30

Understanding User Privacy Preferences for mHealth Data Sharing

Aarathi Prasad, Jacob Sorber, Timothy Stablein, Denise L. Anthony, and David Kotz

CONTENTS

30.1 Introduction

Mobile health (mHealth) technologies, including health text messaging, mobile phone apps, remote monitoring, wearable devices, and portable sensor devices, have grown rapidly in the past 5 years and are expected to play an important role in improving access to health information, resources, and clinical care. mHealth devices can be used to monitor activities (Fitbit [9]), sleep (Wakemate [35]), emotions (Affectiva [1]), vital signs like blood pressure (Withings blood pressure cuff [38]), or fetal conditions (HeartSense [14]). Users can collect their personal health and physical and social activity information and upload it to a vendor website, social networking website, a personal health record (Microsoft HealthVault [21] or, formerly, Google Health [11]), or a health-provider-operated electronic health record (EHR). Once the data is uploaded, users can share the information with health providers who help diagnose their illness or monitor their treatment. Family and friends can motivate them as they work toward a healthier lifestyle. People can also

share their experiences with their peers (e.g., others suffering from similar medical conditions) and provide support while in recovery [10]. New mHealth technologies might also enable users to share health information with pharmacists, insurance companies, drug companies, employers, or others involved in their health care.

Studies of mobile location tracking applications show that at least some users vary in their willingness to share depending on the benefits [25], place and context [3], or by recipient [7]. We set out to examine whether similar variations in patterns of use existed with mHealth technologies. We conducted exploratory focus-group discussions to gain preliminary understanding about users' privacy preferences. We discovered that if users are not comfortable with the way their information is being collected or shared, they may not use mHealth technologies at all, or use them in limited ways, thereby reducing the potential for mHealth technologies to improve health and health care. In addition, users' preferences for collecting and sharing information are likely to vary depending on the types of information, the types of recipients, and how the information was to be used.

Prior work, including the preliminary study we mentioned earlier, studied users' sharing behavior through focus groups, surveys, and interviews; in these cases, study participants either were given hypothetical scenarios about health data management, had a brief opportunity to use a health device, or were assumed to have experience with collecting and sharing health information. People's stated privacy preferences and concerns, however, may differ from their actual sharing behavior [6,16]; thus, it is important to examine actual sharing behavior with real mHealth devices that can share real data with real people.

To study how new mHealth users share different types of personal information with different recipients over time, we conducted a user study with $n = 41$ participants. To the best of our knowledge, ours is the first study that explores users' privacy concerns by requiring them to *actually* share the information collected about them using mHealth devices; our subjects could decide whether to share the information and if so, how much information to share with others. The device we used for our study is one of the most popular devices, a fitness device called Fitbit. None of the participants in the user study had ever used a Fitbit prior to the study. At least 10 participants had previously used a pedometer but had never uploaded its data to a website or online application.

In this chapter, we first describe users' privacy preferences based on the results of the focus group. Then we use the findings from our user study to answer the following questions:

- Did the participants share different types of personal or sensed information more or less frequently?
- Do participants' decisions about sharing health information differ across types of sharing partners (family members, friends, third parties, and the public)?
- Does sharing behavior change over time; are participants' privacy preferences dynamic?

We confirmed that people's sharing behavior depends on the type of information being shared and the sharing recipient. Our results showed that the participants were generally less willing to share personal demographic information or context information collected by the mHealth device than about sharing the health information that the device is meant to collect. Our results also showed something surprising—study participants were more willing to share some information with *strangers* than with their own family and

Downloaded by [David Kotz] at 11:35 20 December 2014

friends; among strangers, they were more willing to share some information with specific third parties than with *the public* at large. We also confirmed that people's privacy behavior is dynamic; participants' sharing behavior changed during the course of our study. It is important to understand people's willingness to share, so that mHealth devices can provide patients with the controls to share their information in a manner such that they can enjoy the benefits provided by the device without disclosing more information than is necessary.

In this chapter, we use the term *user* to denote the mHealth device user and *sharing partner* to denote the person(s) with whom the user shares her fitness information.

Downloaded by [David Kotz] at 11:35 20 December 2014

30.2 Focus Groups

We conducted exploratory focus-group discussions to gain a preliminary understanding about users' privacy preferences. The focus groups were approved by Dartmouth's Institutional Review Board. We conducted eight focus-group sessions with 3–7 participants each, who were college students (aged 19–30), hospital outpatients (aged 80–85), or residents of a retirement community (aged 65–100). Each focus group lasted for not more than 90 min and all the participants were paid for their time. We chose these groups since we wanted to talk to users who have some health experiences—some who have been recently hospitalized and others who are monitored continuously outside the hospital—and users who have limited health-care-related experiences.

Since mHealth devices are not yet common, the focus-group participants were presented with hypothetical scenarios where mHealth devices were used. There were four scenarios in which an mHealth device was used to collect a user's personal information (measuring medication intake, diet and exercise, location or social interactions); the collected data was uploaded to a private website and then shared with health providers, family, or friends. The scenarios for the young and the old differed in the age of the protagonists and their medical condition but were similar in every other aspect like the information collected and the manner in which it was collected, stored, and shared; the scenarios are available in the technical report [26].

We presented each scenario to the participants, after which they were asked about the advantages and disadvantages of using mHealth sensors in that scenario. They discussed their concerns regarding the collection of the particular health information in each scenario and whether there were certain times and places when they did not want to collect that information. The participants talked about why they would want to share certain health information types with health providers, caretakers, family members, and friends. They also raised some concerns regarding storage and transmission of the collected information.

We recorded the discussions. We coded the discussions manually and grouped the statements into categories—privacy concerns were broadly classified into three categories and challenges for reducing privacy concerns were classified into seven categories.

30.2.1 Privacy Concerns

Unintended disclosure. One student brought up the issue of how someone could make sensitive inferences from seemingly trivial information, "You can draw some kind of analogy or trend [from the collected health information] that could be misused." Some participants

were worried about the information being sent to a website, via the Internet. A student was concerned about "the level of encryption and transmission [of information from] the device and [to] the website. Also, how is [the website] categorizing [the user]? His name, date of birth, social security number?" Another student was more open to using the device if it did not have any Internet connectivity; he said, "If you connect to the Internet, *I* start to become skeptical in terms of privacy, the information has the ability to leave the device." Another student was worried about losing the device; she asked, "What if you misplace the device? Is there security on the device."

Misuse of information. A majority of the participants were worried that their personal information might be used by people they had not intended to share it with. A few students were worried that potential employers might not hire them, if they wear the device to a job interview. Some participants were worried about discrimination by insurance companies. After hearing the scenario about Jack who uses an mHealth device to track his medication intake, an elderly participant said, "Insurance companies might not want to insure Jack if he is lax about taking his medication." A student was worried about the information being misused by the government; he said, "I'm not too into the government knowing where I am going and what I am doing." Some participants were worried about their information being used for marketing purposes. A student commented, "Wouldn't people want [our personal information] for other things to sell products and to target [a specific] audience?" Another student was concerned about stalkers, she said, "If someone can hack into the website, then someone can track you like a stalker."

Change in trust relationships. A student was concerned about using a device to monitor patients' adherence to their treatment because it meant that "the doctor didn't trust [the patients] to be honest." An elderly participant said that he would not use the mHealth device unless he trusted his doctor; he said, "The more the information you collect, the more trust you need to have that information is secure." A few students felt that constant patient monitoring would improve the doctor–patient relationship; according to one student, "They are working together, it's like a partnership." Another student pointed out that "[The device] *holds* [the patient] accountable a lot more, compared to when she could lie to her doctor and say that [the treatment] is not working." Some elderly participants were concerned about sharing information with their family. One said, "[Suppose you share sensitive information] with one family member, then there is a family gathering and they discuss [the medical situation]." Another elderly participant said that if a patient's wife was to constantly monitor his location and his activities, "it would destroy the trust [he had] in [his] wife." One elderly participant was open to sharing his information only with his daughter, since she took care of him. One student, on the other hand, pointed out that sharing health information with family would lead to "more arguments in the family." Most students agreed that they would trust their doctor with their health information more than their family. One student said, "If I like had a medical condition, I would feel obligated to talk to a doctor but less obligated to talk to a sibling about it on a daily basis." Most students were not open to sharing their health information with their friends and some felt that if they had to share their health information with their friends, they would trust only their closest friends.

