080/1369118X.2019.1577475

[59] Johnny Saldaña. 2015. *The Coding Manual for Qualitative Researchers.* Sage.

[60] Jordan Samhi, Kevin Allix, Tegawendé F. Bissyandé, and Jacques Klein. 2021. A first look at Android applications in Google Play related to COVID-19. *Empirical Software Engineering* 26, 4 (April 2021), 57. https://doi.org/10.1007/s10664-021-09943-x

[61] Awanthika Senarath and Nalin A. G. Arachchilage. 2018. Why Developers Cannot Embed Privacy into Software Systems?: An Empirical Investigation. In *Proceedings of the 22Nd International Conference on Evaluation and Assessment in Software Engineering 2018* (Christchurch, New Zealand) *(EASE'18)*. ACM, New York, NY, USA, 211–216. https://doi.org/10.1145/3210459.3210484

[62] Katie Shilton and Daniel Greene. 2019. Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development. *Journal of Business Ethics* 155, 1 (March 2019), 131–146. https://doi.org/10.1007/s10551-017-3504-8

[63] Laura Shipp and Jorge Blasco. 2020. How private is your period?: A systematic analysis of menstrual app privacy policies. *Proceedings on Privacy Enhancing Technologies* 2020, 4 (Oct. 2020), 491–510. https://doi.org/10.2478/popets-2020-0083

[64] Sarah Spiekermann. 2012. The Challenges of Privacy by Design. *Commun. ACM* 55, 7 (07 2012), 38–40. https://doi.org/10.1145/2209249.2209263

[65] Sarah Spiekermann, Jana Korunovska, and Marc Langheinrich. 2019. Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers. *Proceedings of the IEEE* 107, 3 (2019), 600–615. https://doi.org/10.1109/JPROC.2018.2866769

[66] Stack Exchange. 2021. *Stack Exchange Data Explorer.* Retrieved Dec 2021 from https://data.stackexchange.com/stackoverflow/queries

[67] Statista. 2021. *Mobile operating systems' market share worldwide from January 2012 to June 2021.* Retrieved Dec 2021 from https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/

[68] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Deciding on Personalized Ads: Nudging Developers About User Privacy. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, 573–596. https://www.usenix.org/conference/soups2021/presentation/tahaei

[69] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. ACM, 1–15. https://doi.org/10.1145/3411764.3445768

[70] Mohammad Tahaei, Tianshi Li, and Kami Vaniea. 2022. Understanding Privacy-Related Advice on Stack Overflow. In *Proceedings on Privacy Enhancing Technologies*. 1–18. https://doi.org/10.2478/popets-2022-0032

[71] Mohammad Tahaei, Kopo M. Ramokapane, Tianshi Li, Jason I. Hong, and Awais Rashid. 2022. Charting App Developers' Journey Through Privacy Regulation Features in Ad Networks. In *Proceedings on Privacy Enhancing Technologies*. 1–24. https://doi.org/10.2478/popets-2022-0059

[72] Mohammad Tahaei and Kami Vaniea. 2019. A Survey on Developer-Centred Security. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 129–138. https://doi.org/10.1109/EuroSPW.2019.00021

[73] Mohammad Tahaei, Kami Vaniea, and Naomi Saphra. 2020. Understanding Privacy-Related Questions on Stack Overflow. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. ACM, 1–14. https://doi.org/10.1145/3313831.3376768

[74] Gioacchino Tangari, Muhammad Ikram, Kiran Ijaz, Mohamed Ali Kaafar, and Shlomo Berkovsky. 2021. Mobile health and privacy: cross sectional study. *BMJ* 373 (2021). https://doi.org/10.1136/bmj.n1248

[75] The European Parliament and the Council of the European Union. 2018. *General Data Protection Regulation (GDPR).* Retrieved Dec 2021 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[76] U.S. Department of Health & Human Services. 2021. *Health Information Privacy.* Retrieved Dec 2021 from https://www.hhs.gov/hipaa/index.html

[77] Christine Utz, Sabrina Amft, Martin Degeling, Thorsten Holz, Sascha Fahl, and Florian Schaub. 2022. Privacy Rarely Considered: Exploring Considerations in the Adoption of Third-Party Services by Websites. https://doi.org/10.48550/ARXIV.2203.11387

[78] Christine Utz, Steffen Becker, Theodor Schnitzler, Florian M. Farke, Franziska Herbert, Leonie Schaewitz, Martin Degeling, and Markus Dürmuth. 2021. Apps Against the Spread: Privacy Implications and User Acceptance of COVID-19-Related Smartphone Apps on Three Continents. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, Article 70, 22 pages. https://doi.org/10.1145/3411764.3445517

