An Analysis of Requirements and Privacy Threats in Mobile Data Donations

1st Leonie Reichert
Humboldt University Berlin
reicleon@hu-berlin.de

2nd Björn Scheuermann
TU Darmstadt
scheuermann@kom.tu-darmstadt.de

***Abstract*—In recent years, personal and medical data collected through mobile apps has become a useful data source for researchers. Platforms like Apple ResearchKit try to make it as easy as possible for non-experts to set up such data collection campaigns. However, since the collected data is sensitive, it must be well protected. Methods that provide technical privacy guarantees often limit the usefulness of the data and results. In this paper, we model and analyze mobile data donation to better understand the requirements that must be fulfilled by privacy-preserving approaches. To this end, we give an overview of the functionalities researchers require from data donation apps by analyzing existing apps. We also create a model of the current practice and analyze it using the LINDDUN privacy framework to identify privacy threats.**

1. Introduction

The widespread use of smartphones and wearables has made it easy for users to continuously collect data about themselves regarding their movement and health [25]. For research purposes, people are willing to share data even if it is sensitive [6]. As a result, an increasing number of studies rely on voluntary *data donations* [23]. Existing platforms like Apple's ResearchKit [4] distribute apps designed by researchers to the public. Here, the responsibility to protect the collected data and the privacy of data donors is placed on the shoulders of researchers. However, healthcare facilities and associated researchers can be hacked or compromised. As a result, data breaches have become a frequent occurrence [34]. Legal frameworks such as the GDPR allow the imposing of fines on offenders in case data is lost or misconduct can be proven [13]. Even so, it would be preferable if disclosure of private information could be prevented before it can occur. A large body of research aims at providing technical and statistical privacy guarantees in diverse settings and under various threat models. Tools to this end are, among others, multi-party computation and homomorphic encryption, but also trusted execution environments and local differential privacy. However, these can limit the utility and the expressiveness of the collected data, analysis methods, and final results.

In this paper, we take a look at the requirements that need to be fulfilled by a privacy-preserving analysis platform collecting data from mobile devices. Our contributions are:

- A review of 74 existing data donation apps, identifying common functionalities required by medical researchers.
- A model of the parties involved in mobile data donations, taking into account their motivations and goals, as well as their privacy, security, and functional needs.
- A comprehensive data flow diagram representing an exemplary data donation campaign based on the analyzed apps.
- We analyze threats to privacy, security, and functionality of the existing data donation workflow using the LINDDUN framework. We thereby follow data minimization principles to identify data leaks and privacy threats.

The paper is organized as follows. Section 2 presents the functionalities of existing data donation apps. In Section 3, the relevant parties and their requirements are modeled. Section 4 presents the LINDDUN Framework as well as the system model we used to represent a common data donation campaign using mobile devices. Privacy and security threats that were identified using this model are discussed in Section 5. Related work is presented in Section 6. We close with a conclusion.

2. Research using Mobile Data Donations

Using mobile devices in data collection campaigns for research purposes has many advantages over conventional study designs [23]. Potential participants are easier to reach if the geographic location is not a barrier. It is also a simple way to conduct studies that monitor behavior or habits over time. Additionally, shorter data collection intervals are feasible and built-in sensors allow for objective measurements. Problems with mobile studies arise from the fact that non-sensor data is collected by the study subjects themselves, making it subjective and unreliable in some cases.

2.1. Functionalities used in Practice

To understand what functionalities a privacy-preserving data donation system has to provide, we analyze the existing scientific literature on studies that use mobile devices for collecting sensitive and medical data. To this end, we queried the medical publication platform PubMed [21] for clinical trials with a focus on mobile health using smartphones and apps. We first identified categories of app functionalities. In the next step, for each of the 74 apps we analyzed the provided functionalities. Multiple categories per app were possible.

The literature review revealed that the following functionalities are relevant to researchers (see Table 1 for a quantitative overview). Informing and educating participants about the study and the studied health issue as well as providing self-help information was the most required feature.

Also important was the self-tracking of study participants to collect a history of data on symptoms, triggers, medication, quality of life, and other subjective measures. Here, the focus lies on collecting a small number of measures continuously in regular intervals. Self-tracking is directly linked to providing feedback to the study participant for example about the progress that was made. If an app requires study participants to manually enter values measured by external (unconnected) instruments on a regular basis, the app also falls into this category.

Closely related to self-tracking are questionnaires. However, in contrast to self-tracking, questionnaires allow for more complex questions and a larger number of questions. Here, the focus does not lie on providing feedback to study participants but questionnaires are rather a method for evaluation. Study participants can be asked to fill out questionnaires once or multiple times during the study period.

Half of the analyzed apps provided feedback to study participants using the supplied data. The nature of this feedback was diverse. Some apps visualized the collected data, while others used notifications, for example, to inform participants how many calories they have left for the day. Sending push notifications for example for reminders was a feature used by many apps.

Aside from manual data collection through questionnaires and self-tracking, a third of the apps required study participants to interact with the app, e.g. for experiments, tasks, training, or games. Some apps that fall into this category provided direct feedback to study participants to help them understand the mistakes they made and help them progress.

Another category was apps that used external sensors to collect measurements from study participants. These sensors were paired with the mobile device to directly transfer measurements to the study app. Note, that apps which used off-the-shelf wearables were considered separately. Both approaches for collecting objective measurements turned out to be almost equally as important. Surprisingly, only a few apps required access to the internal sensors of the mobile device such as the gyroscope, the GPS, or the pedometer. Apps that used one internal sensor often also used other internal sensors. The number of apps that tracked usage of apps or online behavior of study participants, in short monitoring the habits in the digital realm, was also low.