30.2.2 Benefits versus Privacy Trade-Off

Some participants wanted to use the devices, because they understood the benefits of the device, since they or their family or friends had suffered from a similar condition and they agreed that they would wear the device at all times. One student said, "If I'm being tracked and for my own benefit, I'll keep it on whenever I can and as long as it is with

Downloaded by [David Kotz] at 11:35 20 December 2014

my doctor and utmost with my family." Another student said, "If you want [the device], it makes you a bit more willing to put more information up there. If it is something that is forced upon you, you might not respond well to it." A few participants felt that they would not be concerned about privacy if they were using the device to get better; one student pointed out, "If I was really concerned about the disorder, I think I would definitely not be concerned about the privacy."

30.2.3 Challenges to Reduce Privacy Concerns

Need for clarity of information collection and usage. Most participants expressed the need to be aware of what information was being collected by the device. A student pointed out that his privacy concerns depended on what information was being collected; he said, "[If the device takes] into account details of someone's life, that is going to affect the way they act and get into privacy issues."

Ignorant users. One student could not understand why anyone would steal or misuse her health information. A user who cannot comprehend the consequences of a privacy breach might end up disclosing more information than necessary.

Providing adequate control to the user. All the participants wanted the control to decide what information to share and with whom and under what circumstances. Some of them felt that having the control to turn the device on or off or to take the device off would defeat the purpose of using the device. After hearing the scenario about a patient using an mHealth device to track his medication intake, one student said, "If you have to remember to turn it on or off, it becomes optional. It's like taking your medication in the first place." Another student wanted the control to delete some information collected by devices before it was shared with others. An elderly participant said she wanted complete control over all the decisions she made; she said, "People [at the retirement home] *l*ike to have control over their lives as much as possible. Unless I became incapable, I will consider everything intrusive unless I can choose what to do with the information."

Flexibility of privacy controls, based on recipients. We discovered that privacy concerns varied with the data recipient. One student wanted to share the data with someone who could help him understand the data that was collected. A few students said they would share their information only if it could not be traced back to them by strangers; one student said, "I wouldn't mind if [my information] wasn't associated to my name in any way, if I was purely a number." Some participants wanted to share information only with sharing partners who they felt could offer some medical help. One student said sharing decisions "depend on kind of help [family and friends] can give based on the position I'm in." Most participants were more open to sharing their health information with doctors than with their family. One student said, "Your doctor has your health in mind. Your parents have, like, so many other interests in mind," while another student said, "What the parents view as social norm, whereas the doctor views it from medical point of view." On the other hand, one elderly participant said, "We want to be independent [from our family] as long as we can. We just want to be dependent on people [at the retirement home]. But I will be okay sharing it with caregivers." One elderly participant said, "I didn't want my wife to know [about my stroke] since I didn't want her to worry, since she was [out of town]," while another elderly participant said, "I would tell her, [she] would worry less if [she] knew early." According to a few students, health information should not be shared with family unless the patient could not make decisions on their own, for example, if the patient was a minor or an elderly person.

Downloaded by [David Kotz] at 11:35 20 December 2014

Flexibility of privacy controls, based on information type. We discovered that privacy concerns varied with the type of information that was being collected and shared. After hearing about the different scenarios, most participants felt that they would be more open to sharing their diet and exercise information with others than medication, location, and social interactions, though one student said that even though she would base her sharing decisions on who the information was being shared with, she would be most concerned about sharing her location and her diet with others. Some students said that collecting information about location and social interactions would be desirable if the patients had a criminal record, if they were suspected to be terrorists or if they were in prison.

Laws. A few students were concerned about privacy laws. One student was worried about their complexity, "Some things are difficult to be explained to people, especially the huge privacy laws," while another student was worried whether his information will still be protected when laws change in the future, "Laws change. [Suppose] right now, no third party can [access the information collected using the mHealth devices]. What if ten years down the road, the supreme court says [the third parties] have the right?"

Device form factor. A majority of the students said that they would not wear the device if it was conspicuous because they were worried about being judged by others. A student said, "If it's like conspicuous, you know, people would always be like asking, what does that device do?" Elderly participants were concerned about physical comfort (one participant gave an example of his watch: "I used to wear it 24 hours a day, now it keeps me awake, so I take it off but forget to put it on") and they did not want the device to disrupt their normal routine, with notifications.

Downloaded by [David Kotz] at 11:35 20 December 2014

30.3 Fitbit User Study

During the focus groups, the participants voiced concerns that they thought they might have about the collection and sharing of their health information, based on the hypothetical scenarios that we presented to them. To better understand what concerns people might have when they actually share their health information, we conducted a social experiment to examine users' decisions to share particular types of information with various types of information recipients (and requesters) over a 5-day period. The participants carried a device that collected their personal health information and shared the collected information with family, friends, and third parties. From the focus groups, we found that exercise was considered to be the least sensitive type of personal health information when compared to medications, location, and social interaction. So we decided to conduct a user study where users would use a device that collects exercise information, to understand whether users would have privacy concerns when sharing seemingly insensitive information like steps, calories, and sleep.

30.3.1 Study Design

During the study, users were asked to carry a Fitbit [9], a popular mHealth device that uses an accelerometer to estimate a user's calories burned, steps taken, distance traveled, and sleep quality. During the 5 days of the study, each subject was asked to wear the Fitbit at all times, except when swimming, bathing, or any time they felt uncomfortable wearing it. They were asked to upload the collected data at least daily to fitbit.com. Unfortunately,

TABLE 30.1
Participants

	Male	Female	Total
Students	8	13	21
Working	5	7	12
Retired	0	8	8
Total	13	28	41

fitbit.com only provided users with limited coarse-grained data sharing options, and no mechanism for monitoring sharing behaviors. So, we developed a custom web interface that displayed both uploaded Fitbit data and personal traits and allowed users to share data with others. The participants used this interface (instead of fitbit.com) to view their data and make sharing decisions, throughout the study.

The goal of the user study was to understand people's willingness to share their personal health/fitness information with family, friends, third parties, and the public. Previous work has shown that young and old people have different views about sharing health information [8,15,34]. So, we recruited a sample of college students, working adults, and retirees for the user study. We recruited 21 undergraduate students, 12 adult workers from the local area including Dartmouth employees, and 8 female elderly residents of a local retirement home, as shown in Table 30.1. It was not an aim of the study to understand the influence of gender and occupation on privacy concerns, so we did not focus on the distribution of participants among these categories. The recruitment flyer presented the study as a study of a new device to help individuals trying to lose weight and/or improve fitness and health. To avoid self-selection bias, the participants were not told that the study was about privacy. The subjects were required to own a computer, to be injury-free, and to be able to walk and carry the device with them during the 5 days. Study participants were paid for their time.

We did not retain any sensitive information, like the participants' fitness information collected using the Fitbits, after the study; we stored only the sharing settings that they chose. Study participants were debriefed after the study to make them aware of the deception used in the study and to inform them that the goal of the study was to understand their privacy concerns and not just to collect their activity data and that we shared their data only with the people they chose as their sharing partners. This study, including our use of deception and subsequent debriefing procedure, was approved by Dartmouth's Institutional Review Board.

To study participants' willingness to share secondary information, apart from the primary sensed information, we also collected other related personal information about each participant, including his or her age, gender, height, weight, health goals, overall activity level, and academic major. Henceforth, we refer to these seven characteristics as *traits*.

To understand how the participants share information with real people, we asked them to select family members and friends to receive their shared information. Throughout the study, the participants also received requests to share data with specific third parties. These specific third parties represent academic researchers, medical labs, private companies, and the government. The third parties were real, but the requests were fake (e.g., one of the e-mail requests was from a fictitious group of students at Harvard University, requesting activity data for use in a machine-learning class). Each participant also had a *public profile* available on the website with their Fitbit data; we told

Downloaded by [David Kotz] at 11:35 20 December 2014

the participants that this profile was visible to anyone who had the URL (unless they changed the setting, as described in the following).

The website provided opt-out sharing settings; by default, all the collected information was shared in the finest detail unless the participants changed the settings to *opt-out* of sharing. We used an opt-out policy (instead of opt-in) to be consistent with the majority of online applications now available in which the default privacy setting is to share, with the option to *opt-out* of sharing. We understand, though, that people's sharing decisions are influenced by default settings [31]. Although we agree that opt-in settings give more control to the user, for our study, we used opt-out to provoke action (visit website and change settings) that we could observe among those with privacy preferences.

