EXPOSING PRIVACY CONCERNS IN MHEALTH DATA SHARING

Dartmouth Computer Science Technical Report TR2012-711

A Thesis

Submitted to the Faculty

in partial fulfillment of the requirements for the

degree of

Master of Science

in

Computer Science

by

Aarathi Prasad

DARTMOUTH COLLEGE

Hanover, New Hampshire

February 2012

Examining Committee:

David Kotz (chair)

Sean Smith

Denise Anthony

Brian W. Pogue, Ph.D.

Dean of Graduate Studies

Abstract

Mobile health (mHealth) has become important in the field of healthcare information technology, as patients begin to use mobile devices to record their daily activities and vital signs. These devices can record personal health information even outside the hospital setting, while the patients are at home or at their workplace. However, the devices might record sensitive information that might not be relevant for medical purposes and in some cases may be misused. Patients need expressive privacy controls so that they can trade potential health benefits of the technology with the privacy risks. To provide such privacy controls, it is important to understand what patients feel are the benefits and risks associated with the technology and what controls they want over the information.

We conducted focus groups to understand the privacy concerns that patients have when they use mHealth devices. We conducted a user study to understand how willing patients are to share their personal health information that was collected using an mHealth device. 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. We found that patients tend to share more information with third parties than the public and prefer to keep certain information from their family and friends. Finally, based on these discoveries, we propose some guidelines to developing defaults for sharing settings in mHealth systems.

Acknowledgements

This work would not have been possible without the continued support, patience, and guidance of my advisor Professor David Kotz. I would like to thank Jacob Sorber, for his constructive criticism to my half-baked ideas and also for his advice regarding graduate student life. I am very grateful to Professor Denise Anthony and Timothy Stablein for their patience and for helping me learn and appreciate sociological methods and research. I would like to thank my lab group Shrirang Mare, Cory Cornelius and Ronald Peterson for their continued guidance and feedback. I am grateful to WISP interns Christina Ma and Alexandra Della Pia for helping me design the user study and manage the focus groups. I would also like to thank Professor Sean Smith for being on my thesis committee and providing valuable comments on my thesis. The focus groups and user study would not have happened without assistance from some very special people among the staff of the Dartmouth Computer Science department, Institute of Security, Technology and Society (ISTS), the Office of the Associate Dean of Faculty for the Sciences and Dartmouth-Hitchcock Medical Center and the residents of Kendal at Hanover.

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.

I would also like to thank Professor Prasad Jayanti for his words of wisdom on how to succeed as a graduate student. This research took more than two years, and I never lost enthusiasm, due to the encouragement from Mashfiqui Rabbi, Priya Natarajan, Paritosh Kavatekar, Ranganath Kondapally and Umang Bhaskar. I am very grateful to Nimit Dhulekar for being a patient listener

and for encouraging me to put in my best. Words are not enough to express the gratitude to my wonderful family, for loving me, having faith in me and being there for me.

1 Introduction

Mobile health (mHealth) devices make it possible for patients to monitor daily activities and record vital signs. The devices can help the patients work towards a healthier lifestyle or allow them to share the collected information with their doctor to diagnose their health issues or manage a chronic disease. The goal of such devices is to better patients' health and improve the efficiency and effectiveness of healthcare. Since mHealth devices are portable, patients can record their health information even while outside the hospital setting. There are many types of mHealth devices; two examples include an armband, BodyMedia Fit, that tracks daily activities [7] and a wrist watch, Glucowatch, that monitors blood glucose level [32].

An mHealth device can deliver continuous health monitoring to patients throughout their daily activities, allowing them to be closely monitored by their health providers, family and friends, as patients work towards improving their health. mHealth devices can be used to monitor your activities (Fitbit [2], BodyMedia Fit [7]), sleep (Wakemate [6]), emotions (Affectiva [1]), vital signs (Withings blood pressure cuff [35], Glucowatch [32]) or fetal conditions (Monica AN24 [5]). Doctors can use sensors to monitor patients after they are discharged from the hospital and thus can have access to detailed health information about the patient during normal life activities. Patients can collect their personal health information and upload it to a vendor website, social networking website, a personal health record (Microsoft HealthVault [4] or Google Health [3]), or a hospital-owned electronic health record. Once the data is uploaded, they 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 towards a healthier lifestyle. Patients can also share their experiences with their peers (others suffering from similar medical conditions) and work together to get better [15]. Patients might also want to share some health information with pharmacists, insurance companies, drug companies, employers, and others involved in their healthcare.

If these sensors are collecting personal health information while patients are at home or at their workplace, they might record other sensitive information, like the location of their home, when they leave for work, or who they interact with; this information might not be relevant for medical purposes, and may in some cases be misused. Furthermore, the inadvertent disclosure of sensitive health information can cause harm to the patient. Potential employers might refuse job offers to applicants with risky health conditions. Unnecessary disclosure of health information about celebrities and public figures can lead to embarrassment. Since some mHealth sensors are used outside the hospital setting, they can record non-health information (like location, daily activities, or social contacts) that could be used for marketing purposes or by stalkers or criminals to harm the patient.

Patients might be concerned when the sensors are collecting and sharing sensitive information and they might not use such sensors if their privacy is not protected. The National Committee for Vital and Health Statistics (NCVHS), a key advisory committee to the US Department of Health and Human Services, defines *health information privacy* as “an individual’s right to control the acquisition, uses, or disclosures of his or her identifiable health data”. We expect that patients will want to be able to decide what information is necessary to be shared and who can be trusted with the information. Patients need to trade the potential health benefits with potential privacy risks, just as consumers can opt for discounts in supermarkets in return for their personal information.

Of course, many consumers might not know what the actual privacy risks are in the case of store discount cards. To receive immediate benefits of the mHealth device, however, patients might share their personal information without considering the different sharing options. It is important for mHealth systems to provide "sensible" default settings to allow them to enjoy the immediate benefits of the system, without worrying about their privacy.

We use the term "user" or "Patient" to denote the mHealth device user and "sharing partner" to denote the person(s) with whom the user shares her personal health information. In the following scenario, Jane (the user) shares her diet and exercise information with her friend (her sharing partner). In the second scenario, Ravi (the user) shares his health information with the hospital, his doctor, the research institute and his insurance company (his sharing partners).

In the first scenario, Jane wants to lose weight, and starts training with her friend. They set up a diet and exercise regime, and purchase an mHealth device that could help them both monitor their daily activities and food and compute an estimate of the calories burned. Jane carries it with her at all times, since she doesn't have a fixed exercise schedule, but exercises whenever she finds time. Jane's activity information is sent to her mobile phone, which is periodically uploaded to a private website where she shares the information with her friend. When Jane looks at the website, she realizes that when the device synchronized with the phone, it also accessed the phone's GPS to create a map of her movements throughout the day. She is hesitant to share this map with her friend, but the controls on the website are complicated and she cannot disable the sharing of the map.

Consider another scenario. Ravi is a diabetic who finds it difficult to manage his condition effectively resulting in significant variation of his diurnal blood-glucose levels. Ravi's doctor advises him to subscribe to a Diabetes Management Program offered by his hospital. As a part of the program, Ravi wears a hospital-provided device that continuously monitors his activity level and calories burned, and installs hospital-provided software on his mobile phone. The software processes data it receives from the activity/calorie monitor and also acquires other contextual information such as Ravi's location, calendar schedule and time of the day. It reminds him to take his medication, alerts him to long periods of inactivity, encourages him to log diet information and tracks his daily goals of calorie intake and expenditure. The mobile phone periodically synchronizes with a backend server that maintains Ravi's Personal Health Record. Ravi chooses to allow complete access to his personal health information, including contextual data such as his current location, to his family members. The Diabetes Management Program is an initiative by the Diabetes Research Institute, which is part of the hospital. When Ravi joined the program, he opted to share his health information, collected by the device, with the research institute as well. Once a week, Ravi records his weight, blood glucose and blood pressure, using devices that send the measurements wirelessly to his mobile phone. Ravi also enters his dietary information manually into his mobile phone daily, which the software records as part of his PHI. Due to his participation in the diabetes management program, Ravi's insurance company offers to reduce his premium if he shows significant improvement in controlling his diabetes. To demonstrate improvement, Ravi must provide the insurance company access to his aggregate health data. Unfortunately his PHR does not give him controls to restrict the sharing of the other contextual data being collected by his phone with the insurance company and he chooses to share everything with his insurance company.

In the scenarios, Jane and Ravi choose to give up some privacy to enjoy the benefits of the mHealth device. Indeed, due to inadequate controls in the software, they give up more privacy than they wish, and more than is needed for the sharing purpose. We believe Patients should be allowed to enjoy the benefits without such an excessive loss to privacy. We need to provide them usable privacy mechanisms that allow them to enjoy the benefits of the mHealth device, without reducing their privacy more than necessary. To build such privacy mechanisms, we need to understand how patients want to control the sharing of their health information. Jane and Ravi wanted to change the sharing settings because they were aware of the privacy risks of sharing the information. But most Patients will not be able to decide what information they want to share and with whom, perhaps because they are not aware of the privacy risks of disclosing sensitive information – or perhaps because they are busy, lazy or not tech-savvy. Before we provide privacy controls to Patients, it is important to understand what Patients think are the benefits and risks of the technology and whether they want control over the information. Our work provides three contributions: We conducted focus groups to understand privacy concerns that patients have when they use mHealth devices. We conducted a user study to understand how willing patients are to share their personal health information that was collected using an mHealth device. Then, based on our findings from the focus groups and user study, we suggest default sharing settings for personal health information for mHealth systems. We expect our work to help the development of mHealth systems in the future.