Communication turned out to be an important aspect for data donation apps in the medical field. Supporting or facilitating communication with professionals such as doctors, nurses, or medical technicians was a feature of a quarter of the apps. Facilitating communication between study participants/people with the same health issues occurred less often. These two aspects are especially interesting in the context of privacy.

Some studies employ functions described above in combination with conventional or sit-in data collection such as scans, DNA analysis, or ECG. Unlike classical crowd-sourcing, study apps in the medical field often intend to provide a simple form of health care for the participants. Some apps also fall under the category of public health intervention which aims to improve the physical or mental health of the general public.

Category	Count
Informing and educating	45
Self-tracking	44
Reminders and notifications	37
Feedback to participant	29
App interaction	24
Questionnaires	23
Communication with professionals	19
External sensors	10
Wearables	9
Camera	7
Communication between participants	6
Habits in the digital realm	4
Gyroscope	2
GPS	2
Pedometer	2
Sound	1

TABLE 1: This table shows the most relevant functionalities used by data donation apps. A total of 74 apps from PubMed were analyzed.

2.2. Methodology

The literature review above was performed following the PRISMA guidelines for reporting systematic reviews and meta-analyses [19].

The Pubmed search was conducted on the 24. February 2023 and was limited to publications since 2018. In total, the search returned 339 publications. We analyzed the top 100 publications presented by the platform when sorted by relevance. Of these, two publications were duplicates. Another 20 papers were excluded because no full-text version was publicly available. An additional four publications were ignored because they either did not present an app or presented apps not targeting patients or their caretakers. The remaining 74 publications included in our review were all peer-reviewed and published. A total of four publications of these presented two or three apps in the same paper. In these cases, the authors of the respective paper tested the same app with an increasing set of functionalities or in combination with an app for professionals. In our evaluation, we only considered the app for patients or their caretakers in the configuration with the most functionalities.

A reason why only a few of the analyzed apps used internal sensors or tracked online behavior and digital health might be related to the methodology. Only medical apps associated with clinical trials were selected. Clinical trials might not be required for research on mobility and digital health. Research apps that use more internal sensors might also be associated with the field of psychology and computer science. Such publications may be unlikely to be indexed by PubMed.

3. Relevant Parties and their Requirements

As we have seen in the prior section, there is a wide range of functionalities mobile apps can offer for crowdsourced medical research. The motivations of researchers and donors are an important part to understand their security and privacy needs. To this end, we conducted a literature review which we contextualize to model the needs of the relevant parties toward a data donation system. Privacy requirements are derived from literature on data-sharing behavior and the assumptions that parties behave in their self-interest. In the following, the security, privacy, and functional requirements of researchers, donors, app store, and professionals as well as their motivations are discussed.

3.1. Researchers

Researchers want to collect private data from participants for their study through an app on the participant's mobile devices. This *study app* is developed by the researchers or a third party hired by the researchers. It is provided for download on a website or in an app store.

In the first step towards such a study app, the study needs to be designed. While doing so, researchers need the flexibility to select the best study design for their research question. Studies can have various formats such as questionnaires, continuous measurements of specific data types, or assignments to participants where they have to react to or interact with input. Data collection of studies can occur once or continuously by querying participants repeatedly.

When conducting the study, there are several aspects that researchers must consider to obtain meaningful results [23]. A minimum number of participants is required so that statistics become meaningful. To improve the study's statistical validity, the pool of potential participants should be as large as possible. A wide variety of participants is also necessary. Especially in studies with human subjects, it is often important to have participants from diverse demographics so that results do not suffer from selection bias. Conclusions drawn from a study involving only participants from a specific university are unlikely to generalize over the larger population. Here, studies using mobile devices provide an advantage to researchers over conventional study designs as potential participants are easier to reach through advertisements on the Internet [29]. Also, app-based data collection can be performed across large geographic areas if no data is collected in a lab or by a doctor.

Rich data is of particular interest to researchers when trying to understand complex relations. Often a large amount of data points is required by researchers for certain analyses. Modern methods of data collection such as self-tracking apps or wearables also open up new possibilities. However, for data to be useful to researchers it has to fulfill certain qualitative requirements. Incomplete, inconclusive, or illogical responses and outliers have to be identified to guarantee good and stable results. Metrics that can not be objectively measured require special attention during analysis to identify biases. It is also important that the impact of manipulated or bad data is limited. This means that researchers need to be able to filter data and identify bad donors to remove their data.

As researchers are required to follow legal guidelines for data protection such as the GDPR [13], it can be assumed that they aim to protect the collected data from unauthorized third-party access. Researchers also have a self-interest in protecting intermediate results and findings until publication. Proper data privacy can also ensure that researchers retain the trust of participants. This is especially relevant if further studies are to be conducted. On the other hand, the main goal of researchers is to conduct a study and focus on the evaluation. They may not be IT experts so it can be assumed that they do not spend large amounts of resources on privacy or security considerations.

3.2. Data Donors

Study participants, also called *data donors*, take part in a study conducted by researchers. They provide data they collected themselves through the study app. The reasons for data donors to participate in studies are manifold. Apart from financial incentives and simple altruism, data donors might want to improve research on a problem they experience themselves or try to understand the research topic at hand [17], [28]. Data donations can also come from a sense of social duty. Benefiting the public good and a legitimate scientific cause also impact the decision to donate data [17], [28]. In the case of study apps which also function as public health interventions, taking part in a mobile study can be an easy and private way to get help [23]. Especially if the target of the study is mental health, downloading an app might be less stigmatizing than going to a doctor. Also, help is immediately available as compared to the long waiting times common in the health sector.