We wanted to study people's willingness to share their information, and not how they adapted to the device and controls on the website. So, the study was divided into two phases: a learning phase, in which participants were given 2 days to get used to the device and website, and the study phase, in which we observed participants' sharing settings during days 3–5 of the study.

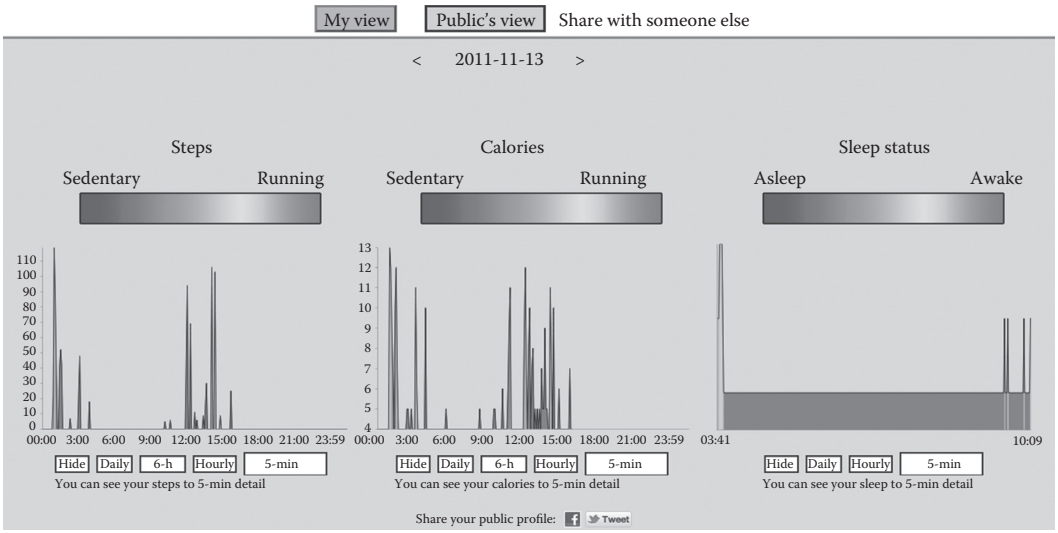
The learning phase—day 1 and 2. The researchers met with the participants, individually, on both days to answer any questions they had about using the device and the website. On the first day of the study, the participants were asked to select at least one family member and two friends with whom to share their information. An e-mail was sent to these sharing partners, informing them about the study and asking them to be a part of the study.

On the second day, we told the participants that their information would be shared with their family and friends from the next day onward and that they could decide, by using the controls on the website, whether and what they wanted to share with their family members and friends. We also informed the participants that over the next few days, they might get requests from third parties to share their information but that they could use the controls on the website to limit sharing of their information; they were required to visit the website for each third-party request so that we could observe their sharing choices. Similarly, we informed them that their data on the website would be open to the public but they could use controls to opt-out of sharing. We did not tell the participants that the third-party requests were fake or that their information was not actually exposed to the public.

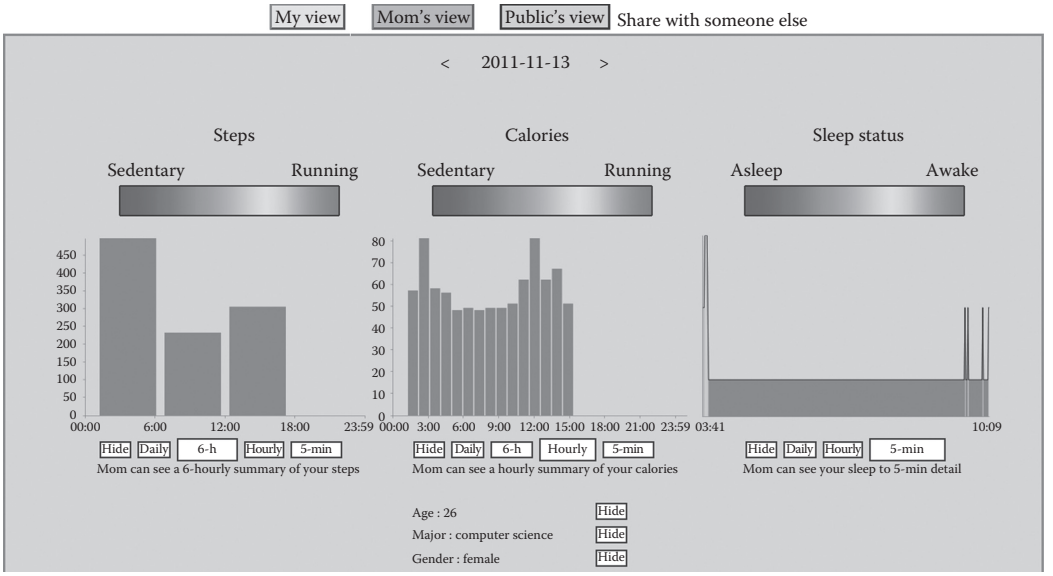
The sharing phase—days 3–5. On the third day of the study, an e-mail was sent to the family members and friends with a link to a webpage where they could see the participant's shared Fitbit information and traits. Throughout the study, the participants could change the sharing settings for each type of information and for each sharing partner. The Fitbit-collected activity data (i.e., steps, calories, and sleep) could be shared in 5 min, hourly, 6 hourly, or daily summaries, or it could be not shared at all. By default, activity data was shared at the maximum setting, that is, 5 min granularity. The participants were also able to share or hide their personal traits (age, height, weight, gender, activity level, health goals, academic major), independently by type and for each sharing partner. The participants also received e-mails everyday during the 5-day period of the study, containing status information. From the third day of the study onward, these mails explained who was receiving their information and what sharing settings they had chosen for each information type for each sharing partner. The message also contained a link to the site where they could change these settings at any time.

The web interface showed different views of the same information. The default view, shown in Figure 30.1a, was the participant's view. The interface also had views corresponding to each sharing partner (see Figure 30.1b). On these views, the participant could decide what information she wanted to share with her sharing partner, make changes with the click of a button, and observe exactly what her sharing partner will be able to

Downloaded by [David Kotz] at 11:35 20 December 2014



(a)



(b)

FIGURE 30.1
Screenshots of views on the study website. (a) Own view. (b) Sharing partner's view (Mom's view).

see; the goal of our website design was to reduce the disconnect between sharing controls and the information being shared.

The e-mails from third parties, requesting to access participant information from the website, including all information and their e-mail addresses, were sent by us as if from six different organizations/groups. Each third-party e-mail explained who the group was and why they wanted the data. The groups identified were college students, a research lab, a government agency, an engineering company, a wellness institute,

Downloaded by [David Kotz] at 11:35 20 December 2014

and a pharmaceutical company. Here, we do not examine differences in willingness to share between these different types of third parties. Instead, we analyze sharing behavior with all third parties as a category to compare to other sharing partner categories (family, friends, the public). We told the participants that the data on the website to be shared with third parties was not anonymous (e-mail address was shared), but that their e-mail address would be used by the third parties only if the researchers needed to contact them. The e-mail address was, however, not visible on their public profile and hence not shared with the *public*. The order of third-party e-mail requests was randomized, and the number of requests varied across the days (three on the third day, one on the fourth, and two on the last day). We did not actually share the participants' data with any third-party organizations, but crafted the messages to be as believable as possible.

We monitored participants' website activity through logs, which recorded when they logged in, when they looked at their own data view or the views of their various sharing partners, and when they changed the sharing settings. To understand the reasons behind participants' sharing behavior, we conducted poststudy interviews in which we asked the participants several questions: whether they ever took off the device to hide any information, whether they ever changed the sharing settings and why, and whether they fell for our deception (that the study was really about privacy-related behavior and that no data was actually shared with the public or with third parties). After the interviews, we revealed the deception and explained to them that the goal of the study was not to collect their fitness information, but to observe their sharing behavior. We recorded the interviews, then transcribed and coded them manually.

Downloaded by [David Kotz] at 11:35 20 December 2014

30.3.2 Analytic Methods

We conducted quantitative analysis of the website logs to understand the participants' sharing settings and a qualitative analysis of the poststudy interviews to give us insight into the reasons for their sharing behavior. We use the analysis to answer the questions listed earlier.