Jane was comfortable sharing her activity information with her friend, but not the GPS information collected by her mobile phone. Ravi was comfortable sharing his health information with his health providers and researchers but did not want to share the contextual information collected by his phone with his insurance company. Jane and Ravi shared some information with some sharing partners but not others. So understanding who Patients want to share their health information with could help us understand what sharing settings they need and lead us to the default sharing settings that mHealth systems should provide.

We expected Patients to share information based on personal relationships (friends and family), professional relationships (employers and colleagues), medical relationships (doctors, hospital, nurses, insurance company), indirect relationships (hospital payment group, doctors of another hospital), temporary trust relationships (third-party researchers), and no relationship (public). We wanted to understand whether Patients trusted some sharing partners more than others with some types of information, i.e., do Patients want to share certain types of information with their family and friends, but not others, and whether there is some information they want only their doctor to know. Does their willingness to share their personal health information vary with their age, gender or their health experiences? We conducted several focus groups to understand Patients' privacy concerns [29]. During the focus groups, we presented participants with scenarios where patients use mHealth devices to monitor their health and then asked participants open-ended questions about how they would collect and share health information in those scenarios. Since the focus groups were based on hypothetical scenarios, we also conducted a user study to determine how people actually share their own health information with others. Students, employees and retirees used a fitness device to collect and share their activity information and personal characteristics with family, friends, third parties, and the public.

We discovered that people share more information with third parties than with the public, because they believe third parties use the information for research purposes. But even in this case, they will share information only to the detail which they think is sufficient for use by third parties. People tend to hide certain information from their family and friends either because the information is embarassing or because they do not want their family and friends to be involved in their health care. It might be possible to identify the different types of information that might be collected using mHealth sensors and predict the default sharing settings that people might choose for these information types, based on the demographics of the patient. We suggest that by default, very little or no information should being shared with others; if the patient is interested in sharing more, she could always change the sharing settings using the controls on her health record or the private website where her health information is uploaded.

This document is organized as follows. Section 2 describes work done in similar fields and explains why our work is different. Section 3 describes the focus groups and Section 4 describes the user study. Finally, we discuss our findings in Section 5 and suggest future work in Section 6.

2 Related Work

Several studies have been conducted to understand people's perception of information (not restricted to health information) privacy. Even though people advocate privacy, they tend to be ignorant or are willing to give up their privacy to enjoy the benefits offered to them in exchange for their information [26]. For example, on Online Social Networks (OSNs), people are willing to share information without realizing who has access to it and how it could be used [25]. But even though new OSN users may not realize the consequences of sharing sensitive information, Nov et al. showed that long-time OSN users tend to adopt more restrictive privacy settings and reduce the amount of information that is being shared [27], while a study of Facebook app users showed that their privacy attitudes depended on whether or not they had an adverse privacy experience on a social networking site [22]. Surprisingly, studies have shown that people's views towards information privacy do not vary significantly with their age [18]. This could imply that people's privacy concerns increase with experience, but does not vary with their age.

User privacy has taken on an altogether new meaning in the modern mobile world; users own smartphones that collect their personal information at all times - at home and at work. A recent survey of mobile phone users showed that 98% of respondents were concerned about privacy when using their mobile phone and that they wanted control over their personal information that was collected by mobile apps [8]. Several attempts have been made to build systems that cater to users' privacy concerns [19]. One piece of information that is particularly important to users, and has been extensively studied by researchers, is location. With the advent of location-sharing services, users are getting more hesitant about sharing this private information with others and are concerned about controlling who has access to their location [33]. Studies have shown that users share location information to the detail that they think would be useful for the consumer [14, 20] and also depending on where they were, who they were with, and who was requesting the information [9]. Do patients have similar privacy preferences regarding their personal health information?

As in location sharing, users are sensitive about sharing their health information [31]. Major laws provide a legal basis for healthcare privacy [16, 17], but the protection they provide could vary with jurisdictions and might, in some cases, be inconsistent with other laws protecting the same jurisdiction. Many conceptual privacy frameworks have also been defined to protect patients' health information privacy [24]. Such laws and frameworks recommend that the patients should be allowed to make decisions about the collection, disclosure and use of their information. But are patients capable of deciding what information is necessary to be shared and who can be trusted with the information? To understand people's attitude towards health information privacy, researchers have studied the privacy needs of adolescents and elderly people regarding healthcare. Adolescents need informational, physical, social and psychological privacy [12] and seniors in an aging-in-place setting desire solitude and confidentiality [11]. However, the ability to make good privacy decisions about sharing of information using medical assistive technologies might decrease with age [34]. This implies that medical assistive technologies should provide sensible default sharing settings to prevent elderly patients from disclosing their sensitive health information.

Patients have healthcare privacy needs, but many existing medical assistive technologies do not provide expressive privacy controls that can help both young and elderly Patients to make sharing decisions such that they can enjoy health benefits without violating their privacy constraints.

Benish et al. showed that expressive privacy mechanisms improve users' ability to make these sharing decisions without violating their privacy constraints [10]. So mHealth systems also need to provide expressive privacy controls that can help Patients make decisions by providing feedback about their sharing and that allow Patients to express their sharing preferences easily and thus, share information only to the level of detail as they desire.

To provide these controls, we need to understand what privacy concerns Patients might have, so we conducted focus groups and a user study to learn about Patients' willingness to share their personal health information. Maitland et al. conducted interviews to understand the role of peers in weight management and what information people are willing to disclose to their peers [21]. We also wanted to understand users' willingness to share their fitness information, but we gave users an opportunity to share their own fitness 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 with others and they identified similarities in what people wanted to share and who they wanted to share it with [28]. The personal information types included two types that were related to health: pregnancy and health status. Our work is different from theirs in that we conducted a study with young students, employees and retirees, where people collect information about them and actually share that information with real people (or in some cases, believe that their data is being shared with actual people). Klasnja et al. study the privacy concerns of patients using a fitness device by conducting interviews [23]. 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 and have a stake in the data, i.e., if the shared health data is their own [30]. The study participants (in this case, students) filled out a survey after seeing the feedback about their information for 10-15 minutes. But people will not be aware of real privacy risks until they actually share the information with others and receive feedback about the sharing [13]. 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.

3 Focus Groups

We conducted exploratory focus-group discussions to gain a preliminary understanding about Patients' privacy preferences. The focus groups were approved by Dartmouth's Institute Review Board (CPHS #22425). 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 minutes and all participants were paid for their time. We chose these groups since we wanted to talk to Patients who have some health experiences – some who have been recently hospitalized and others who are monitored continuously outside the hospital – and Patients who have limited healthcare-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 Patient'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. For the pilot study with hospital outpatients, we used scenarios in Figure 8 (see Appendix B). The college students were presented with scenarios in Figure 9 (see Appendix B). After the pilot study, we decided to use scenarios in Figure 10 (see Appendix B) for elderly participants, both hospital outpatients and members of community organizations.

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.

3.1 Results

Disadvantages of sharing 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. 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 that *"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."*

Reasons for using an mHealth device. 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 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."*

Reasons for not using an mHealth device. 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. 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".* One elderly participant was worried about the presence of the device in his everyday life, he pointed out, *"It is controlling,* [what if the patient] *doesn't want to be reminded of his disease?".* One elderly participant pointed out that the devices might give a sense of false security that someone was constantly monitoring your activities.

Collection of health information. 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".* Some participants were concerned that a lot of unnecessary information was being collected by the devices in the scenarios. According to some elderly participants, *"The doctor should not be spending time on* [unimportant] *details during the appointment"* and *"It might not be in the doctor's expertise to analyse the collected information, so they might have to share it with others* [without the patient's knowledge]*".* One elderly participant was worried that devices could collect wrong information, he said *"a pedometer doesn't get correct values always."* Some students pointed out that some devices might collect information about people around the patient without their knowledge and their consent.

Consequences of sharing. One student could not understand why anyone would steal her health information, while another student pointed out, *"You can draw some kind of analogy or trend* [from the collected health information] *that could be misused".*

Reasons for sharing. 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] *wasnt associated to my name in any way, if I was purely a number"*.

Reasons for not sharing. 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"*. A few participants were not happy about being compared with their peers; one elderly participant said, *"It might be discouraging if you fall behind others.* [I would be] *happier when I didn't know."*

Relationships with doctors, family and friends. 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 didnt want my wife to know* [about my stroke] *since I didnt want her to worry, since she was in Beijing"* 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, e.g., if the patient was a minor or an elderly person.

Trust issues. 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, *"More the information you collect, 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.

Control. 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. Its like taking your medication in the first place."* Another student wanted the control to delete some information being sharing it with others. An elderly participant said she wanted complete control over all the decisions she made; she said, *"People* [at the retirement home] *like 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."*

Usability. All participants agreed that the devices should be usable, even by patients who were unfamiliar with technology. An elderly participant said, *"People might not be techies.* [They would have] *no idea how to operate* [the device]".

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?"*

Information types. 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.

By conducting the focus groups, we learned about some of the different type of concerns people might have when collecting and sharing their personal health information. We also understood that people might base their sharing decisions on who they were sharing the information with, why their sharing partners needed it and what was already being shared with others. The focus groups, however, were based on hypothetical scenarios and did not reflect how a patient might actually behave when they share their own personal health information collected using a mobile health device that they carry with them at all times.

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 user study where participants carry a device that collects their personal health information and share 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.

To the best of our knowledge, ours is the first study that explores Patients' privacy concerns by requiring them to *actually* share the information collected about them using mHealth devices; Patients can decide whether to share the information and if so, how much information to share with others.

4 User Study

The focus-group discussions were based on hypothetical scenarios, which were designed to help participants imagine the benefits and the privacy risks of using mHealth devices. Since most people have no real experience with or knowledge of mHealth devices, we devised a user study in which a sample of subjects used an mHealth device. Furthermore, we wanted them to actually share the data, to push them to make real privacy decisions. Once they are aware of what information can be collected, they should be able to make a better judgment about the privacy rules that define sharing of this information.