Privacy is an important aspect for data donors. They will not partake in a study if they expect disadvantages or drawbacks due to their participation [17], [27]. Data donors also want to protect their data from misuse such as unauthorized publishing, selling, or usage for purposes unrelated to the initial study [16], [17]. This can conflict with researchers' interests as they might want to use collected data for further studies, redo evaluations or share it with colleagues internationally [20]. Data donors expect their data to be protected from unauthorized access after they were donated. More generally, data donors want to retain autonomy over their data [1], [17], [24]. They might also want to withdraw their consent to data sharing after data has been donated. In countries where the GDPR applies, researchers are required to provide this functionality [13].

The user experience is also an important aspect when donating data [7], [14]. Data donors require simple ways to donate their data and will not spend a long time trying to find relevant studies or figuring out upload processes. The app needs to be easy to use as donors shy away from burdensome processes [26]. Another usability requirement is that the process of donating data with a mobile device should only take few resources and be finished quickly so that the device can be used again for other purposes. While this seems self-evident, it is a crucial part when looking at computation or communication-heavy mechanisms for privacy protection.

3.3. App Store

It is important not to forget that researchers and data donors need some way to connect. Typically, this is done over a university mailing list or via advertisements. In the context of data donations using mobile devices, the respective app store can fulfill this function. It distributes information about studies and researchers' study apps to potential participants.

The app store is a platform that offers third-party apps to its user base. It is therefore not directly responsible for the apps which are available for download. However, to retain the trust of its user base the app store has a self-interest in ensuring the quality and reputability of published apps. For this reason, the app store enforces requirements on new apps that are uploaded. Among other things, this includes privacy policies as well as malware screening. If it distributes (too many) malicious apps, users might switch to other platforms.

We derive some functional requirements the app store itself needs to satisfy in a data donation system. First, it should make it simple for researchers to announce their study to a wide audience and to address their target demography. It also should inform potential participants about the purpose of the study and about the institution collecting the data. Additionally, it needs to provide a form of authenticity to data donors. This means that the app store should make it easy for the data donor to identify legitimate studies and institutions. To this end, the app store needs to have the trust of both potential participants and researchers. Researchers might fear that their reputation is in danger if they release research apps in an app store with too many bad apps.

3.4. Professionals

As we have seen in Section 2, some studies rely on professionals as a point of contact for donors. These professionals can be hired through the study or they may be the donors' existing primary care providers. They aim to help donors with their medical, psychological, or technical problems. Since it is their job, the fact that professionals work for a certain study is not private. Professionals are unlikely to share personal details with their clients. However, the way they interact with donors as well as how, when, and where they use the study app is sensitive information.

4. Methodology and Model for Threat Analysis

In this section, we present the method used to identify threats. The LINDDUN framework is explained briefly and the analysed system model is described.

4.1. Threat Model

For our privacy analysis, we assume that all parties can behave in a malicious fashion. This includes data donors, researchers, professionals, the app store, as well as external third parties such as hackers and network observers. Hackers gaining access to the infrastructure of a party are mostly equivalent to the party behaving in a malicious manner. Using the systematic analysis threats are identified that result from such behavior. We assume that the operating systems of mobile devices and servers are trusted to not upload data to external parties per default. However, all devices and servers are in danger of being hacked. This can happen for example through a vendor or via a supply chain attack.

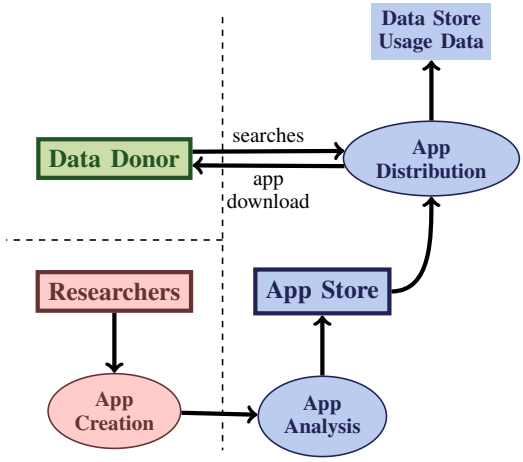

Figure 1: Model of the data donation process from app creation to data donation. Processes under the control of the researcher are highlighted in red. For the donor, green is used and the app store is blue. Trust boundaries are shown as dashed lines.

During the analysis, we followed data minimization principles to identify data leaks and privacy threats. Sensitive data that is not been collected or stored can not be lost.

4.2. The LINDDUN Framework

The LINDDUN privacy engineering framework [9] enables an analysis of systems to identify new and unknown privacy threats. The framework separates threats into the following categories: linkability (L), identifiability (I), non-repudiation (N), detectability (D), disclosure of information (D), unawareness (U), and non-compliance (N). To analyze a system with LINDDUN, it must first be modeled as a data flow diagram. Here, entities, data stores, processes, and data flows of the system are identified. Not all aspects of the system have to be modeled. However, all processes where potentially private data is processed, stored, or transferred should be represented.