30.3.3 Measuring Sharing Behavior

To measure participants' willingness to share their information with a group of sharing partners, we defined a *sharing score* for each participant. The sharing score was computed as follows:

$s(u, p, t, d)$ is the setting chosen by user (u) on day (d) when sharing information type (t) with sharing partner (p). For steps, calories, and sleep, the setting can be 0, 1, 2, 3, or 4, which corresponds to the five possible settings: hide, share daily summary, share 6 hourly summary, share hourly summary, and share 5 min detail, respectively. For the other information types, the setting can be either 0 (hide information) or 1 (share information). By default, $s(u, p, t, d) = 4$ for $t = \{\text{steps, calories, sleep}\}$ and $s(u, p, t, d) = 1$ for $t = \{\text{age, gender, health goals, height, activity level, academic major, weight}\}$. That is, the default setting is the maximum sharing setting. We normalize each score by dividing by $\max(t)$:

$$\max(t) = \begin{cases} 4 & \forall\, t \in (\text{steps, calories, sleep}) \\ 1 & \text{otherwise} \end{cases} \tag{30.1}$$

To represent the amount of information shared with a category of sharing partners (i.e., family, friends, third parties, the public), we computed an overall sharing score for that category, labeled as *group sharing score*. Equation 30.2 defines the group sharing score for participant (u) on day (d) as the mean of all sharing scores for type (t) for each member of the sharing partner group (g). For example, if a participant identified two friends then the friend group sharing score for weight would be the mean of the sharing scores for weight for the two friends:

$$\text{grpscore}(u, g, t, d) = \frac{1}{|g|} \sum_{\forall p \in g} s(u, p, t, d) \tag{30.2}$$

To measure how personal traits were shared, we also computed a combined sharing score for traits, which is the average of the sharing scores of all the personal traits, labeled *traits*.

We focus most of our analysis on two snapshots: the initial sharing score, grpscore($u, g, t, 2$) for the last setting on day 2 for each type t, and the final sharing score, grpscore(u, g, t, 5). We normalize each score by dividing by max(t), on day 5. Unless mentioned otherwise, we used t-tests to compute the difference between normalized sharing scores, to understand how different information types were shared with the different groups; paired sample t-tests were used to compare different behaviors of a single subject, whereas independent sample t-tests were used to compare one subject to another. We used *analysis of variance* (ANOVA) post hoc testing using Bonferroni's method to compare the sharing behavior of students, employees, and retirees; whereas the t-test is used to compare the means between two groups, ANOVA is a statistical procedure used to compare means between three or more groups.

Downloaded by [David Kotz] at 11:35 20 December 2014

30.4 Results

We present in the succeeding text the results from the quantitative and qualitative analysis. We highlight only some of the important results in this paper; full results are available in the technical report [26].

30.4.1 Information Sharing Analysis

Twenty-seven of the 41 participants identified both a family member and friends with whom to share information. Among the 27 participants, the mean number (and standard deviation) of family members and friends that the participants chose were 1.26 (0.44) and 2.11 (0.5), respectively. Two participants did not identify a family member, but did identify friends, while 11 participants did not select any friends or family members (the reasons given by these respondents included privacy concerns, not wanting to bother them, and expectation of lack of interest, as discussed in Section 30.4.2). These 11 participants, however, were not considered when we computed sharing scores for friends and family. Similarly, when comparing sharing scores between family and the public, we used the scores of all participants who selected at least one family member.

TABLE 30.2

Mean and (Standard Deviation) of Final Normalized Sharing Scores for Family

Information	Family
Steps	0.96 (0.19)[a]
Calories	0.96 (0.19)
Sleep	0.96 (0.19)
Activity	0.93 (0.26)
Age	0.96 (0.19)
Gender	0.93 (0.26)
Goals	0.86 (0.36)[a]
Height	0.93 (0.26)
Major	0.95 (0.21)
Weight	0.84 (0.36)[a]

[a] Sharing score for sensed information (steps, calories, and sleep) is significantly higher than for weight and goals, sharing score for weight is significantly less than the score for most personal traits (age, gender, academic major, height, and activity level), and sharing score for goals is significantly less than the score for age, $p \leq 0.1$.

Downloaded by [David Kotz] at 11:35 20 December 2014

Did the participants share different types of personal or sensed information more or less frequently? Table 30.2 shows the final normalized sharing scores for family used to evaluate within-subject differences in sharing different types of information.

Table 30.2 shows that with family members, the study participants shared weight and health goals less than age, academic major, activity level, and the sensed information (steps). It is not surprising that the participants were willing to share obvious information known to their family members such as age and gender, but at least some participants seemed to consider information like weight and health goals as more private. In the post-study interviews, some participants were reluctant to share this information because they worried that family members might judge them and even reprimand them. A web interface might influence sharing behavior, but in the web interface we built, however, sensed information was more prominent than personal traits, so the sensitivity of weight and health goals had nothing to do with the interface layout.

Do participants' decisions about sharing health information differ across types of sharing partners (family members, friends, third parties, and the public)? Table 30.3 shows the normalized final group sharing scores for sensed information (steps, calories, sleep), traits (the combined score), weight, goals, and academic major across three comparison categories: family versus friends, family versus public, and public versus third parties. Recall that a score of 1 implies that the information has been shared to its maximum with all the sharing recipients in that group.

More information shared with family than friends. Subjects shared weight with family significantly more often than with friends. The sharing scores for friends were marginally less than that for family members for all other information types as well, but the differences are not statistically significant. From the interviews, we learned that some participants were more concerned about sharing their information with their friends because they were worried of being judged by their friends more than by their family, especially in the case of students, since they see their friends every day.

More information shared with family than with the public. Table 30.3 shows that the participants shared more information about their steps, calories, and sleep with family than with the

TABLE 30.3

Final Normalized Sharing Scores for Family versus Friends, Family versus Public, and Public versus TP

	Family	Friends	Family	Public	Public	TP
Steps	0.96	0.94	0.96	0.91[a]	0.89	0.89
	(0.19)	(0.14)	(0.19)	(0.22)	(0.27)	(0.25)
Calories	0.96	0.94	0.96	0.89[a]	0.89	0.89
	(0.19)	(0.17)	(0.19)	(0.25)	(0.27)	(0.25)
Sleep	0.96	0.95	0.96	0.87[a]	0.87	0.87
	(0.19)	(0.14)	(0.19)	(0.30)	(0.30)	(0.29)
Traits	0.91	0.83	0.91	0.78[a]	0.80	0.83
	(0.23)	(0.26)	(0.23)	(0.29)	(0.29)	(0.32)
Goals	0.85	0.73	0.86	0.61[a]	0.68	0.82[a]
	(0.36)	(0.42)	(0.36)	(0.50)	(0.48)	(0.38)
Major	0.94	0.91	0.95	1.00	0.98	0.82[a]
	(0.21)	(0.25)	(0.21)	(0.00)	(0.16)	(0.38)
Weight	0.83	0.64[a]	0.84	0.54[b]	0.59	0.74[a]
	(0.37)	(0.46)	(0.36)	(0.51)	(0.50)	(0.43)
	$n = 27$		$n = 28$		$n = 37$	

TP, Third parties.

[a] Final scores for the two groups are different, $p \leq 0.05$.

[b] Final scores for the two groups are different, $p \leq 0.01$.

public. The participants said that they felt uncomfortable sharing sensed information with strangers because it made them feel like they were *being watched*. Not surprisingly, the participants also shared personal traits significantly more with family than with the public.

Less information shared with the public than with third parties. Table 30.3 shows that the participants were generally more open to sharing weight and health goals with specific third parties than with the public. In the poststudy interviews, some participants said this was because they perceived some benefit in sharing information with specific third parties. Third-party request e-mails contained a reason for wanting the participants' data, and at least some participants apparently expected the third parties to use their data for the purposes mentioned in the e-mail. In contrast, some participants expressed concern about who among the public would be accessing their information or how they might use it.

Surprisingly, the participants were less willing to share academic major with the specific third parties than with the public. Some participants said during the poststudy interview that they shared information with specific third parties because they thought that the information would be useful, based on the purpose stated in the third-party request. Some of them felt that academic major was not relevant to the request.

Given the comparison on personal traits, we were surprised to see no difference in sharing of sensed information between the public and third parties.