4.1 Study design

The goal of the study was to understand people's willingness to share their personal health information. Information can be of two types: it can either be shared or hidden from others or it can be shared at different granularities. We wanted to observe whether people share information differently with different groups like family members, friends, third parties and the public; for example, do they share some information with family that they hide from their friends or do they share information at a finer granularity with third parties than the public? Also we wanted to learn whether people increase or reduce the amount of information they share with time. We recruited students, employees and retirees for the study. They selected family members and friends to share their information with and received emailed requests to share their information with third parties. The third parties were real, but the requests were fake. (For example, one of the email requests were from a group of students in Harvard University who needed the participant's activity information for their machine-learning class.) The participants could also share their information with the public, people not involved in the study (for example, friends on social networks), by sharing a link to their information. We considered involving a doctor in the study, to understand what information participants would want to share with a doctor. We finally decided not to do so for several reasons: people might be comfortable sharing information with their own doctor, but not with unfamiliar doctors and we realized that inviting participants' doctors to be a part of the study

	Male (M)	Female (F)	Total
Students (S)	8	13	21
Working (W)	5	7	12
Retired (R)	0	8	8
Total	13	28	41

Table 1: Participants

would be difficult, especially since the study was only for five days.

4.2 Methods

For the study, we recruited 21 undergraduate students, 12 adult workers from local area including Dartmouth employees, and 8 female elderly residents of a local retirement home, as shown in Table 1.

We recruited the participants with flyers (Figure 11 in Appendix B), which presented the study as a study of a new device to help individuals trying to lose weight and/or improve fitness and health. The subjects were required to own a computer, to not be injured, to be able to walk and to be able to carry the device with them at all times during the five days. The study was approved by Dartmouth's Institutional Review Board (CPHS #22791).

The participants carried an mHealth device for five days; this device, called Fitbit, is a 3-axis accelerometer packaged in a clip-shaped body that resembles a Bluetooth headset [2]. It tracks calories burned, steps taken, distance traveled and sleep quality. It is not waterproof. It can be worn on the waist, in pockets or on undergarments. At night, it can be clipped to a wristband to track sleep. The collected data is uploaded to a user's personal account on Fitbit.com when the user walks past the USB base station. The user study required the participants to carry the Fitbit on them at all times for five days. They could take the device off during swimming, bathing or any time they felt uncomfortable carrying it in certain situations. They had to upload the collected information at least once a day.

When the participants signed up for the study, we collected from them several pieces of information: their health goals, activity level and academic major. After they configured the Fitbit, we collected their age, gender, height and weight from the fitbit.com website. For the study, we developed a web interface that presented each participant's uploaded Fitbit data and their personal characteristics and allowed them to share the information with others. The fitbit.com website did not have an option to share Fitbit users' personal characteristics, nor a capability for us to monitor sharing settings. Using the web interface we developed, the participants could see and share their activity information as a daily summary, six-hourly summary, hourly summary or as a detailed five-minute version. They could also hide their activity information and personal characteristics from everyone else.

On the first day of the study, the participants selected at least one family member and two friends to share their Fitbit information with. An email was sent automatically to these sharing partners, informing them about the study and asking them to be a part of the study. About 27% (n=11) of the participants did not select any friends or family members to share their data with; so they were not considered when we analyzed how the participants shared their data with friends and family. Table 2 shows the number of family and friends selected by the participants.

On the second day, the participants signed a consent form, giving us permission to share their

Table 2: Number of participants who selected family and friends

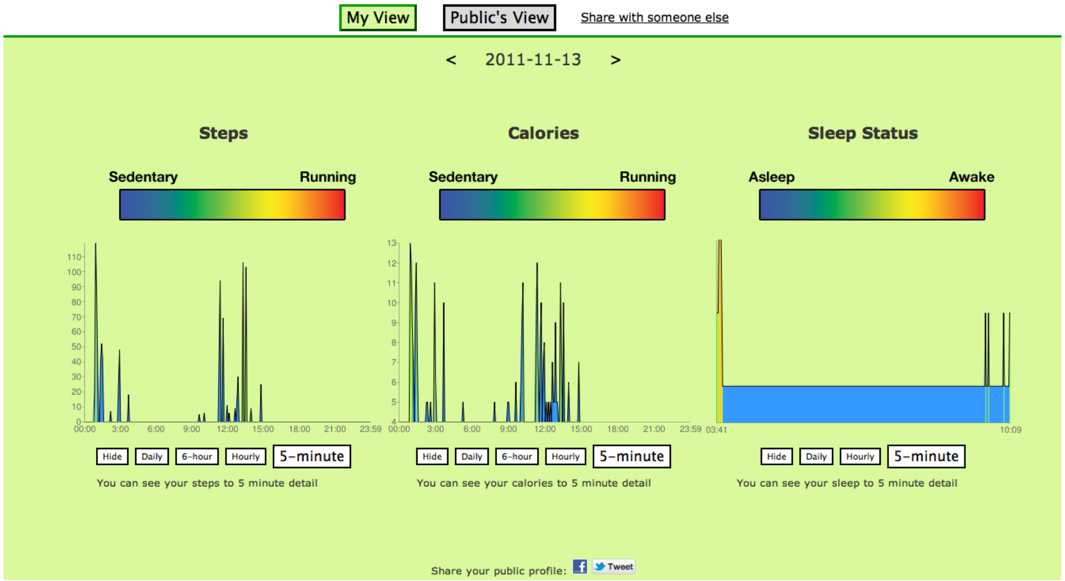
		Friends	
		=0	≥1
Family	= 0	27%	5%
	≥1	2%	66%

Table 3: Mean and (std. deviation) of the number of family and friends selected by the 66%

Family	Friends
1.26	2.11
(0.44)	(0.5)

activity information and personal characteristics with the people they chose. We told the participants that their information would be shared with their family and friends from the next day onwards and that they could decide, by using the controls on the website, what they wanted to share with their sharing partners. We told the participants that they might get requests from third parties to share their information and that their data would be open to the public and that they could use the controls on the website to control the disclosure of their information. We did not tell the participants that the third-party requests were fake and that their information was not actually exposed to the public.

On the third day of the study, an email was sent to the family members and friends with a link to a webpage where they could see the Fitbit information and personal characteristics of the participant who chose them to be part of the study. For activity data (i.e., steps, calories and sleep), and for each sharing partner, participants could either share a detailed 5-minute version, share an hourly, 6-hourly, or daily summary, or hide it completely. The default setting shared activity data at the maximum sharing setting, i.e., 5-minute granularity. Participants could also share or hide their personal characteristics (age, height, weight, gender, activity level, health goals, academic major),



You can see your steps to 5 minute detail

You can see your calories to 5 minute detail

You can see your sleep to 5 minute detail

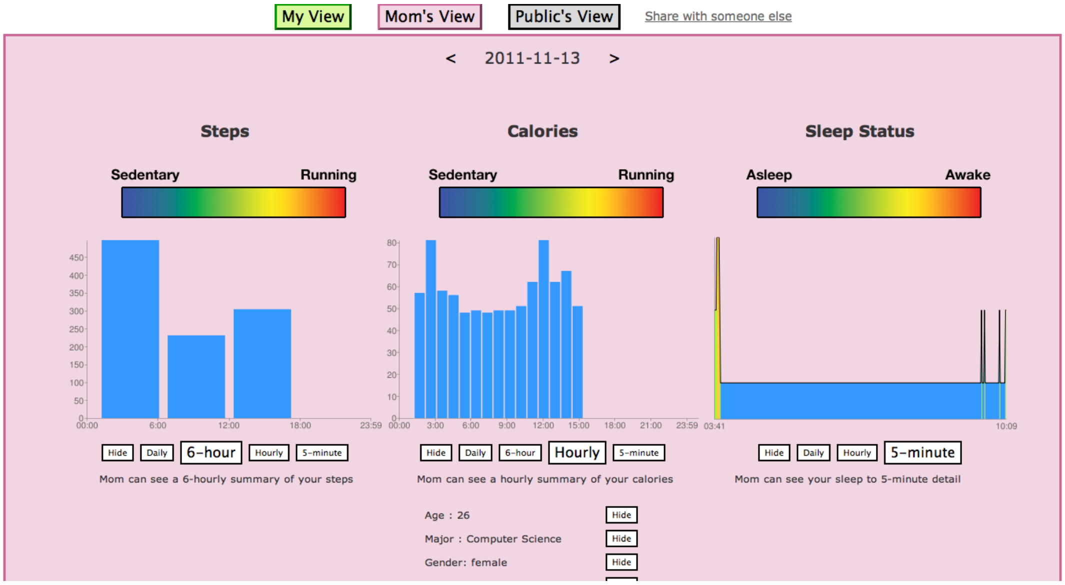
Share your public profile:

Figure 1: Default view for participant

independently by type and for each sharing partner. The family members and friends received mails on the fourth and fifth day of the study as well, reminding them to visit the web interface. The participants received mails everyday during the five-day period of the study. From the third day of the study onwards, these mails explained who was receiving their activity information and personal characteristics and what sharing settings they had chosen for each information type for each sharing partner.

The webpage had different views of the same information. The default view was the view for the participant, as shown in Figure 1. There was one view corresponding to each sharing partner. Figure 2 shows the view for “Mom”. 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 see.

To understand how participants would share their fitness information with third-party organi-



Mom can see a 6-hourly summary of your steps

Mom can see a hourly summary of your calories

Mom can see your sleep to 5-minute detail

Age : 26

Major : Computer Science

Gender: female

Figure 2: View for sharing partner named Mom

zations and groups, we sent mails to the participants on behalf of 6 different organizations and groups. This mail explained who the group was and why they needed the data; see Figure 12 in Appendix C. The groups represented college students, research labs, government agencies, engineering companies, wellness institutes and pharmaceutical companies. These requests were sent in random order to the participants during the last three days of the study (three on the third day, one on the fourth and two on the last day). The participants received the mails at the same time, but parties requesting the data were chosen randomly. We did not share the participants' data with any third-party organizations, but crafted the messages to be believable hoping that the participants would act as if actually sharing.