In the next step, threats are identified. For each entity, data store, process, and data flow, it is checked if one of the LINDDUN threat categories (see above) applies. The categories of unawareness and non-compliance are only relevant for entities. If a threat category can be applied to an element (for example a data store), the LINDDUN threat tree catalog is used to determine if they pose an actual threat to the system. Each threat tree represents common attack paths for a specific threat category and element type (either entities, data stores, processes, or data flows). Relevant threats which are identified this way are documented. Assumptions made regarding the system are also recorded. The framework provides a methodology

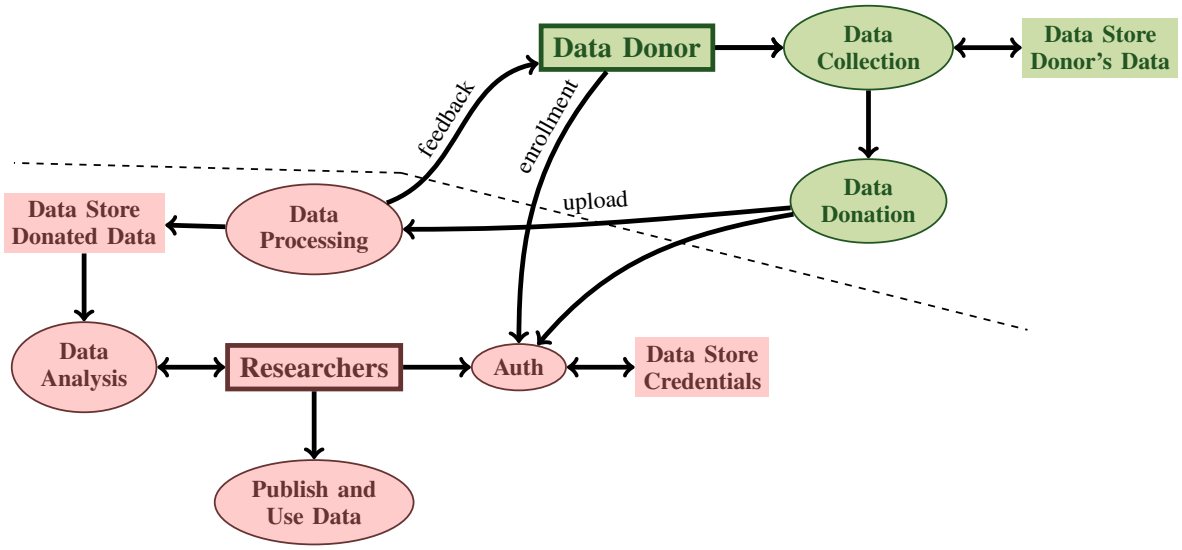

Figure 2: The data flow of a minimal study app. Trust boundaries are shown as dashed lines.

to manage the identified threats. As we only analyze an exemplary system, we do not apply this last step. However, we discuss potential solutions for the identified threats.

4.3. A Model for Common Data Donation Campaigns

Figures 1, 2, and 3 taken together represent the data flow model of a common data donation campaign. For simplicity and better comprehensibility, we split the model into three parts.

Figure 1 shows how the researcher's app is installed via the app store on the mobile device of data donors. Researchers publish their study app via the app store. The app store analyzes new apps to ensure compliance with its policies and to detect if malware was incorporated. While not specifically relevant for privacy, this step is important to ensure security. Data donors search for new apps and download the study app from the app store.

Figure 2 shows the basic flow of data between the researchers and the donors after the app is installed. Using the app, donors collect data on their mobile devices. To donate they upload the collected data to the researchers' servers after authenticating themselves with a username and password. Feedback for the donor can be generated based on the uploaded data. Data are processed, stored, and analyzed by the researchers. The results are published or shared with third parties.

As we have seen in Section 2, a not negligible number of study apps aim to facilitate communication between donors or between donors and (medical) professionals. We modeled both of these flows in Figure 3. Donors can communicate with other study participants and professionals via the researchers' server. We assumed here, that researchers host the communication infrastructure themselves. However, even if this is not the case, and a third party manages this infrastructure, the same privacy threats arise. The communication is stored on the servers, the donors' devices, and if applicable on the devices of the professionals. To initiate conversations, donors, and professionals have to authenticate themselves. Data regarding the communication such as metadata or contents can also be donated by the donors. The donated communication data and data collected from the message exchange server can be used during the researchers' analysis.

We made assumptions during the creation of the model regarding the represented system. First, it is assumed that there is an app signing process. The app store properly detects malicious apps that contain malware or try to trick donors. Communication between entities is properly encrypted even if messages are exchanged via a platform such as the researchers' server. All private keys are only available to the party which uses them and can not be derived by another party.

All data stores are accessible to all internal users. In the case of the researchers, this can be a larger number of people. Collaborations between different entities such as the app store and researchers are not in the self-interest of the app store. However, the app store can assume the role of a researcher.

We do not consider the fact that researchers plan on conducting a certain study as private information. Due to the declaration of Helsinki, it is best practice for medical studies to inform the public about planned studies and their study design before starting [5]. For this reason, it was also assumed that researchers do not make changes to the app while the study is in progress.

Detailed data flows inside the same zone of trust are only modeled when necessary. During the analysis, we only checked and analyzed data flows that transfer information between entities.

5. Threats

In this section, we present the attack surface exposed by the data flow of common mobile data donation campaigns. We present 13 different threats to privacy. At the end of the section, we discuss some additional issues that endanger the function of mobile data donation campaigns.