Does sharing behavior change over time; are participants' privacy preferences dynamic? In Table 30.4, we show select traits and sensed information by the initial (end of day 2) and final (end of day 5) sharing scores for three sets of sharing partners: family, friends, and the public.

Sharing sensed information. For family, the participants did not change sharing behavior of sensed information over the course of the study, while for friends, there was a slight (nonsignificant) change. For the public, however, we found that there was a statistically

Downloaded by [David Kotz] at 11:35 20 December 2014

TABLE 30.4

Initial and Final Normalized Sharing Scores for Family, Friends, and the Public

	Family		Friends		Public	
	Initial	**Final**	**Initial**	**Final**	**Initial**	**Final**
Steps	0.96	0.96	0.97	0.95	0.94	0.88[b]
	(0.19)	(0.19)	(0.10)	(0.14)	(0.22)	(0.26)
Calories	0.96	0.96	1.00	0.95	0.93	0.88
	(0.19)	(0.19)	(0.02)	(0.17)	(0.23)	(0.27)
Sleep	0.96	0.96	0.98	0.95[b]	0.93	0.87[a]
	(0.19)	(0.19)	(0.09)	(0.16)	(0.22)	(0.30)
Traits	0.95	0.91	0.93	0.84[b]	0.92	0.80[c]
	(0.19)	(0.23)	(0.13)	(0.26)	(0.17)	(0.29)
Activity	0.96	0.93	0.95	0.84[a]	0.98	0.85[b]
	(0.19)	(0.26)	(0.20)	(0.36)	(0.16)	(0.36)
Goals	0.93	0.86	0.95	0.75[b]	0.83	0.68[b]
	(0.26)	(0.36)	(0.29)	(0.41)	(0.38)	(0.47)
Weight	0.89	0.84[a]	0.80	0.63[c]	0.83	0.61[c]
	(0.31)	(0.36)	(0.35)	(0.46)	(0.38)	(0.49)
	$n = 28$		$n = 29$		$n = 41$	

[a] Initial and final scores are different, $p \leq 0.1$.
[b] Initial and final scores are different, $p \leq 0.05$.
[c] Initial and final scores are different, $p \leq 0.01$.

significant reduction in sharing scores for steps and sleep. Some participants felt uncomfortable sharing their steps and sleep, as the study progressed; they said that they felt like they were being watched.

Sharing traits. Similarly, in the case of the trait information, there was a slight (nonsignificant) reduction in sharing scores for family. However, there was a statistically significant difference between the initial and final sharing scores for friends and for the public. We learned from the poststudy interviews that some participants were embarrassed to share certain personal traits with friends and concerned about sharing their personal traits with strangers; they might have realized it only seeing their data over time. More details of the poststudy interviews are given in Section 30.4.2.

Demographic differences. Though the study was not designed to examine differences in sharing by characteristics like occupational status or gender, we did find some differences across these characteristics and so present them as preliminary findings that are suggestive of future study. As shown in Table 30.5, independent sample *t*-tests revealed that females shared traits (the combined score), weight, and goals with friends, significantly less than did male subjects. Table 30.5 shows only the difference in sharing with friends, but there was a statistically significant difference in the extent that personal traits, weight, and activity level were shared with the public and third parties as well [26].

As shown in Table 30.6, students shared their weight with family more than employees shared with family. In contrast, they shared their health goals less with the public than employed adults did with the public. Some of the employees said they did not want to share weight information with their family to avoid discussion about weight management. Students considered health goals to be sensitive and did not want to share this information with the public, but surprisingly, employees were more willing to share this information with the public.

Downloaded by [David Kotz] at 11:35 20 December 2014

TABLE 30.5

Final Normalized Sharing Scores Based on Gender

	Female	Male
grpscore(*u*, Friends, Traits, 5)	0.78	0.95[a]
grpscore(*u*, Friends, Weight, 5)	0.47	0.95[b]
grpscore(*u*, Friends, Goals, 5)	0.64	0.95[c]

[a] Sharing scores of females and males are different, $p \leq 0.1$.
[b] Sharing scores of females and males are different, $p \leq 0.01$.
[c] Sharing scores of females and males are different, $p \leq 0.05$.

TABLE 30.6

Final Normalized Sharing Scores—Students versus Employees

	Students	Employees
grpscore(*u*, Family, Weight, 5)	0.90	0.50[a]
grpscore(*u*, Public, Goals, 5)	0.48	0.83[a]

[a] Sharing scores of students and employees are different, $p \leq 0.1$.

Downloaded by [David Kotz] at 11:35 20 December 2014

Students were much more concerned than retirees about sharing their personal traits, weight, and goals with the public, as shown in Table 30.7. (*Caveat:* Recall that we had only female retirees; given that females shared less than males with friends in Table 30.5, we are not sure why female retirees shared more with the public than students.) There are several possible reasons for this difference in behavior: we speculate that the retirees are not used to the technology or do not want to bother their family and friends by sharing with them information that the retirees feel will not be of interest; when they do share this information with others, they are less concerned about the information than students. We expect students, on hand, to be used to the technology and used to sharing information electronically with others. We speculate that they might have changed the default settings either because they were curious about the different settings or because they were really concerned about what they were sharing with others. We expect students and employees to have more reasons to be worried about their activities and to hide it from their family and friends than retirees, either because they were embarrassed about some information, maybe their weight, or they wanted to hide some information, like partying or sexual activity. Students and employees were more engaged in the study than retirees. In Section 30.4.2, we present anecdotal evidence of such behavior and concerns.

To summarize, we found that weight and health goals appeared to be most sensitive among the information collected during the study. The participants exhibited disparate and dynamic sharing behavior of this information. We found some evidence that sharing behavior might vary with occupational status and gender. After observing the

TABLE 30.7

Final Normalized Sharing Scores—Students versus Retirees

	Students	Retirees
grpscore(*u*, Public, Traits, 5)	0.74	1.00[a]
grpscore(*u*, Public, Weight, 5)	0.48	1.00[b]
grpscore(*u*, Public, Goals, 5)	0.48	1.00[b]

[a] Sharing scores of students and retirees are different, $p \leq 0.1$.
[b] Sharing scores of students and retirees are different, $p \leq 0.05$.

participants' sharing behavior, we wanted to understand the reasons for their sharing behavior, as discussed in the next section.

30.4.2 Poststudy Interviews

To give us insight into the reasons for participants' sharing behavior, we conducted poststudy interviews. We discuss the answers to the following questions: "Did you change the sharing controls on the interface at any point? If so, what influenced that decision? Did you change the sharing controls for X? If so, why?" For answers to other questions, please refer to our technical report [26]. We recorded the interviews. We coded the interviews manually and grouped the statements into categories. We discuss in the succeeding text the reasons for the participants' sharing behavior.

Amount of information collected. Three participants mentioned that they felt the information was not sensitive because the device collected information only for 5 days. One female student said that the reason she shared the information with third parties was because "it was a study and it wasn't very long."

Context of data collection. A few students were concerned about sharing information that was collected by devices while they were at parties or staying up late. A male employee asked, "Would [the device] be something you would keep on during sexual activity or when you go to the bathroom?"

Sensitivity of the data. One male student shared all his information with others, but said that he might have had concerns about sharing "If maybe I was someone who [was] trying to exercise more and I exercised less." A few female students did not want to share their activity information because they felt like they were being watched. One of them said, "They can see every step I take, that was just a little weird."

Information utility. Some participants decided to share their information with others depending on how they would use the information. One female student said, "I think I hid my weight from almost everybody, except for people who actually needed it for medical purposes." One employee, being a researcher, was open to sharing her health information with other researchers. Some participants considered the third parties differently, based on their reason for requesting the data. One female student said, "I was fine with sharing things [with universities]; for some reason, they felt a lot more legitimate, you know what they would be doing, studying. It was random people that I didn't know what they were doing that I [did not want to share my information with]." One male student said he would share information with everyone, as long as it would not affect him in the future when he was applying for insurance or jobs. He said, "I would be fine with all of those, with the exception if that has an impact on the ability to apply for insurance or something of that nature, in which case I would start to worry."

Anonymity. A few students felt their information would not be linked to them (even though they were aware that their e-mail was being shared), so they were comfortable sharing it with third parties. According to a female student, "They don't know who I am, they are just doing research." One male employee felt that his identity is linked more to his name than his e-mail. He said, "It's my name, but I control [my e-mail]. I control what I get, I can change my e-mail address."