We logged the participants' activity on the website to monitor their activity: when they logged in, when they looked at their view or the view of the others with whom they are sharing their data, and when they changed the sharing settings. We conducted interviews at the end of the study, for the questions, see Section C.2 in Appendix C, where we asked the participants several questions: whether they ever took off the device to hide any information, if 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). We recorded the interviews, transcribed and coded them manually.

4.3 Results

We first analyze the information we extracted from the website logs and then summarize what we learned from the post-study interviews.

4.3.1 Website logs

Using the logs, we first tried to understand the participants' involvement in the study.

Based on number of visits to own views. We first observed how many times participants visited the different views on their account on the study website. From the logs, we extracted the number of times participants visited their own view and views of their sharing partners. When a participant logged in to her account, she was directed to her own view. The mean and standard deviation for the number of times participants visited their own view (including distinct logins) was 6.32 and 5.37 respectively; the maximum number of visits was 23.

Based on number of visits to views of sharing partners. We then computed the number of times participants looked at the views of their sharing partners. The female student who visited her own view 23 times also had the maximum number (120) of total visits to the views of the third parties (20 visits each to the views of the third parties). Table 4 shows the number of times participants looked at the views of their sharing partners averaged across the number of partners they chose (in the case of family and friends) and the number of requests they received (in the case of third parties). We are not distinguishing between participants who visited the view of just one partner in a group and those who visited the views of all the partners in the same group. We conducted paired sample t-tests and found a statistically significant difference in the number of times participants looked at the views of friends and family and the views of third parties and the public, as shown in Table 4. Participants were clearly concerned about how the public and third parties were viewing their shared information, more so than their family and friends. So we expect them to share less information with the public and third parties than with family and friends; we explore this hypothesis below.

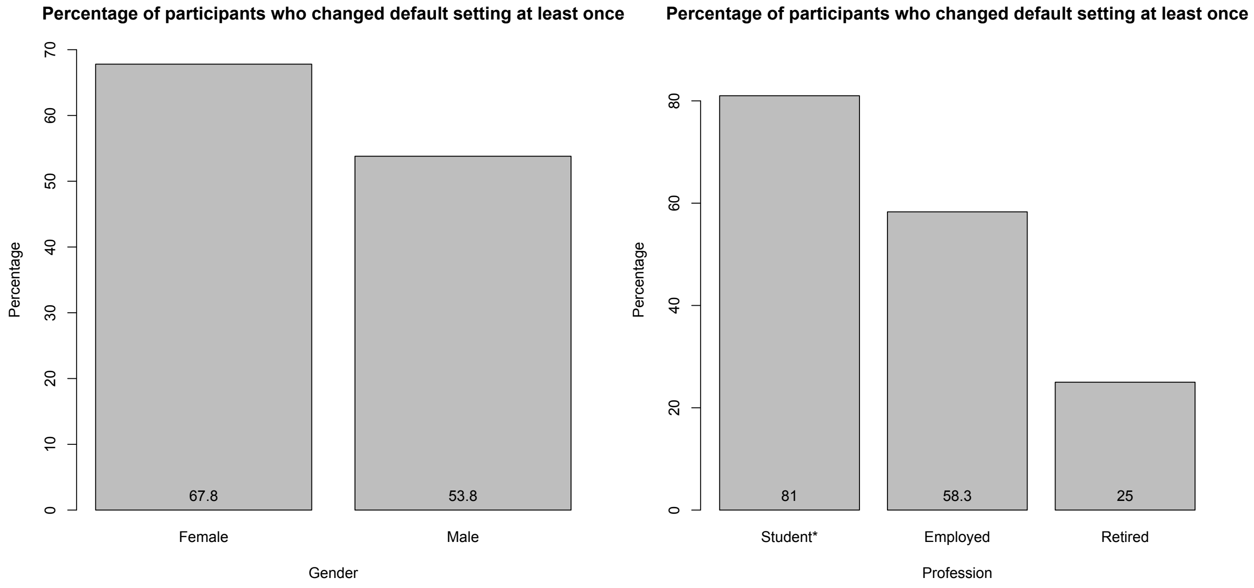
Table 4: Mean and (standard deviation) of the number of visits to public view and average number of visits to views of friends, family, and third parties

Family views	Friend views	Public view	Third-party views
1.33 (3.53)	1 (2.76)	8.78** (8.32)	3.17† (4.31)

** Visits to public view $>$ visits to family, friends and third-party views ($p \leq 0.01$).

† Visits to third-party views $>$ visits to family ($p \leq 0.1$) and visits to friend views ($p \leq 0.05$).

Based on change of settings on own views. We then looked at how many times participants changed the settings on their own views. The mean and standard deviation of the number of changes in settings were 41.07 and 42.68; the maximum number of times was 175. Five out of the 41 participants changed the settings on their own views more than 100 times and all of them were students. One of these five students never changed the default sharing settings for any of his sharing partners. So we speculate that the participants' reasons for changing settings could have been either privacy concerns or mere curiosity.



(a) Based on gender

(b) Based on profession

Figure 3: Percentage of participants who changed default settings at least once.

Based on at least one change to default settings. By default, activity information (to 5-minute detail) and participants' personal characteristics are shared with all their sharing partners. The participants could restrict sharing information about their activity information by selecting settings like hide information or share a daily, 6-hourly, or hourly summary of the information. They could also hide their personal characteristics. Figure 3 shows the percentage of participants who changed the default setting at least once. Figure 3a shows the percentage of male and female participants who changed the default settings at least once and Figure 3b shows the percentage of students, employees and retirees who changed settings at least once. We can see that more than 80% of students and nearly 70% of female participants changed the default settings, whereas 75% of elderly participants never changed the default settings for any sharing partners, not even for

*Number of students who changed the default settings is significantly greater than retirees ($p \leq 0.05$ with ANOVA post-hoc testing using Bonferroni's method).

the ‘public’ partner. Using post-hoc ANOVA test with Bonferroni’s method, we discovered that there was a statistically significant difference in the number of students who changed the default setting when compared to the number of retirees. The above percentages were based on all 41 participants, including those participants who had not selected a family member or a friend to share their information with. Even though we told all the participants that their information was being shared with the public, we speculate that some participants might have forgotten that they were sharing the information, since they did not select any one to share their information with. This could be one of the reasons for the difference in behavior (especially since only three retirees selected at least one family member or friend), although it may appear that students were more concerned about their sharing settings than retirees.

So we focus on the 73% of participants who selected at least one family or friend to share their information with. Based on gender, we discovered that 80% of the female participants and 60% of the male participants in this group changed the default sharing settings at least once for at least one partner. Basing our comparison on profession, we found that 80% of students, 70% of employees and 33% of the retirees in this group changed the default settings at least once for at least one partner. Using post-hoc ANOVA test with Bonferroni’s method, we discovered that there was a statistically significant difference in the number of students who changed the default setting when compared to the number of retirees ($p < 0.01$).

Next, we focus on the 90% of the participants who received the third-party requests. Based on gender, we discovered that 75% of the female participants and 54% of the male participants in this group changed the default sharing settings at least once for at least one partner. Basing our comparison on profession, we found that 80% of students, 64% of employees and 33% of the retirees in this group changed the default settings at least once for at least one partner. Using post-hoc ANOVA test with Bonferroni's method, we discovered that there was a statistically significant difference in the number of students who changed the default setting when compared to the number of employees and retirees ($p < 0.05$).

It appears that students are more concerned about their sharing settings than retirees. This difference in behavior could be due to several reasons: we speculate that the retirees are not used to the technology and 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 the 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 hiding it from their family and friends than retirees; either because they were embarassed 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 4.3.2, we present anecdotal evidence of such behavior and concerns.

Next we wanted to understand how the different types of information was shared with the different groups of sharing partners.

Defining sharing scores. Let $s(u, p, t, d)$ denote 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 hide, share daily summary, share 6-hourly summary, share hourly summary, and share 5-minute detail respectively. For the other information types, the setting can be either 0 (hiding the information) or 1 (sharing the information). By default, $s(u, p, t, d)$=4 for t={steps, calories, sleep} and $s(u, p, t, d)$=1 for t={age, gender, health goals, height, activity level, major, weight}.

We computed a group sharing score for each participant to represent the amount of information shared with that group. Equation 1 defines the sharing score for participant u for group g for type t on day d.

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

We focus most of our analysis on two snapshots: the initial sharing score, which is the mean of the last setting chosen by the participant, on the 2nd day of the study, $\mathbf{score}(u, g, t, 2)$, and the final sharing score, which is the mean of the final settings chosen by the participants, on the 5th day of the study, $\mathbf{score}(u, g, t, 5)$.

First we analyze how the participants shared their information with their family, friends and the public.

Computing number of users who shared some information. For a given information type t and a group g of partners, how many participants u selected at least one partner p in a group and chose to share some information (for personal characteristics like age or gender) or share at least a daily summary (for activity information like steps, calories and sleep) with at least one of the partners in that group? We computed this value for each information type and each group (friends/family).

$$\mathbf{share}(u, g, t) = |\{u \mid \exists p \in g : s(u, p, t, 5) > 0\}| \tag{2}$$

We found that 31% of participants (who selected at least one friend, n=29) did not share their weight and 21% did not share their health goals with any of their friends, whereas all of them shared some information about their steps, calories and sleep with at least one friend. We also found that 14% of participants (who selected at least one family member, n=28) did not share their weight and health goals with any of their family members.