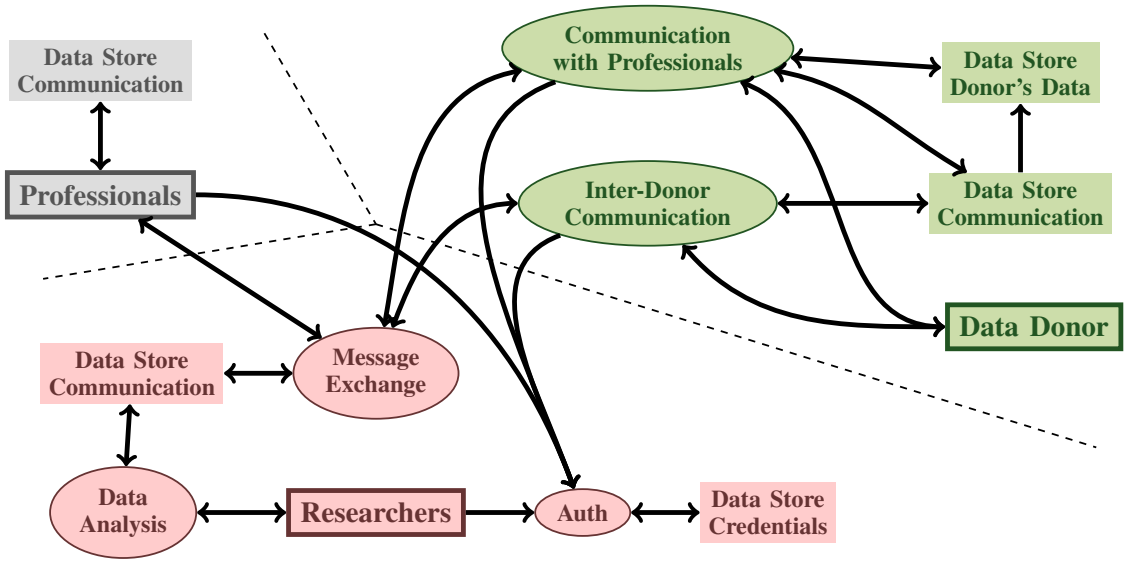

Figure 3: Data flow model for a study app that, in addition to the basic functionalities, allows donors to communicate with one another and with professionals. Trust boundaries are shown as dashed lines.

5.1. Privacy Threats

We identified the following threats to privacy using the LINDDUN threat taxonomy. See Table 2 for a summary.

5.1.1. Unawareness of Data Sharing. The data collected by the study app from donors, their devices, or their communication might diverge from what is expected by the donor. This can happen because donors are unaware certain data is collected, stored, and processed at all. They might also not realize how data is handled. The reasons for this can be diverse. Donors might not read the privacy policies because they are too long [1]. The language used by the privacy policies or the study descriptions might be difficult to understand.

Donors might also provide too much information due to insufficient feedback about which data is collected or due to a lack of user-friendly privacy support. Professionals may also be unaware of the data being collected about them and their communications with donors. Although they themselves are not study subjects, their professional advice, interaction with donors, and messaging behavior are private and can become part of evaluations.

5.1.2. Removal of Data. We assume that researchers follow the GDPR and provide donors and professionals with means to delete their data. However, it becomes more difficult if a person wants to have the data of others deleted because it contains information about them. Once a message has reached the device of another study participant or professional, it can not be ensured that the relevant data is deleted if this is requested. The data might have already been saved as a screenshot or copied to a location where the study app can not delete it.

5.1.3. Non-Compliance. Extensive data sharing might also be caused by an insufficient privacy policy that leaves out details. Furthermore, researchers might simply choose not to comply with the privacy policy and use donated data for other purposes. For example, they might conduct a different study than advertised. They could also use the collected data to get their company going, similar to the Cambridge Analytica case [30]. Here, data collected via Facebook for psychological research was misused for political campaigns.

In studies where donors are only identified through pseudonyms, both researchers and professionals might try to identify data donors. The reidentified private data can be used to harm or break donors' privacy through information disclosure to third parties. Researchers can also harm the privacy of donors and professionals through inadequate anonymization of published results.

5.1.4. Data Extraction. An external adversary can try to extract data from study participants who communicated with others or donated their data. The latter is feasible if the researchers' feedback (see Figure 2) is calculated based on data collected from other donors. If no anonymization is used, it may be possible for the adversary to calculate the responses of other donors by uploading specifically crafted data.

If the study app allows interactions between participants, the attack surface increases. An attacker might pose as study participant in order to communicate with honest participants and extract information. Both content and metadata can be used to link or identify these participants, which can result in medical data being leaked. Honest study participants might not be aware that the receiver of their messages can not be trusted.

We assume that professionals do not reveal private information about themselves in communications with donors. However, the way they interact with donors as well as how, when, and where they use the study app is private. This information can be learned by a fake study participant and used against them.

We have not made any assumptions about how professionals are selected for the study. They might be the participant's primary care provider, an outside professional willing to participate in the study, or they might be associated with the researchers. An adversary might choose to

Threat	Target	Source
Unawareness of Data Sharing	DD	R,H
Removal of Data	DD	DD, P
Non-Compliance	DD,P	R,P
Data Extraction	DD,P	DD
Leaks from Data Stores	DD,P	R,H
Verification of Participation	DD	H
Leaks through the App Store	DD	AS, H
Leaks through Network Traffic	DD	NO
Donor-to-Professional	DD,P	R,H
Donor-to-Donor	DD	R,H
Message Boards	DD	R,H
Message Types	DD	R,H
Deanonymisation from Logs	DD	R,H
Bad Data	R	DD
DDoS	R	DD,H
Fake Researchers	R, DD	R
Off-Brand Studies	R, DD	AS

TABLE 2: This table summarizes the list of threats to privacy and functionality. It lists the parties which are threatened as well as the source. The following abbreviations are used: DD - Data Donor, R - Researchers, AS - App Store, P - Professional, H - Hacker, NO - Network Observer.

impersonate a professional to provide bad advice to study participants and exfiltrate data. To combat the threat of fake professionals, the enrollment process for professionals needs to be well-secured.