Sharing partners. Most participants said they would share information depending on who it was being shared with. One female student said "If there was someone who was a lot heavier than me, I probably would have given them the 5 minute calories, because they might feel bad that I used so many calories throughout the day. With friends who were less active than me, I would have shared less."

Downloaded by [David Kotz] at 11:35 20 December 2014

Partner involvement. One male student was happy to share his activity information with others; he said when you share activity information, "You feel like other people are in this with you, it makes it easier to keep going," and he said encouraging feedback from his friends made him feel good about sharing his information. A female student shared her Fitbit information with third parties, because according to her, "When I was wearing [the device] and getting data requests all the time, it felt like what I was doing was important," and she was disappointed that the requests were fake, and to her, it meant that "no one actually cares about your data and no one's going to use it, it was all for nothing kind of thing." Some students did not want to share certain information due to fear of being judged by others. A female student said, "With my friends, I wasn't sure whether to share my height and weight, because sometimes especially if I am sharing with my girlfriends, oh they are like you are heavier than me, lighter than me." Another female student said, "I don't mind articulating [my health information] in person, but on a website, I feel it is more easily judged in the wrong way that I can't fully explain what is going on."

Negative experiences. A female student was concerned about sharing information with the government, because she grew up in a country where "everything was monitored by the government." One female employee was sharing all her information with the third parties during the study, until she noticed that she started getting spam about weight loss, which must have been coincidental.

Relationships. One elderly participant was not comfortable with sharing her activity information with her children. She said, "I didn't want them to have to encourage me to walk more. They don't need to know. We are very, very close but they don't need to know how much I walk." A male student said, "I told [my mom] I would tell her of any results of any significance, but I told her that I was hiding the data and I wasn't going to let her see it. Honestly, my friends didn't care about the data."

Some students were more comfortable sharing their information with family than their friends. One said, "If it was someone I didn't know I would share everything. Friends they know you, but you are not close enough to share everything with them. I shared everything with my mom."

Some female students were more comfortable sharing personal information with their family and third parties than with their friends. One student said "I might have left height and weight with family, but friends don't need to know that. I shared it with companies and researchers, because I think it is pertinent."

Some students were more comfortable sharing their information with family and friends than third parties. Two of them said, "I didn't share any information with the extra researchers. I don't know who they are and I have no affiliation with them," and "I don't know [the requesters]. I don't think it is weird that they were asking for [the information], but it was weird sharing with them. From teammates, hid my weight and my health goals. From my mom, I didn't hide anything."

Some students wanted to share their information with third parties more than with people they knew, like their family and friends. They said they wanted to share less information with family and friends: one participant said "because I know them personally, whereas the third parties they seem, not that personal … so I felt like more of a pressure to hide more specific activity levels from [my family and friends]." Another said "Because my parents are people who are big on exercise. If I don't do much exercise, they wouldn't like that," while a third participant said "A bunch of researchers looking at the data, I don't care. But I might think twice about some people I know, depending on who they are." Another participant said, "People who don't know me, it would be fine. My age doesn't

Downloaded by [David Kotz] at 11:35 20 December 2014

bother me, it would be mostly my weight. It all depends on who gets it, what is the purpose. If it is somebody studying what is the better way to do things."

Some participants did not want to share information with private companies. A male student said, "I'm against corporations. I probably wouldn't want any of them [to have access to my information], except students." A male employee said, "Oh yeah, I would share that info [with students]. With individuals, with family members, or friends who are interested and people doing research, I have no problem. It is just third-party companies [that I wouldn't want to have the data]."

One elderly retiree was not tech savvy; her husband was helping her manage her Fitbit account and he might have had an influence on her sharing decisions.

Information types. We asked the participants whether they would use a mobile device that collects personal health information like their heart rate, breathing rate, pulse rate, medication, diet and exercise, location, and social interactions, if it gave them similar sharing controls as the Fitbit in our study. Most students considered medications to be most sensitive. A male student said, "Just like bodily functions, you can't really use that against you, whereas medication you are taking, that's something like, there are some medications people don't want other people finding out that they are taking." Some of them were worried about sharing location and social interactions. Students who were athletes were concerned about sharing their vital signs and exercise information. One female employee was open to sharing any information "as long as [she] could control who saw what."

Downloaded by [David Kotz] at 11:35 20 December 2014

30.5 Discussion

In addition to the focus groups, the user study helped us identify the key factors that influence privacy decisions regarding health and fitness information collected using mHealth devices. The findings from this study can help guide mHealth device and application developers and privacy advocates to build flexible privacy controls for mHealth devices, with sensible defaults and expressive controls for users to change the settings thereafter.

We discovered that people were concerned about sharing more information than necessary with their sharing partners. They based their decisions to share information on the type of information being shared and people the information was being shared with, that is, the sharing partners. While making the sharing decision, people take into account the volume of information that is shared, why the sharing partner needs the information, the context in which the information was collected, and how sensitive the information is to them. People considered a certain type of information to be sensitive if sharing partners could misuse the information to cause harm to them or if sharing the information could cause a change in the relationship that the people shared with the sharing partner. So their decision to share information with sharing partners also depended on how they expected the sharing partners to use the information and whether their relationship with the sharing partners would be affected if the sharing partner was aware of this information. On the other hand, they shared information if it was already known to the sharing partners; for example they shared age and gender with family and friends.

People were more willing to share their health information with sharing partners who had a positive influence on their health decisions, while they were hesitant to share it with sharing partners with whom they have had prior negative interactions. People seemed to be willing to share their personal information when they felt that the sharing partner would use the data for the betterment of society, for example, by using the data for research; in such cases, the

sharing did not directly benefit them, but it benefited the society. Even in these instances, some people ensured that they would not be harmed; they were particular about their anonymity and wanted to ensure that their health information could not be linked to their identity. On the other hand, people also took into account their prior experiences with sharing partners when making the decision to share their information; some participants had prior negative experience with the government and refused to share any information with government agencies.

We also observed that the participants changed their sharing settings during the course of the study after receiving (negative and positive) feedback from sharing partners. For example, one female employee was sharing all her information with the third parties during the study, until she noticed that she started getting spam about weight loss; she assumed it was from one of the third parties involved in the study and stopped sharing her data with all third parties.

When designing sharing controls for a system, especially a system that handles sensitive information like personal health information, it is important to ensure that the controls are easy to use, flexible, and convenient and account for ignorant users and changing privacy laws. Care should be taken that only adequate control is given to the patient since they should not restrict the sharing partner from accessing information that could be crucial to their health care; determining how much control is adequate remains a challenge.

Our study revealed three interesting findings about people's privacy concerns regarding their sensed health information:

1. *Demographic information shared less than sensed information*. The study revealed that the participants were less willing to share the demographic information we collected than the activity information that was sensed by the device. For example, initial sharing scores for weight and health goals were less than the initial sharing scores for other information types, including the sensed information. We expect users to be concerned about sharing certain context information, depending on how it might affect the value they perceive in the information being shared. For example, a user might share her location information when it is being collected by her asthma sensor and shared with her mother, but she might not want to share her location, when it is collected as part of her activity information by her fitness device.
2. *Information shared more with strangers than their own family and friends*. We discovered that sharing scores for friends were lower than scores for family, while sharing scores for friends were lower than for third parties. However, sharing scores for the public were mostly the same or less than for friends. The focus groups and the poststudy interviews revealed different reasons for people's sharing behavior, including their relationship with the sharing recipients. The participants were more willing to share if they perceived benefits in sharing, especially when it came to sharing with specific third parties, as opposed to the public.
3. *Dynamic sharing behavior*. We confirmed that privacy concerns are not static; mHealth device users may change their sharing decisions over time.

Given these findings, we elaborate on two recommendations that will help guide the development of flexible privacy controls that enable users to express their sharing preferences easily:

Flexible controls need to support both fine- and coarse-grained approaches to sharing. Throughout the study, we observed a wide diversity in sharing behavior, which was in accordance with the varied privacy preferences of the focus-group participants. Some study participants used

Downloaded by [David Kotz] at 11:35 20 December 2014

a very coarse-grained approach, while others took the time to fine-tune their privacy settings. Sensible default settings are required to support those users who never change their sharing settings, either because they are busy, lazy, not tech savvy, or want immediate benefits from the system. The availability of granular controls encouraged the participants, who were averse to sharing everything, to share some information, instead of hiding all information. The participants expressed disparate sharing preferences and exhibited dynamic sharing behavior in our study, which implies that default *one-size-fits-all* settings are not enough.