Computing number of users who hid, shared partial and shared all information. Next, we looked at how many participants hid all information, shared partial information and shared everything with all friends, family and public and how many shared differently with the different partners in one group.

Given an information type t and a group of sharing partners g, how many participants u chose at least one partner p in that group and hid all their information from all the partners in that group?

$$\mathbf{nothing}(u, g, t) = |\{u \mid \forall p \in g : s(u, p, t, 5) = 0 \text{ and } |g| > 0\}| \tag{3}$$

We found that 4 out of 28 participants hid their weight from their family, 9 out of 29 participants hid their weight from all friends and 16 out of 41 hid their weight from the public. Similarly 4 out of 28 participants hid their health goals from their family, 6 out of 29 participants hid their health goals from their friends and 13 out of 41 hid their goals from the public. Furthermore, 5 out of 41 participants hid their age, 6 hid their major and activity level and 7 hid their gender from the public. None of the participants hid their steps, calories and sleep from all of their friends. Some participants were not comfortable sharing their weight and health goals with their friends and public, so weight and health goals were more sensitive than all the other information that was collected. A few participants also hid their age, major and gender (identifying information) from the public.

Given an information type t and a group of sharing partners g, how many participants u chose at least one partner p in that group and shared some, but not all, information with all the partners in that group?

$$\mathbf{partial}(u, g, t) = |\{u \mid \forall p \in g : 0 < s(u, p, t, 5) < 4 \text{ and } |g| > 0\}| \tag{4}$$

We found that 7 out of 41 participants shared partial information about their steps with public whereas 6 out of 41 participants shared partial information about their calories and sleep. Two participants hid their steps, calories and sleep from the public, and one other participant (a male student) also hid his sleep from the public.

Given an information type t and a group of sharing partners g, how many participants chose at least one partner in that group and shared all the collected information with all the partners in that group?

$$\mathbf{all}(u, g, t) = |\{u \mid \forall p \in g : s(u, p, t, 5) = \mathbf{max}(t) \text{ and } |g| > 0\}| \tag{5}$$

where,

$$\mathbf{max}(t) = \begin{cases} 4 & \forall t \in \text{(steps,calories,sleep)} \\ 1 & \text{otherwise} \end{cases} \tag{6}$$

Except for one participant (a male student), no one changed the default sharing settings for steps, calories and sleep when sharing with their family, that is, they shared that information at full detail, even though some of these participants shared only partial information with the public. It appears that they wanted their friends and family to be supportive of their goal to improve their health.

Given an information type t and a group of sharing partners g, how many participants u chose at least two partners p in that group and shared information differently among at least two partners in that group?

$$\mathbf{diff}(u, g, t) = |\{u \mid \exists p_1, p_2 \in g : s(u, p_1, t, 5) \neq s(u, p_2, t, 5) \text{ and } |g| > 1\}| \tag{7}$$

Only one participant, a female employee, shared her major and weight differently with the two family members that she chose and her academic major differently among her three friends. One male student shared all his information, except for calories, differently with his friends; he hid all this information from one friend and from above, we see that he is the only participant who hid his steps, calories and sleep from a family member, his mother. This student's reasons for hiding are explained in the next section; he preferred sharing his health information in person to his friends over sharing it electronically. A female student shared her goals, weight and her academic major differently with her friends. One other female student shared goals differently and another female student shared her weight differently with her friends. These students said that they shared sensitive information differently with their friends, based on their relationship with them; they were closer to some friends than others.

Change in sharing scores over time. We then computed the number of people who changed their settings for sharing information with the different groups, causing a difference in their sharing score, during the last three days of the study; we counted how many chose to share more (increase in sharing score) or share less (decrease in sharing score) and how many did not change their settings at all (no change in sharing score). Among those who restricted sharing of the different types of information, most participants reduced the amount of information they shared with the public. When sharing with the public, five participants reduced sharing settings for steps, height and activity level, six participants reduced sharing settings for goals and major and nine reduced settings for sharing weight. This implies that some participants (a total of ten participants; some reduced settings for more than one information type) were concerned about the information they were sharing with the public, as the study progressed and they became more aware of the information that was collected. Among the participants who restricted sharing with friends, five participants hid their health goals after the second day and five hid their weight. Apparently, some participants realized that their health goals and weight were sensitive; as the study progressed they hid this information from friends and the public.

Next we looked at how information was shared with the different third parties TP. Four participants did not receive the third-party requests due to technical issues and these participants are not included in the computations below. For four other participants, the requests went to their spam folder and they did not see the requests because they failed to login to their accounts after the second day of the study. These participants, however, have been included in the study.

Computing number of users who changed settings from default for third parties. First, we wanted to determine how many participants changed settings from default for at least one third party p for a given information type t.

$$\mathbf{changed}(u, t) = |\{u \mid \exists p \in TP : s(u, p, t, 5) \neq \mathbf{max}(t) \text{ and } |TP| = 6\}| \tag{8}$$

We also computed the number of participants who chose different sharing settings for the different third parties p for a given information type t.

$$\mathbf{difftp}(u, t) = |\{u \mid \exists p_1, p_2 \in TP : s(u, p_1, t, 5) \neq s(u, p_2, t, 5) \text{ and } |TP| = 6\}| \tag{9}$$

Nine out of 37 participants changed the default settings (to limit sharing) while sharing steps, calories and sleep with third parties. Out of the nine, four had different settings for the different third parties for sharing steps and sleep and five had different settings for calories. These participants shared activity information differently with the third parties; from the interviews, we learned that they shared what they thought was useful for the third parties. Six changed default setting for height and activity level; all the six participants had different settings for height for the different third parties and five out of six had different settings for activity level. Seven changed default settings for health goals and major; out of the seven, five had chosen different settings for health goals and major, while sharing with the different third parties. Ten changed default setting for weight; nine out of the ten participants chose a different setting for the different third parties. Participants were strangely more comfortable sharing their age and gender with the third parties; most of the participants said that they trusted the third parties more than the public. But some participants had concerns sharing their height, health goals, major and weight with the third parties and most of these participants shared this information with only some third parties; some participants said they trusted some third parties more than others whereas some felt that detailed information was not needed by the third parties for the purpose they stated. We explore the different reasons for sharing information with third parties in Section 4.3.2.

Comparing scores within and between groups. Table 5 and Table 6 give the initial and final sharing score chosen by participants for each group. Initial sharing settings are the settings chosen on the second day of the study. On the second day, the participants learn that their information will be shared with the different sharing partners on the following day. The sharing score for a group is computed as the mean of the sharing settings chosen for all the partners in that group, as given in Equation 1. In these tables we normalize each score by dividing by $\mathbf{max}(t)$. We used these tables to understand whether there was any difference between the means of

- the initial and final sharing scores chosen for each group, or
- the final sharing scores chosen for the different groups,

and then conducted paired sample t-tests to determine whether there was any statistically significant difference between the means.

Comparing initial and final sharing scores for family, friends and public. From Table 5, we found that there is a statistically significant difference in the initial and final sharing scores for the public, for steps and sleep. Some participants felt uncomfortable sharing their steps and sleep,

Table 5: Initial and final normalized sharing scores for activity information for family, friends and public; two cases show a significant reduction from the initial score

	Family		Friends		Public	
	Initial	Final	Initial	Final	Initial	Final
Steps	0.96 (0.19)	0.96 (0.19)	0.97 (0.10)	0.95 (0.14)	0.94 (0.22)	0.88^* (0.26)
Calories	0.96 (0.19)	0.96 (0.19)	1.00 (0.02)	0.95 (0.17)	0.93 (0.23)	0.88 (0.27)
Sleep	0.96 (0.19)	0.96 (0.19)	0.98 (0.09)	0.95 (0.16)	0.93 (0.22)	$0.87^\dagger$ (0.30)

* The mean final sharing score for steps for the public is less than the initial sharing score ($p \leq 0.05$).
† The mean final sharing score for sleep for the public is less than the initial sharing score ($p \leq 0.1$).

as the study progressed; they said that they felt like they were being watched.

From Table 6, we see that there is a statistically significant difference between the initial and final sharing scores for friends and the public, averaged across all the personal characteristics. We learned from the post-study interviews that some participants were embarassed to share certain personal characteristics with friends and concerned about sharing their personal characteristics with strangers; they might have realized it only after the second day or they might not have had the chance to change the settings until the third day. There was no significant change in sharing scores when sharing personal characteristics with family and no significant change in sharing scores for age, gender and major for friends. Age, gender and major are generally known to friends and family. There was a significant difference in sharing scores for all the personal characteristics for the public, except age and gender. Most participants were clearly concerned about sharing their personal characteristics with the public and they changed the sharing settings as the study progressed; we give anecdotal evidence to support this behavior in Section 4.3.2.

Comparing final sharing scores for family and friends. Tables 7 and 8 show the final sharing scores for family and friends. These tables show a statistically significant difference in the way weight was shared with family and friends. The sharing scores for friends were marginally less than that for family members for all other information types as well, even though the differences are not statistically significant. Participants were more concerned about sharing their information with their friends because they were worried of being judged by their friends.

Comparing final sharing scores for public and third parties. Tables 9 and 10 show the final sharing scores for the public and third parties. Participants were generally more open to sharing their information with third parties than with the public since they said they perceived some benefit in sharing with third parties. Third-party request emails contained a reason for why the third parties needed the participants' data and the participants apparently trusted the third parties to use their data for the purposes mentioned in the email. Participants might have hesitated to share information with the public, because they were unaware of who might have access to their information and how they might use it.