5.1.5. Leaks from the Data Stores. All data stores in the model are in danger of revealing private information in case of a leak. A leak can occur through a malicious app on the same device, a hack, or a stolen PIN. Access can also be forced for example by law enforcement or domestic partners. Gaining access to a donor's data stores can reveal their medical information if they already started collecting data as well as their communication history with professionals and other donors. Leaks from the data stores of professionals potentially reveal the health problems of all the study participants they have been in contact with. We assume that data stores that are controlled by the researchers contain mostly the same data as in the data stores of donors and professionals but in larger amounts. Therefore, they need to be properly protected from internal and external unauthorized access.

5.1.6. Verification of Participation. An external party may try to authenticate with a username and password often used by the person. Sadly, password reuse is still a very common occurrence. The attacker could be targeting a specific person using their knowledge of this person. Alternatively, the attacker could be looking for potential targets through a dictionary attack or by using a database of stolen credentials. Measures against such attacks include rate-limiting the number of authentication attempts per account or IP as well as temporarily disabling the IP from making requests.

5.1.7. Leaks through the App Store. App stores collect detailed user profiles including information on their users' search, purchase, and download history. They can use this data to recommend new apps. The collected data can reveal private information such as certain medical predispositions and other private information such as location. Depending on the app store's privacy policy, this data can be sold to third parties. This is especially problematic if users are unaware of this data disclosure or if methods and tools for improving privacy are not user-friendly.

5.1.8. Leaks through Network Traffic. It is well known that network providers collect personal data regarding their customers based on their traffic [11]. This is possible because network providers can monitor the traffic in their network. Even if parts of the packets are encrypted, the routing information is transmitted in clear. By analyzing the flow of traffic, such a network observer can learn who communicated with the researchers' servers which reveals who participated in a certain study. This can again be solved by using cover traffic. However, in the setting of a study app that is only downloaded by interested parties, this might be difficult to realize. Another option to mitigate this data leak is using anonymization networks such as Tor [31] or more powerful but high-latency mix-networks [8]. Covert channels can also be used to hide metadata from a network observer. Here, the real data is hidden beside or inside other data. For example, using domain fronting [32], the IP of the researchers' server can be the same as the one of another highly popular service that is unconnected to the study. The traffic of study participants is therefore hidden.

5.2. Privacy Threats due to Insecure Messaging

In Section 2 we have seen that a surprisingly large number of studies employed some form of communication between donors or with professionals. Due to the large number of attack vectors that become possible when messages are exchanged, we now address this topic in more detail.

Active sharing and interacting with people in similar situations through online communities benefit patients [12]. However, it has been shown that anonymity plays an important role in the decision to share clinical information online [12]. When researchers or a hired third party host a message exchange service for a study, a large amount of communication metadata becomes accessible to them. Since the 2013 Snowden-Leaks, is well known that metadata of communication is private information and can reveal the encrypted contents [18]. This means that metadata leakage also needs to be taken into account when building an environment where data donors can communicate privately or anonymously. Data donors might be willing to donate parts of their communication data but not all of it. Especially if a third party is hired to realize a message exchange service or if an existing platform such as Facebook or any common messaging service is used, metadata collected from the study might be misused.

The adversary in this case is the researcher, a third party that hosts the message exchange service, or a hacker who gained access to the infrastructure.

In the following, we assume here that the message exchange service is set up guided by best practices for using end-to-end encryption and authentication between

communicating parties. This assumption is made as most papers in Section 2 presenting mobile data donation apps analyzed did not go into detail regarding their app implementation. A wide array of approaches for private messaging exist. For example, the Signal protocol [33] supports encrypted communication point-to-point or in groups. It provides confidentiality, integrity, authentication, forward secrecy, and future secrecy in case one of the end devices is compromised for some time. Signal provides some degree of message unlinkability as messages are not authenticated with non-repudiable cryptographic signatures, but instead with ephemeral keys and MACs. This allows only the receiving party to verify authorship. However, the facilitating server can still learn who communicated with each other and when.

5.2.1. Donor-to-Professional. Let us take a look at the case where donors communicate with professionals. Most studies analyzed in Section 2 which provided this feature expected donors to only communicate with doctors when there is an acute problem. The only exception was an app that used the messaging service for doctors to prepare their clients for the next in-person meeting or to assign tasks after the meeting. Both messaging patterns reveal personal information about the donor and in the latter case about the professional. Discovering that a study participant communicated with a professional is fairly easy for an adversary with access to the servers running the message exchange service. The fact that a message exists, even if its contents are encrypted, can reveal that a health emergency occurred.

To prevent an attacker from observing these communication patterns, a system can hide users' messages in *cover traffic*. Cover messages are indistinguishable from real traffic to the observer, but they are sent at random. The pattern and frequency of fake messages need to realistically imitate real traffic. A straightforward approach to cover traffic would be broadcasting encrypted messages to all users [33]. Depending on the number of participants, this is a simple but cost-intensive solution. Some protocols, such as Express [10] and Pung [3], provide metadata-resistant communication with formal guarantees. Similar to protocols for private information retrieval [33], they can be computation or communication intensive.

5.2.2. Donor-to-Donor. Communication between donors can be either be one-to-one or via a message board. When communicating one-to-one, an adversary monitoring the communication on the message exchange server (such as a hacker, the host, or a malicious researcher) can build a social graph of the donors. This can reveal information about which people struggle with similar issues and problems. Knowing further information about an individual in the social graph allows for deriving information about their contacts. However, it can be assumed that study participants do not know each other outside of the study. If they do, they are unlikely to use the study app for communication. So the dangers to privacy resulting from leaking the social graph between study participants are limited, as long as they can not be directly identified. However, revealing the social graph of a network where study participants also connect to people from outside poses a greater risk. This would be the case if existing platforms where study participants already have an account are used to facilitate communications, such as Facebook or commonly used messaging services. Solutions for making donor-to-donor communication private and metadata resistant are the same as those mentioned in the prior section.