We observed contradicting behavior among participants; some participants shared more with their friends than with family, while others shared more with their family than with their friends. We also observed dynamic sharing behavior; some participants changed the amount of information they shared during the course of the study. Granular levels of sharing and expressive controls, which we discuss next, can help such users change their sharing setting easily to map their preferences.

Reducing disconnect between information and granular controls. Users make their sharing decisions based on what information they are sharing and who they are sharing it with. Since sharing decisions are dynamic, the information should be clearly presented and the controls flexible and easy to use, to allow the participant to map their privacy preferences easily. Narrowing the gap between settings and what is actually shared can help users change their behavior easily to suit their sharing preferences. For example, in our study, the website home page for every participant was divided into different views, one view corresponding to one sharing recipient, where the participant could decide what information she wanted to share with that recipient. View for sharing recipient "Mom" on the participant's home page displayed exactly what Mom would see as the participant's health information. By combining the information and the granular controls, the interface made it possible for the participant to observe what Mom would see for different choices of sharing settings and finally choose the setting that best mapped her privacy preferences. We did not test the usability of the system, so we cannot claim that our design is the best way to provide granular controls for sharing health information. Designing an interface for an mHealth device and application that collects a large amount of sensed, personal demographic, and context information and whose user has the option to choose a large number of sharing recipients is an interesting and challenging problem.

User studies, like ours, could benefit from a bigger sample size, better population sampling, and longer duration. Nevertheless, the study helped us understand people's willingness to share and their dynamic sharing behavior. We expect these findings to hold broadly for other mHealth devices and applications as well. A general privacy setting for all mHealth devices is not possible, given the disparate sharing behavior among users for even a single mHealth device. We recommend seeking a general approach to health information visualization: a flexible design that supports all mHealth devices and allows users to also visualize how they are sharing their health information with others.

30.6 Related Work

Previous work has looked at people's willingness to share information with others. Previous work suggests that users will change behavior when the context of information sharing varies [23]. For example, studies of location tracking show that at least some users will vary their willingness to share depending on place and social context [3], time since the start of information sharing [28], recipients [7], and their closeness to the recipients [36].

Downloaded by [David Kotz] at 11:35 20 December 2014

Downloaded by [David Kotz] at 11:35 20 December 2014

Other studies of context show that users are more likely to reveal information when the reward from the exchange increases [25] but less likely to do so when risk of identity theft increases [4]. Our findings confirm that these results hold even for people's willingness to share their health information.

Willingness to share. Previous work has shown that people make privacy decisions based on the information being shared and the person they are sharing it with. It has been shown, through surveys and interviews, that users share location information based on the sharing recipient, why the recipients want the information, what would be useful to them, and whether the users want to disclose that information with them; during the study, users received hypothetical sharing requests from family and friends [7]. (Our findings confirmed that people use the same sort of logic to make privacy decisions with health information.) An online survey showed that the participants do not understand the value of sharing location information and their privacy decisions depend on the sharing recipient [33]. The aforementioned two studies, however, never gave the participants an opportunity to actually share the information with real people but just learned about their sharing preferences through interviews and surveys. People may not be aware of real privacy risks until they actually share the information with others and receive feedback about the sharing [6]; our study gave the participants the opportunity to actually share the information with real people. Our study showed that people did have privacy concerns about sharing certain information types, but they changed their sharing settings during the course of the study. Our findings confirmed results from previous work, which showed that the participants change their privacy policy decisions with time, but the participants in that study knew the information was not being shared with real people [20]. The manner in which people think they might share their information changes once their information is actually shared with real people; the findings from our study are more valid than previous work, because our study participants actually shared information with real people. Also, the other studies were focused on understanding privacy concerns while sharing other types of information; we wanted to understand how sharing behavior changes when it comes to health and fitness information. Certain types of health information might be more sensitive than other types of personal information, like location, so it is important to study people's privacy preferences regarding health information.

Health information. Maitland and Chalmlers conducted interviews to understand the role of peers in weight management and what information people are willing to disclose to their peers [17]. Caine and Henania studied people's desires for sharing their health information, using questionnaires, card tasks, and interviews [5]. We, too, wanted to understand users' willingness to share their fitness and health information, but we gave users an opportunity to actually share their own information with family, friends, and third parties. Olson et al. conducted surveys with employees (median age of 35) to study people's willingness to share their personal information, including pregnancy and health status, with others and they identified similarities in what people wanted to share and who they wanted to share it with [24]. Our work is different from theirs in that we conducted a study with young students, employees, and retirees, where subjects collect information about themselves and actually share that information with real people (or in some cases, believe that their data is being shared with actual people).

Information collected using sensors and mobile devices. Klasnja et al. study the privacy concerns of patients using a fitness device by conducting interviews [18]. We also study privacy concerns of patients using a fitness device, but we focus on their willingness to share the collected information. Raij et al. showed that people are more aware of privacy risks once they receive feedback about their shared health information, collected using mobile sensors,

and have a stake in the data, that is, if the shared health data is their own [27]. The study participants (in this case, students) filled out a survey after seeing feedback about their information for 10–15 min. In our study, we allow the participants to share the collected information with real individuals chosen by them and study how willing they are to share their activity and sleep information with friends, family, and third parties. To the best of our knowledge, ours is the first study that explores users' privacy concerns by giving them the opportunity to actually share the information collected about them using mHealth devices.

Our work focuses on the privacy concerns that people will have when they share their health information; we expect people to have these concerns irrespective of the system used to share the health information. In our study setup, health information was collected using a mobile device called Fitbit and uploaded to a private web server and shared with sharing partners through the web. However, health information can also be shared via EHRs and social networks. In the following, we highlight research that focuses on the privacy concerns that users have when sharing health information using these systems. The following research complements our work since it addresses privacy concerns that people have when using systems, other than private websites, to share their health information.

Electronic health records. In the context of EHRs, several studies have showed similar results as ours. Shaw et al. conducted a literature review of 21 articles (with publishing dates between 1994 and 2008), which focused on the privacy concerns that patients and health-care providers have about EHRs in various countries [30]. The study revealed that patients' willingness to share health information depended on how sensitive they considered the information to be; sexual and mental health were considered to be most sensitive. Patients were willing to share their health information with health-care providers involved in their care but were against sharing it with other medical and nonmedical individuals. In a recent study, Caine and Henania showed that sharing preferences varied by type of information and recipient, and overall sharing preferences varied by participant [5]. Haas et al. presents a set of design requirements for privacy-preserving EHRs; their requirements, however, are for controls to manage privacy policies and, unlike ours, will not be able to support the actual sharing behavior of patients [12]. Researchers have also highlighted the need for a balance to protect individuals from potential harm that may be caused by exposing personal information and the quality and safety expected of the health-care system [29]. Finally, Alemán et al. presents a survey of all the security and privacy issues and proposed solutions for EHRs [2].

Social networks. Prior research describes the privacy risks introduced by social networking in health-care domain [13,19,37]. Newman et al. conducted interviews to understand health interactions on online health communities and social networks and propose design recommendations for future systems that will support health-oriented social interactions [22]. Thompson et al. discovered how medical professionals violated patient privacy by posting protected health information on their publicly available social networking sites [32].

30.7 Case Studies

This chapter described a study conducted to understand privacy preferences and sharing behavior of mHealth device users.

Raij et al. and Caine and Henania are two other studies with similar goals [5,27]; the first one was conducted to understand privacy risks that might arise with the use of mHealth

Downloaded by [David Kotz] at 11:35 20 December 2014

devices and other wearable sensors, while the second one was conducted to understand the privacy preferences of patients who use electronic medical records.

30.8 Summary

To provide flexible and expressive privacy controls, it is important to understand users' willingness to share their personal health information collected using the device. Other researchers used interviews and surveys to understand people's willingness to share; their results might not reflect real privacy concerns, since people remain unaware of real privacy risks until they actually share the information with others. We conducted a user study to understand how willing users were to share their personal health information that they collected using an mHealth device that they carried with them at all times for 5 days. We recommend a flexible design for sharing controls that narrows the gap between controls and the information being shared, allowing patients to visualize how they are sharing their health information with others.