Table 6: Normalized sharing scores for personal characteristics

	Family		Friends		Public	
	Initial	Final	Initial	Final	Initial	Final
Characteristics	0.95	0.91	0.93	0.84*	0.92	0.80**
	(0.19)	(0.23)	(0.13)	(0.26)	(0.17)	(0.29)
Age	0.96	0.96	0.97	0.95	0.88	0.90
	(0.19)	(0.19)	(0.13)	(0.20)	(0.33)	(0.30)
Gender	0.96	0.93	0.98	0.91	0.98	0.93
	(0.19)	(0.26)	(0.09)	(0.27)	(0.16)	(0.26)
Major	0.96	0.95	0.97	0.91	0.98	0.83*
	(0.19)	(0.21)	(0.11)	(0.24)	(0.16)	(0.38)
Height	0.96	0.93	0.98	0.88†	0.98	0.85*
	(0.19	(0.26)	(0.09)	(0.32)	(0.16)	(0.36)
Weight	0.89	0.84	0.80	0.63**	0.83	0.61**
	(0.31)	(0.36)	(0.35)	(0.46)	(0.38)	(0.49)
Activity	0.96	0.93	0.95	0.84†	0.98	0.85*
	(0.19)	(0.26)	(0.20)	(0.36)	(0.16)	(0.36)
Goals	0.93	0.86	0.88	0.75*	0.83	0.68*
	(0.26)	(0.36)	(0.29)	(0.41)	(0.38)	(0.47)

† Initial and final scores are different, $p \leq 0.1$

* Initial and final scores are different, $p \leq 0.05$

** Initial and final scores are different, $p \leq 0.01$

Table 7: Final normalized sharing scores for activity information

	Family	Friends
Steps	0.96 (0.19)	0.94 (0.14)
Calories	0.96 (0.19)	0.94 (0.17)
Sleep	0.96 (0.19)	0.95 (0.14)

† Sharing scores of family and friends are different, $p \leq 0.1$
* Sharing scores of family and friends are different, $p \leq 0.05$
** Sharing scores of family and friends are different, $p \leq 0.01$

Steps, calories and sleep were shared similarly with public and third parties.

We found a statistically significant difference between the sharing scores for major, weight and goals for third parties and public (Table 10). Major was shared more with the public than with third parties. Some participants said they shared information that they thought was useful to the third parties based on the purpose they stated in the request; we speculate that some participants did not think major was relevant to be shared with the third parties. Weight and health goals was shared less with the public than with the third parties; we speculate that participants might have considered this information useful to the third parties and that they were concerned about sharing this sensitive information with the public.

Table 8: Final normalized sharing scores for personal characteristics

	Family	Friends
Characteristics	0.91 (0.23)	0.83 (0.26)
Age	0.96 (0.19)	0.94 (0.21)
Gender	0.93 (0.27)	0.91 (0.28)
Major	0.94 (0.21)	0.91 (0.25)
Height	0.93 (0.27)	0.87 (0.33)
Weight	0.83 (0.37)	0.64* (0.46)
Activity	0.93 (0.27)	0.83 (0.37)
Goals	0.85 (0.36)	0.73 (0.42)

† Sharing scores of family and friends are different, $p \leq 0.1$

* Sharing scores of family and friends are different, $p \leq 0.05$

** Sharing scores of family and friends are different, $p \leq 0.01$

Table 9: Final normalized sharing scores for activity information

	Public	Third Parties
Steps	0.89 (0.27)	0.89 (0.25)
Calories	0.89 (0.27)	0.89 (0.25)
Sleep	0.87 (0.30)	0.87 (0.29)

† Sharing scores of third parties and public are different, $p \leq 0.1$
* Sharing scores of third parties and public are different, $p \leq 0.05$
** Sharing scores of third parties and public are different, $p \leq 0.01$

Comparing final sharing scores for family and friends with public and third parties. Table 11 shows the final sharing scores for activity information for family and public. As we expected, participants shared more activity information with family than with the public. Participants said that they felt more comfortable sharing their activity information with people they knew because sharing it with strangers made them feel like they were being watched. But from Table 12, which shows the final sharing scores for activity information for friends and public, we found that there was no statistically significant difference in the sharing scores for steps and calories. Some participants said that they had a different relationship with their family and their friends (some were closer to friends and others closer to their family), which affected the way they shared their

Table 10: Final normalized sharing scores for personal characteristics

	Public	Third Parties
Characteristics	0.80	0.83
	(0.29)	(0.32)
Age	0.89	0.87
	(0.31)	(0.34)
Gender	0.92	0.89
	(0.28)	(0.31)
Major	0.98	0.82*
	(0.16)	(0.38)
Height	0.84	0.84
	(0.37)	(0.37)
Weight	0.59	0.74*
	(0.50)	(0.43)
Activity	0.84	0.84
	(0.37)	(0.36)
Goals	0.68	0.82*
	(0.48)	(0.38)

† Sharing scores of third parties and public are different, $p \leq 0.1$

* Sharing scores of third parties and public are different, $p \leq 0.05$

** Sharing scores of third parties and public are different, $p \leq 0.01$

Table 11: Final normalized sharing scores for activity information (family and public)

	Family	Public
Steps	0.96 (0.19)	0.91* (0.22)
Calories	0.96 (0.19)	0.89* (0.25)
Sleep	0.96 (0.19)	0.87* (0.30)

† Sharing scores of family and public are different, $p \leq 0.1$
* Sharing scores of family and public are different, $p \leq 0.05$
** Sharing scores of family and public are different, $p \leq 0.01$

steps and calories with them.

Again, as expected, from Table 13, we found that sharing scores for personal characteristics was significantly more for family than for the public; some participants said that they shared their personal characteristics with family members because their family members already knew most of their personal characteristics. We expected participants to hide their identifying characteristics (age, gender, major) from the public, but there is no significant difference in the way this information was shared with family and the public; some participants said during the interviews that they hid their identifying characteristics from the public.

Table 14 shows the final sharing scores for personal characteristics for friends and public.

Table 12: Final normalized sharing scores for activity information (friends and public)

	Friends	Public
Steps	0.95	0.91
	(0.14)	(0.21)
Calories	0.95	0.90
	(0.17)	(0.25)
Sleep	0.95	0.87*
	(0.16)	(0.29)

† Sharing scores of friends and public are different, $p \leq 0.1$
* Sharing scores of friends and public are different, $p \leq 0.05$
** Sharing scores of friends and public are different, $p \leq 0.01$

Suprisingly, sharing score for major was significantly higher for public than for friends. The sharing score for health goals was more for friends than the public; we speculate that some participants considered health goals to be sensitive and did not want to share this information with strangers. But it is suprising that there is no statistically significant difference in the sharing scores for weight for friends and public; this implies that most participants were concerned about sharing their weight with the friends to the same degree as they would be concerned about sharing it with strangers. Many participants said that they were concerned about sharing their weight with their friends, for fear of being judged by them.

Tables 15 and 16 show final sharing scores for activity information for family, friends and third

Table 13: Final normalized sharing scores for personal characteristics (family and public)

	Family	Public
Characteristics	0.91	0.78 *
	(0.23)	(0.29)
Age	0.96	0.93
	(0.19)	(0.26)
Gender	0.93	0.93
	(0.26)	(0.26)
Major	0.95	1.00
	(0.21)	(0.00)
Height	0.93	0.82
	(0.26)	(0.39)
Weight	0.84	0.54 **
	(0.36)	(0.51)
Activity	0.93	0.82
	(0.26)	(0.39)
Goals	0.86	0.61 *
	(0.36)	(0.50)

† Sharing scores of family and public are different, $p \leq 0.1$
* Sharing scores of family and public are different, $p \leq 0.05$
** Sharing scores of family and public are different, $p \leq 0.01$

Table 14: Final normalized sharing scores for personal characteristics (friends and public)

	Friends	Public
Characteristics	0.84	0.77
	(0.26)	(0.29)
Age	0.95	0.90
	(0.20)	(0.31)
Gender	0.91	0.93
	(0.27)	(0.26)
Major	0.91	1.00 †
	(0.24)	(0.00)
Height	0.88	0.83
	(0.32)	(0.38)
Weight	0.63	0.52
	(0.46)	(0.51)
Activity	0.85	0.83
	(0.36)	(0.38)
Goals	0.75	0.62 †
	(0.41)	(0.49)

† Sharing scores of friends and public are different, $p \leq 0.1$

* Sharing scores of friends and public are different, $p \leq 0.05$

** Sharing scores of friends and public are different, $p \leq 0.01$

Table 15: Final normalized sharing scores for activity information (family and third parties)

	Family	Third parties
Steps	0.96 (0.19)	0.90 (0.23)
Calories	0.96 (0.19)	0.90 (0.22)
Sleep	0.96 (0.19)	0.88 (0.29)

[†] Sharing scores of family and third parties are different, $p \leq 0.1$
[*] Sharing scores of family and third parties are different, $p \leq 0.05$
[**] Sharing scores of family and third parties are different, $p \leq 0.01$

parties. We discovered that the participants shared activity information similar to the way they shared it with family and friends and the public. Participants said that they felt more comfortable sharing their activity information with people they knew because sharing it with strangers made them feel like they were being watched.

Tables 17 and 18 shows the final sharing scores for personal characteristics for family, friends and third parties. There was no statistically significant difference between the sharing scores for characteristics for family and third parties, except for major. There was no significant difference between the sharing scores for characteristics for friends and third parties, but the sharing scores for weight and health goals were less for friends than for third parties; some participants said that

Table 16: Final normalized sharing scores for activity information (friends and third parties)

	Friends	Third parties
Steps	0.96 (0.19)	0.88 (0.29)
Calories	0.95 (0.17)	0.91 (0.21)
Sleep	0.95 (0.16)	0.89 (0.28)

† Sharing scores of friends and third parties are different, $p \leq 0.1$
* Sharing scores of friends and third parties are different, $p \leq 0.05$
** Sharing scores of friends and third parties are different, $p \leq 0.01$

they were concerned about sharing certain embarassing information with their friends, because they saw their friends on a daily basis, whereas they were comfortable sharing this information with strangers, because strangers did not know who the participants are.