[79] José Van Dijck and Thomas Poell. 2016. Understanding the promises and premises of online health platforms. *Big Data & Society* 3, 1 (2016). https://doi.org/10.1177/2053951716654173

[80] Carmine Vassallo, Sebastiano Panichella, Fabio Palomba, Sebastian Proksch, Harald C. Gall, and Andy Zaidman. 2020. How developers engage with static analysis tools in different contexts. *Empirical Software Engineering* 25, 2 (March 2020), 1419–1457. https://doi.org/10.1007/s10664-019-09750-5

[81] Jessica Vitak, Yuting Liao, Priya Kumar, Michael Zimmer, and Katherine Kritikos. 2018. Privacy Attitudes and Data Valuation Among Fitness Tracker Users. In *Transforming Digital Worlds (Lecture Notes in Computer Science)*, Gobinda Chowdhury, Julie McLeod, Val Gillet, and Peter Willett (Eds.). Springer International Publishing, Cham, 229–239. https://doi.org/10.1007/978-3-319-78105-1_27

[82] Ari Ezra Waldman. 2018. Designing Without Privacy. *Houston Law Review* 55, 659 (2018). https://ssrn.com/abstract=2944185 NYLS Legal Studies Research Paper No. 2944185. Available via Social Science Research Network. Accessed: 23 November 2018.

[83] Vera Wesselkamp, Imane Fouad, Cristiana Santos, Yanis Boussad, Nataliia Bielova, and Arnaud Legout. 2021. In-Depth Technical and Legal Analysis of Tracking on Health Related Websites with ERNIE Extension. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society* (Virtual Event, Republic of Korea) *(WPES '21)*. Association for Computing Machinery, New York, NY, USA, 151–166. https://doi.org/10.1145/3463676.3485603

[84] Xin-Li Yang, David Lo, Xin Xia, Zhi-Yuan Wan, and Jian-Ling Sun. 2016. What Security Questions Do Developers Ask? A Large-Scale Study of Stack Overflow Posts. *Journal of Computer Science and Technology* 31, 5 (Sept. 2016), 910–924. https://doi.org/10.1007/s11390-016-1672-0

[85] Michael Zimmer, Priya Kumar, Jessica Vitak, Yuting Liao, and Katie Chamberlain Kritikos. 2020. 'There's nothing really they can do with this information': Unpacking how users manage privacy boundaries for personal fitness information. *Information, Communication & Society* 23, 7 (June 2020), 1020–1037. https://doi.org/10.1080/1369118X.2018.1543442

A DATA COLLECTION QUERIES

To collect the data, we ran the SQL query below [66]. We iterated the query for each combination of health-related keyword {health, google-fit, medical, fitness} and operating system {ios, android, watchos, wearos} (due to server limits, we were not able to combine all into one query).

```
SELECT
  DISTINCT *
FROM
  Posts p
WHERE
  (
    (
      Lower(title) LIKE '%fitness%'
      AND Lower(title) LIKE '%wearos%'
    )
    OR (
      Lower(tags) LIKE '%fitness%'
      AND Lower(tags) LIKE '%wearos%'
    )
    OR (
      Lower(title) LIKE '%fitness%'
      AND Lower(tags) LIKE '%wearos%'
    )
    OR (
      Lower(title) LIKE '%wearos%'
      AND Lower(tags) LIKE '%fitness%'
    )
  )
```

B INITIAL AND FINAL DATASETS BY QUERY TERM

Table 3: Initial and final datasets of Stack Overflow posts, by query term. These are based on the posters' tags and titles.

	Fitness		**Health**		**Medical**		**Google-Fit**		**All unique**[1]	
	All	Privacy Related	All	Privacy Related	All	Privacy Related	All	Privacy Related	All	Privacy Related
Android	56	13 (23.2%)	76	15 (19.7%)	12	1 (8.3%)	400	119 (29.8%)	495	129 (26.1%)
iOS	12	3 (25%)	508	128 (25.2%)	5	0	7	1 (14.3%)	526	132 (25.1%)
WearOS	1	1 (100%)	0	0	0	0	5	3 (60%)	5	3 (60%)
WatchOS	1	0 (0%)	84	15 (17.9%)	0	0	0	0	84	15 (17.9%)
All unique[2]	67	16 (23.9%)	620	150 (24.2%)	15	1 (6.7%)	407	123 (30.2%)	1,055	269 (25.5%)

1: Total number of posts tagged or titled for the respective OS. Does not equal the sum of the preceding columns because some posts had multiple health-related keywords.
2: Total number of posts tagged or titled with the respective health-related keyword. Does not equal the sum of the preceding rows because some posts had multiple OS keywords.