Downloaded by [David Kotz] at 11:35 20 December 2014

Acknowledgments

This research results from a research program at the ISTS, supported by the NSF under Grant Award Number 0910842 (TISH) and Award Number 1143548 (PC3) and by HHS (SHARP program) under Award Number 90TR0003-01. We also thank undergraduate research interns Alexandra Della Pia and Tina Ma and our colleagues in the Dartmouth TISH group, for their valuable feedback.

Questions

1. Briefly describe an incident where a privacy breach occurred with an mHealth device. How was it resolved?
2. What can you learn from the controversy, and how would you ensure a similar situation will not happen with an mHealth app that you develop?
3. State five instances in which information collected using mHealth devices can end up disclosed more than necessary?
4. Do you think the recommendations from the study can be applied to mHealth apps collecting nonfitness information? Design an interface, highlighting the available sharing settings (feel free to exclude values) for an app that monitors onset of asthma. The app asks the patient to blow into a spirometer twice a day and suggests them to use an inhaler. It monitors when the patient uses the inhaler and shares with the patient's mom. The app also monitors where the patient goes and the dust and pollen count in the atmosphere in the locations at those times when the readings were taken.
5. How would you extend the study, if the goal were to understand sharing behavior based on gender?

Downloaded by [David Kotz] at 11:35 20 December 2014

References

1. Affectiva, Inc., 2014. http://www.affectiva.com/, January 2011.
2. J. L. F. Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval. Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, 46:541–562, 2013.
3. D. Anthony, T. Henderson, and D. Kotz. Privacy in location-aware computing environments. *IEEE Pervasive Computing*, 6:64–72, 2007.
4. D. Baumer, J. Earp, and J. Poindexter. Quantifying privacy choices with experimental economics. In *Proceedings of Workshop on Economics of Information Security (WEIS)*, June 2–3, 2005, Cambridge, MA, pp. 1–16, 2005.
5. K. Caine and R. Hanania. Patients want granular privacy control over health information in electronic medical records. *Journal of the American Medical Informatics Association*, 20(1):7–15, January 2013.
6. K. Connelly, A. Khalil, and Y. Liu. Do I do what I say?: Observed versus stated privacy preferences. In *Proceedings of Human-Computer Interaction (INTERACT)*, Vol. 4662, Lecture Notes in Computer Science, Chapter 61, pp. 620–623, Springer, New York, 2007.
7. S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge. Location disclosure to social relations: Why, when, & what people want to share. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pp. 81–90, ACM, New York, 2005.
8. G. Demiris, B. K. Hensel, M. Skubic, and M. Rantz. Senior residents' perceived need of and preferences for smart home sensor technologies. *International Journal of Technology Assessment in Health Care*, 24(1):120–124, 2008.
9. Fitbit, Inc., 2014. http://www.fitbit.com, January 2011.
10. J. H. Frost and M. P. Massagli. Social uses of personal health information within PatientsLikeMe, an online patient community: What can happen when patients have access to one another's data. *Journal of Medical Internet Research*, 10(3):e15+, May 2008.
11. Google Health, Inc., 2013. http://www.google.com/intl/en-US/health/about/, January 2011.
12. S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, and G. Müller. Aspects of privacy for electronic health records. *International Journal of Medical Informatics*, 80(2):26–31, 2010.
13. C. Hawn. Take two aspirin and tweet me in the morning: How Twitter, Facebook, and other social media are reshaping health care. *Health Affairs*, 28(2):361–368, 2009.
14. iBaby Labs, Inc., Heartsense. 2013. http://www.ibabylabs.com/product/heartsense, August 2013.
15. C. J. Hoofnagle, J. King, S. Li, and J. Turow. How different are young adults from older adults when it comes to information privacy attitudes and policies? Social Science Research Network Working Paper Series, April 2010. doi: http://dx.doi.org/10.2139/ssrn.1589864.
16. C. Jensen, C. Potts, and C. Jensen. Privacy practices of internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1–2):203–227, July 2005.
17. J. Maitland and M. Chalmers. Designing for peer involvement in weight management. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, ACM, New York, 315–324, 2011.
18. P. Klasnja, S. Consolvo, T. Choudhury, and R. Beckwith. Exploring privacy concerns about personal sensing. H. Tokuda, M. Beigl, A. Friday, A.J. Brush, Y. Tobe (Eds.) In *Proceedings of the International Conference on Pervasive Computing (Pervasive)*, Springer-Verlag, New York, May 2009.
19. J. Li. Privacy policies for health social networking sites. *Journal of the American Medical Informatics Association*, 20:704–707, 2013.
20. M. L. Mazurek, P. F. Klemperer, R. Shay, H. Takabi, L. Bauer, and L. F. Cranor. Exploring reactive access control. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pp. 2085–2094, ACM, New York, 2011.
21. Microsoft, Microsoft HealthVault. https://www.healthvault.com/us/en, January 2011.

22. M. W. Newman, D. Lauterbach, S. A. Munson, P. Resnick, and M. E. Morris. "It's not that I don't have problems, I'm just not putting them on Facebook": Challenges and opportunities in using online social networks for health. In *Conference on Computer Supported Cooperative Work and Social Computing*, ACM, New York, 341–350, 2011.
23. H. Nissenbaum. *Privacy in Context*, Stanford University Press, Palo Alto, CA, 2010.
24. J. S. Olson, J. Grudin, and E. Horvitz. A study of preferences for sharing and privacy. In *Extended Abstracts on Human Factors in Computing Systems (CHI EA)*, pp. 1985–1988, ACM, New York, 2005.
25. S. Patil, G. Norcie, A. Kapadia, and A. J. Lee. Reasons, rewards, regrets: Privacy considerations in location sharing as an interactive practice. In *Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS '12*, ACM, New York, 5:1–5:15, 2012.
26. A. Prasad. Exposing privacy concerns in mHealth sensing. Technical Report TR2012-711, Dartmouth College, Hanover, NH, February 2012. http://www.cs.dartmouth.edu/reports/TR2012-711.pdf.
27. A. Raij, A. Ghosh, S. Kumar, and M. Srivastava. Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, ACM, New York, 11–20, 2011.
28. N. Sadeh, J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, and J. Rao. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal Ubiquitous Computing*, 13(6):401–412, August 2009.
29. A. Shachak and A. R. Jadad. Electronic health records in the age of social networks and global telecommunications. *Journal of the American Medical Association*, 303(5):452–453, 2010.
30. N. T. Shaw, A. Kulkarni, and R. L. Mador. Patients and health care providers' concerns about the privacy of electronic health records: A review of the literature. *Electronic Journal of Health Informatics*, 6(1):e3, 2010.
31. R. H. Thaler and C. R. Sunstein. *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Yale University Press, London, U.K., 2008.
32. L. A. Thompson, E. Black, W. P. Duff, N. P. Black, H. Saliba, and K. Dawson. Protected health information on social networking sites: Ethical and legal considerations. *Journal of Medical Internet Research*, 13(1):e8, 2011.
33. J. Tsai, P. Kelley, L. Cranor, and N. Sadeh. Location-sharing technologies: Privacy risks and controls. In *Proceedings of the Research Conference on Communication, Information and Internet Policy (TPRC)*, Arlington, VA, 2009. Accessed on September 25–27, 2009.
34. M. van der Velden and K. E. Emam. "Not all my friends need to know": A qualitative study of teenage patients, privacy, and social media. *Journal of the American Medical Informatics Association*, 20(1):16–24, January 2013.
35. Perfect Third Inc. WakeMate, 2011. http://wakemate.com/, January 2011.
36. J. Wiese, P. G. Kelley, L. F. Cranor, L. Dabbish, J. I. Hong, and J. Zimmerman. Are you close with me? Are you nearby? Investigating social groups, closeness, and willingness to share. In *Proceedings of the International Conference on Ubiquitous Computing (UBICOMP)*, September 17–21, 2011, Beijing, China, pp. 197–206, 2011.
37. J. Williams. Social networking applications in health care: Threats to the privacy and security of health information. In *Proceedings of the 2010 ICSE Workshop on Software Engineering in Health Care, SEHC '10*, pp. 39–49, ACM, New York, 2010.
38. Withings, Inc., Withings blood pressure cuff. 2014. http://www.withings.com/en/bloodpressuremonitor, November 2011.

Downloaded by [David Kotz] at 11:35 20 December 2014

Downloaded by [David Kotz] at 11:35 20 December 2014