Comparing group sharing scores based on gender. Tables 19 show some of the group sharing scores for male and female participants. Females were more concerned than males about sharing their personal characteristics and potentially embarassing information like their weight, goals and self-reported activity level.

Comparing group sharing scores based on profession. Table 20 shows some group sharing

Table 17: Final normalized sharing scores for personal characteristics (family and third parties)

	Family	Third parties
Characteristics	0.91 (0.23)	0.81 (0.32)
Age	0.96 (0.19)	0.86 (0.35)
Gender	0.93 (0.27)	0.89 (0.32)
Major	0.94 (0.21)	0.79 † (0.40)
Height	0.93 (0.27)	0.81 (0.40)
Weight	0.83 (0.37)	0.72 (0.45)
Activity	0.93 (0.27)	0.82 (0.38)
Goals	0.85 (0.36)	0.79 (0.40)

† Sharing scores of family and third parties are different, $p \leq 0.1$

* Sharing scores of family and third parties are different, $p \leq 0.05$

** Sharing scores of family and third parties are different, $p \leq 0.01$

Table 18: Final normalized sharing scores for personal characteristics (friends and third parties)

	Friends	Third parties
Characteristics	0.84	0.82
	(0.26)	(0.31)
Age	0.95	0.87
	(0.20)	(0.34)
Gender	0.91	0.90
	(0.27)	(0.30)
Major	0.91	0.81
	(0.24)	(0.39)
Height	0.88	0.83
	(0.32)	(0.38)
Weight	0.63	0.71
	(0.46)	(0.45)
Activity	0.85	0.83
	(0.36)	(0.37)
Goals	0.75	0.80
	(0.41)	(0.39)

† Sharing scores of friends and third parties are different, $p \leq 0.1$

* Sharing scores of friends and third parties are different, $p \leq 0.05$

** Sharing scores of friends and third parties are different, $p \leq 0.01$

Table 19: Final sharing scores based on gender

	Female	Male
score(u,‘Friends’,‘Characteristics’,5)	0.78	0.95 †
score(u,‘Public’,‘Characteristics’,5)	0.75	0.93 †
score(u,‘TP’,‘Characteristics’,5)	0.77	0.95 †
score(u,‘Friends’,‘Weight’,5)	0.47	0.95 **
score(u,‘TP’,‘Weight’,5)	0.65	0.92 *
score(u,‘Public’,‘Weight’,5)	0.46	0.92 **
score(u,‘Public’,‘Level’,5)	0.79	1.00 †
score(u,‘TP’,‘Level’,5)	0.76	1.00 †
score(u,‘Friends’,‘Goals’,5)	0.64	0.95 *

† Sharing scores of females and males are different, $p \leq 0.1$
* Sharing scores of females and males are different, $p \leq 0.05$
** Sharing scores of females and males are different, $p \leq 0.01$

scores for students and retirees. We only show those cases with a statistically significant difference. Students were much more concerned than retirees about sharing their personal characteristics, weight and goals with the public.

Table 21 shows some group sharing scores for students and employees. Again we only show those cases with a statistically significant difference. Students were less concerned than employees about sharing their weight with family, but much more concerned about sharing health goals with

Table 20: Final sharing scores based on profession

	Students	Retirees
scores(u,‘Public’,‘Characteristics’,5)	0.74	1.00 †
scores(u,‘Public’,‘Weight’,5)	0.48	1.00 *
scores(u,‘Public’,‘Goals’,5)	0.48	1.00 *

† Sharing scores of students and retirees are different, $p \leq 0.1$
* Sharing scores of students and retirees are different, $p \leq 0.05$
** Sharing scores of students and retirees are different, $p \leq 0.01$

Table 21: Final sharing scores based on profession

	Students	Employees
scores(u,‘Family’,‘Weight’,5)	0.90	0.50 †
scores(u,‘Public’,‘Goals’,5)	0.48	0.83 †

† Sharing scores of students and employees are different, $p \leq 0.1$
* Sharing scores of students and employees are different, $p \leq 0.05$
** Sharing scores of students and employees are different, $p \leq 0.01$

the public.

4.3.2 Post-study Interviews

We asked the participants a set of questions when they returned the device after the five days. We asked them about their opinion about the Fitbit, what they shared with others and how they shared the information and how they would share other types of health information. Please refer to Appendix C, Section C.2 for the questions. The interviews lasted typically for about 15 minutes. We recorded the interviews. We coded the interviews manually and grouped the statements into categories. We do not talk about their opinion about Fitbits here, but we discuss below their reasons for sharing and not sharing their health information.

Collection of health information. A few students were concerned about the device recording information while they were at parties or staying up late. A male employee asked, *"would it be something you would keep on during sexual activity or when you go to the bathroom?"*

Sharing information. 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.

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 actally needed it for medical purposes."*

A few students felt their information would not be linked to them, 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."*

Some participants considered the third parties differently. 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]."

Three participants mentioned that they felt the information was not sensitive, because the device collected information only for five 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."* One participant mentioned that study participants expected their information to be shared, *"When you say a study, people kind of expect their information to be shared, they don't volunteer unless they want their information to be shared, so I think you kind of got a pre-selected group of people."*

A female student shared her activity information with third parties, because according to her, *"when I was wearing it 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 ones going to use it, it was all for nothing kind of thing."* One employee, being a researcher, was open to sharing her health information with other researchers.

Hiding information. 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.

Some students did not want to share their activity 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."*. 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."*

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."*

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."*

One elderly retiree was not tech-savvy and her husband was helping her manage her Fitbit account. He did not want her to share her information with anyone.

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 dont 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 didnt 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 dont 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 *"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 them."* *"Because my parents are people who are big on exercise. If I don't do much exercise, they wouldn't like that."* "

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." "People who don't know me it would be fine. My age doesn't 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 reseearch I have no problem. It is just third-party companies* [that I wouldn't want to have the data]."

Information types. 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"*.

4.4 Limitations

Table 2 showed the number of family members and friends that participants chose to share their Fitbit information with. Students were used to participating in studies and abiding by the rules, so all of them chose at least one family member and two friends to share their information with, while 58% of the working group and 63% of retired participants did not select any family members and 42% of the working group and 75% of the retired participants did not select any friends; they either refused to choose partners or could not come up with names of friends and family members they wanted to share the Fitbit information with. Some participants did not see the third-party requests, because they were more focused on collecting information and did not use the web interface much; they could see the number of steps they took on the device itself.

Most of the students were active and fit; some of them were athletes, which could be why they were not concerned about their activity information. Participants might have made sharing decisions different from what they might make in real-life scenarios because they participated in a study that was conducted by people they trusted and their data was collected only for five days. Some participants could not articulate certain sharing behavior, while others forgot why they made certain sharing decisions.

5 Discussion

Our findings correlated with the results from studies conducted by others. We found that some of the focus-group and study participants were concerned about sharing activity, location and social interactions with others and also about sharing such information with third-party researchers and the public, similar to what was discovered by Raij et al. [30]. Participants' privacy concerns depended on what information was being collected and some were concerned about context in which it was collected, similar to what was found by Klasnja et al. [23]. A few participants' behavior was similar to what was discovered by Olson et al. (some participants shared personal information similarly with friends and family members) [28] and Maitland et al.(some participants were open to sharing their activity information with peers) [21].

From the focus groups, we found that Patients made sharing decisions based on the relationships they had with their sharing partners. The results from the user study supported this observation as well. From the post-study interviews, we learned that the participants shared their health information with family and friends, based on their relationship with them. Some were embarassed about sharing their weight and health goals with their friends or were concerned about sharing their activity information with their family, while other participants were more comfortable sharing this information with friends and family than with strangers. Most participants shared more information with third parties than with the public, because they wanted to support the research done by the third parties whereas they did not know what strangers among the public might do if they had access to the information. Even when they supported the purpose behind a third-party request, some participants did not share all the information with the third parties; they shared what they thought was sufficient for use by third parties. Some participants hid personal characteristics from the public; information that they thought strangers might use to identify them, whereas some hid activity information from the public, because they felt like someone was watching their every move.

mHealth system developers can develop privacy controls by understanding what aspect of the health information Patients consider as sensitive. The information might be considered sensitive depending on how it was collected (periodic, continuous), where it was collected (at home, at work, etc) or what activity the Patient was doing when it was collected and so on. An mHealth system should also define different granularities for the health information it collects, so that Patients who do want to change default sharing settings have more control over the information they are sharing. By default, the system could provide time-based granularities, like we did for the user study. Patients should be able to share a monthly, weekly, daily, hourly summary, or a detailed version of their information, as well as define custom time periods to share information collected during those periods of time. During the focus groups and post-study interviews, participants talked about the need for context-based sharing (some students talked about hiding information that was collected while they were partying, from their parents). For context-based sharing, the system could provide "sharing contexts" like information collected at home, activity information when you were running, etc. To provide context-based sharing, however, the mHealth device needs to collect context along with the Patient's health information. Another way of limiting the information that is shared is by sharing statistics of the information, like maximum, minimum, mean, sum (similar to the temporal summaries we provided in our study) or even a range of the values that was collected for that information; some participants were more comfortable sharing such statistics with third parties.

How can mHealth system developers use the information that we learned from the focus groups and the user study? From the study, we discovered that there was a huge variation in the way the participants shared their information; we cannot have fixed default settings for mHealth systems. The system needs flexible interfaces, since one standard setting is not going to work for every Patient. It will be interesting to see if default settings could be generated based on a Patient's age, gender and health experience, but we will need to conduct more studies to understand whether this is possible. Before the study, we were unsure what the privacy risks are with sharing this information. In the user study, we learned what participants perceived as the privacy risks and how these perceptions influenced their sharing behavior.