5.2.3. Message Boards. Study participants might also communicate with each other via a message board hosted by the researchers or a hired third party. Signal's private groups can be used to realize this feature. To find new groups and conversations to participate in, the general topics need to be visible to all donors and thereby also to the researchers. An adversary with access to the metadata of the message board such as the researcher or a hacker can observe group membership. This information allows for inferring which topics are relevant to a data donor. If a donor receives an (encrypted) message from a certain group or thread, it is likely that the topic discussed is relevant to them. Broadcast protocols are a solution to hide which topics a donor is interested in. However, this only hides the designated receivers. Also, broadcasts can quickly induce performance issues as donors have to download large amounts of data. A less expensive solution building on the idea of cover traffic would be to have donors join random groups and send cover messages to these groups. Similar to one-to-one communication, private information retrieval methods can be used to hide group membership.

5.2.4. Message Types. Some studies analyzed in Section 2 allowed data donors to send images, voice samples, or the configuration of their hearing aid to professionals for examination. These data types differ from standard text messages. The fact that a message with a certain data type was communicated must be concealed as it can leak private information regarding the nature of the conversation. In particular, an adversary on the server should not be able to tell an image from a text message. This can be solved by padding messages. Another option is splitting data into multiple messages with the same length as performed by Tor protocol [31].

5.2.5. Deanonymisation from Logs. Communications via a message exchange service can be linked by a user ID but also via IP address, session ID, client settings, or behavioral patterns. As network connections and login attempts are commonly logged, messages can be linked even if user IDs are pseudonymous. The history of logins can be hidden through anonymous credentials [8]. These credentials allow a verifier to determine that a person is authorized to use a certain service but does not reveal their identity. They are also not cryptographically linkable to previous server interactions. IP addresses can be hidden from the researchers through a VPN, with anonymization networks such as Tor [31], or by using more powerful but high-latency mix-networks [8].

5.3. Threats to the System Functionality

In this section, we discuss additional threats to the data donation model introduced in Section 4.3. These threats were discovered during the analysis but do not threaten privacy but primarily security and functionality.

For example, data donors can manipulate studies by sending bad or skewed data. Donors or an external party can also conduct denial-of-service attacks against researchers' servers, for instance to stop an unpopular study.

Another potential threat is an adversary who poses as researchers from a trusted institution when uploading a study app to the app store. This could be done to trick people into participating or to discredit the respective institution or researchers.

The app store can copy study apps submitted by researchers to create off-brand versions. It can also stop researchers and data donors from collaborating by limiting the distribution of a study app or hiding it. This is a denial-of-service attack that is against the app store's self-interest. We, therefore, consider it unlikely.

6. Related Work

Various publications and surveys exist which analyze the usefulness of apps in health care and research. Schmitz et al. [23] analyzed 36 study apps for health research to evaluate the possibilities and challenges provided by mobile health research applications. However, privacy was not their main target. Aljedaani et al. [2] systematically reviewed the security of research-related mHealth apps. Security is a precondition for privacy, which is the main focus of this work. Nurgalieva et al. [22] analyze health apps that focus on security and privacy. While they do propose best practices, they do not take a systematic approach to model the system or discover threats. Iwaya et al. [15] use the LINDDUN framework to analyze mental health apps from the Google Play Store. Unlike this work, they also do not model the underlying system but instead use static and dynamic analysis to detect potential threats which they then examine with the LINDDUN threat catalog.

A limitation inherent to this and similar works on threat analysis is that it relies on the intuition of the threat analyst, even if a systematic approach is used. This can cause threats to be overlooked.

7. Conclusion

In this paper, we elaborated that the motivations for both researchers and donors to conduct and participate in mobile data donations are manifold and showed that privacy considerations play an important role, especially for donors. Our privacy analysis shows that researchers already collect diverse data via an infrastructure that does not thoroughly protect donors' privacy. Especially studies that allow socializing between donors or facilitate communication with professionals need to pay special attention to metadata leakage. When creating a privacy-preserving alternative, it is important to address these privacy issues but also take the functional requirements into account.

Acknowledgment

The first author would like to thank Florian Tschorsch and Jan Götte for their insights.

References

[1] Esma Aïmeur, Oluwa Lawani, and Kimiz Dalkir. When changing the look of privacy policies affects user trust: An experimental study. *Computers in Human Behavior*, 58:368–379, 2016.

[2] Bakheet Aljedaani and M Ali Babar. Challenges with developing secure mobile health applications: Systematic review. *JMIR mHealth and uHealth*, 9(6):e15654, 2021.

[3] Sebastian Angel and Srinath T. V. Setty. Unobservable communication over fully untrusted infrastructure. In Kimberly Keeton and Timothy Roscoe, editors, *12th USENIX Symposium on Operating Systems Design and Implementation, OSDI 2016, Savannah, GA, USA, November 2-4, 2016*, pages 551–569. USENIX Association, 2016.

[4] Apple Inc. ResearchKit. https://developer.apple.com/design/human-interface-guidelines/researchkit/overview/introduction/, 2022. Accessed: 2022-05-03.

[5] World Medical Association et al. WMA Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects. *Jama*, 310(20):2191–2194, 2013.

[6] Juliana Chen, Adrian Bauman, and Margaret Allman-Farinelli. A study to determine the most popular lifestyle smartphone applications and willingness of the public to share their personal data for health research. *Telemedicine and e-Health*, 22(8):655–665, Aug 2016.

[7] Mick P Couper, Christopher Antoun, and Aigul Mavletova. *Total survey error in practice*, chapter 7. John Wiley & Sons Hoboken, NJ, 2017.

[8] Diaz, Claudia and Halpin, Harry and Kiayias, Aggelos. The Nym network. https://nymte.ch/nym-whitepaper.pdf, 2021. Accessed: 2023-03-03.

[9] DistriNet Research Group, KU Leuven. LINDDUN privacy engineering. https://www.linddun.org, 2020. Accessed: 2022-11-19.

[10] Saba Eskandarian, Henry Corrigan-Gibbs, Matei Zaharia, and Dan Boneh. Express: Lowering the cost of metadata-hiding communication with cryptographic privacy. In Michael Bailey and Rachel Greenstadt, editors, *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021*, pages 1775–1792. USENIX Association, 2021.

[11] Federal Trade Commission. FTC staff report finds many internet service providers collect troves of personal data, users have few options to restrict use. https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-staff-report-finds-many-internet-service-providers-collect-troves-personal-data-users-have-few, 2018. Accessed: 2023-05-08.

[12] Jeana Frost, Ivar E Vermeulen, Nienke Beekers, et al. Anonymity versus privacy: Selective information sharing in online cancer communities. *Journal of medical Internet research*, 16(5):e126, May 2014.

[13] GDPR.EU. What are the GDPR consent requirements? https://gdpr.eu/gdpr-consent-requirements, 2022. Accessed: 2023-03-07.

[14] Marieke Haan, Peter Lugtig, and Vera Toepoel. Can we predict device use? An investigation into mobile device use in surveys. *International Journal of Social Research Methodology*, 22(5):517–531, 2019.

[15] Leonardo Horn Iwaya, M Ali Babar, Awais Rashid, et al. On the privacy of mental health apps: An empirical investigation and its implications for app development. *Empirical Software Engineering*, 28(1):2, 2023.

[16] Yann Joly, Gratien Dalpé, Derek So, et al. Fair shares and sharing fairly: A survey of public views on open science, informed consent and participatory research in biobanking. *PLOS ONE*, 10(7):1–20, 07 2015.

[17] Florian Keusch, Bella Struminskaya, Christopher Antoun, et al. Willingness to participate in passive mobile data collection. *Public Opinion Quarterly*, 83(S1):210–235, 2019.

[18] Susan Landau. Making sense from snowden: What's significant in the NSA surveillance revelations. *IEEE Security & Privacy*, 11(4):54–63, 2013.

[19] Alessandro Liberati, Douglas G Altman, Jennifer Tetzlaff, et al. The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. *Annals of Internal Medicine*, 151(4):W–65, 2009.

[20] Peter Murray-Rust. Open data in science. *Nature Precedings*, pages 1–1, 2008.

[21] National Library of Medicine. Pubmed. https://pubmed.ncbi.nlm.nih.gov/, 2023. Accessed: 2023-03-03.

[22] Leysan Nurgalieva, David O'Callaghan, and Gavin Doherty. Security and privacy of mhealth applications: a scoping review. *IEEE Access*, 8:104247–104268, 2020.

[23] Hannah Schmitz, Carol L Howe, David G Armstrong, et al. Leveraging mobile health applications for biomedical research and citizen science: A scoping review. *Journal of the American Medical Informatics Association*, 25(12):1685–1695, Dec 2018.

[24] LH Segura Anaya, Abeer Alsadoon, Nectar Costadopoulos, et al. Ethical implications of user perceptions of wearable devices. *Science and Engineering Ethics*, 24:1–28, 2018.

[25] Alexander Seifert and Corneel Vandelanotte. The use of wearables and health apps and the willingness to share self-collected data among older adults. *Aging and Health Research*, 1(3):100032, 2021.

[26] Henning Silber, Johannes Breuer, Christoph Beuthner, et al. Linking surveys and digital trace data: Insights from two studies on determinants of data sharing behaviour. *Journal of the Royal Statistical Society Series A: Statistics in Society*, 185(S2):S387–S407, 2022.

[27] Eleanor Singer. Exploring the meaning of consent: Participation in research and beliefs about risks and benefits. *Journal of Official Statistics*, 19(3):273, 2003.

[28] Anya Skatova and James Goulding. Psychology of personal data donation. *PLOS ONE*, 14(11):e0224240, 2019.

[29] Naomi F Sugie. Utilizing smartphones to study disadvantaged and hard-to-reach groups. *Sociological Methods & Research*, 47(3):458–491, 2018.

[30] The New York Times. Cambridge Analytica and Facebook: The scandal and the fallout so far, 2022. Accessed: 2022-07-22.

[31] The Tor Project, Inc. TOR project. https://www.torproject.org, 2022. Accessed: 2022-11-21.

[32] Tor Blog. Domain fronting is critical to the open web. https://blog.torproject.org/domain-fronting-critical-open-web, 2018. Accessed: 2023-03-03.

[33] Nik Unger, Sergej Dechand, Joseph Bonneau, et al. Sok: Secure messaging. In *2015 IEEE Symposium on Security and Privacy*, pages 232–249. IEEE Computer Society, 2015.

[34] UpGuard, Inc. 14 biggest healthcare data breaches. https://www.upguard.com/blog/biggest-data-breaches-in-healthcare, 2023. Accessed: 2023-03-06.