We found that 15 out of 41 participants never changed the default sharing settings, either because they did not care about their privacy, they were lazy or too busy to log in to the website, they did not understand the controls or because they had no sharing partners. mHealth systems should provide sensible default settings, to protect the privacy of Patients who do not change default sharing settings. Default settings could also guide the sharing behavior of Patients who are concerned about unintended disclosure of their information. We suggest possible default settings for mHealth systems based on the findings from the focus groups and the user study, as follows.

Sharing with family and friends. Young and middle-aged Patients share information with family and friends based on their relationship with them. Most of them will want to hide embarassing and sensitive information from their family and friends, but none of them will mind sharing identifying information with family and friends. For example, as we discovered during the user study, some participants wanted to hide their weight from family and friends, but shared their age and gender. From the focus groups and from the interviews, we also learned that young and middle-aged Patients do not want to share sensitive information, like their medication and location information, with their family and friends. They also were comfortable sharing their activity information with family and friends, perhaps without realizing the inferences about their lives that can be made from this information. To protect their privacy, the system should share, by default, seemingly insensitive information at a higher granularity (less detail) with family and friends.

Elderly Patients, especially those who have suffered some serious health issues, do not consider health information as sensitive, though they might not want to share it with their family and friends because they do not want to feel dependent on anyone. Many, however, would share the information with their caregiver, someone who takes care of them and would like to know how well they are doing. So the system should ask the elderly Patient to name their caregiver(s) and initially share a detailed version of their health information with just that person(s).

Sharing with third parties. Most user-study participants wanted to share all their information with the third parties, because they supported research. But as one participant noted, people volunteer to participate in studies knowing that their information will be shared. Other participants mentioned that they shared information with third parties only to the detail that they thought the third parties might need. To protect Patient privacy, mHealth systems should by default share only a summary of the Patient health information with such third parties. On the other hand, it may be necessary to explain to Patients what information is needed and why.

Sharing with the public Most participants chose to share some information with the public, so mHealth systems should by default share only a summary of the Patient health information with the public.

Sharing with doctors. From the focus groups, we learned that all participants wanted to share their medication information with their doctor, including information about drugs and alcohol. However, they were not comfortable sharing personal information like their location with their doctor. By default, mHealth systems should share with doctors only information relevant to the Patient's treatment. This approach is challenging, since even doctors might not know in advance what information might be relevant to the Patient's treatment.

Every Patient is different and will have different privacy preferences. We suggested default sharing settings and different granularities to meet the sharing needs of most Patients. Patients who are more concerned about how the information is shared will explore the available settings and might change the default settings using the controls provided by the system. Patients who are less concerned about how the information is shared may be satisfied with the default settings.

6 Future Work

There are still several challenges to be solved. The system must display all the information that is being shared and with whom it is being shared and how, so that the Patient can change the sharing settings, if necessary. How can the information be presented in a concise manner, without overwhelming the Patient with long lists and choices? How well do Patients understand the choices and risks of different choices? When we conduct studies on privacy and Patients' willingness to share, what incentives should we provide the participants so that they do not over or under-share? A follow-up study could test whether participants prefer default settings that we suggested over the usual share-all or share-none settings. Another study could be conducted to learn more about the different granularities at which Patients want to share their information. What other tools are required to help concerned Patients map their privacy preferences to the sharing settings? A follow-up study could test whether Patients will share more or less if they have feedback about who is actually viewing the shared information. Can a system learn Patients' privacy preferences, so that it can choose the sharing settings on behalf of the Patient, when the Patient shares some information with a new partner? Do users' sharing behaviors change over time? After what time do they stop changing their sharing settings? Is it possible for a system to learn the Patient's relationship with the people she chooses as sharing partners? How well do our results extend to other kinds of mHealth sensing, to other types of health data?

7 Summary

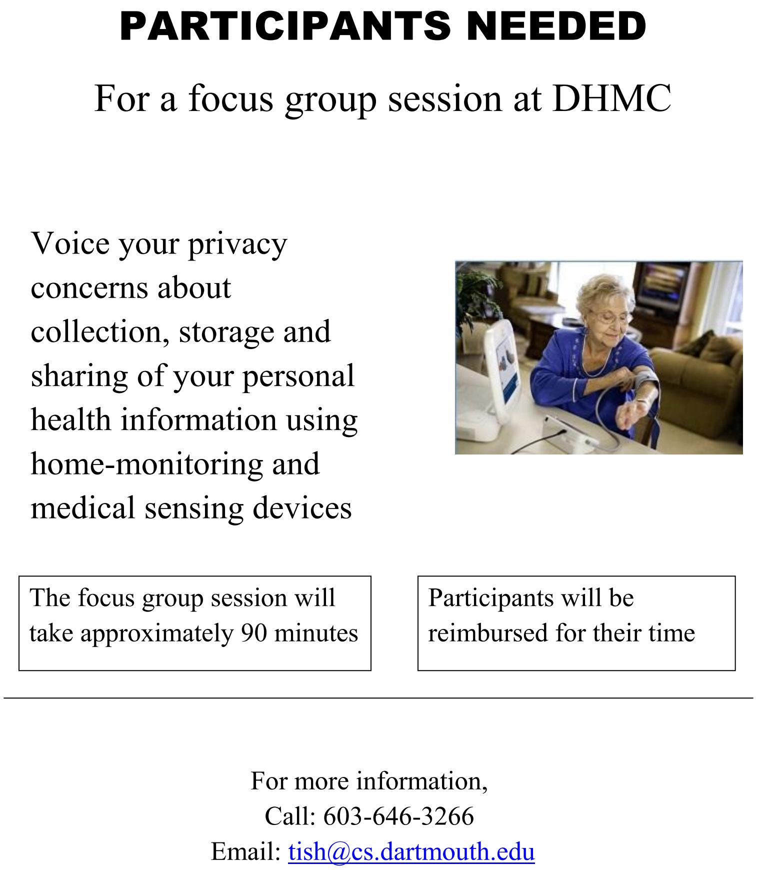
It is important to understand Patients' views of the benefits and risks of mHealth technology and what controls they want over their personal health information collected using mHealth devices. We conducted focus groups with students, hospital outpatients and residents of a retirement home to understand what privacy concerns Patients might have regarding the collection, storage and sharing of their personal health information using mHealth devices. Since focus groups were based on hypothetical devices, the views expressed by the participants did not reflect how Patients might behave when they share their health information that was collected using mHealth devices that they carried at all times. So we conducted a user study to understand how willing Patients were to share their personal health information that they collected using an mHealth device that they carried with them at all times for five days. We discovered that the participants were more concerned about sharing their health information with the public than with third parties and they wanted to hide certain information from their family and friends. Based on these discoveries, we suggest methods to develop expressive privacy controls and sensible default sharing settings for mHealth systems. We expect our work to help the development of mHealth systems in the future.

Appendix

A Focus Group

A.1 Flyers

Figure 4: Flyer distributed among hospital outpatients



PARTICIPANTS NEEDED

For a focus group session at DHMC

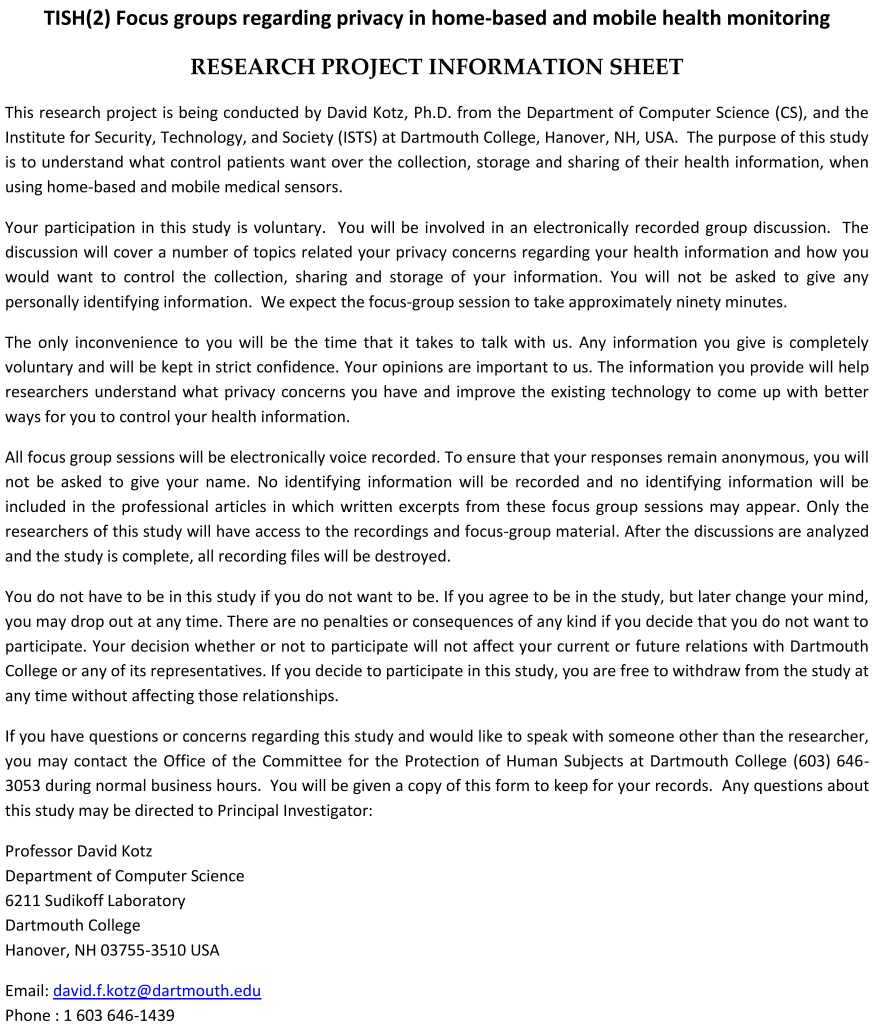
Voice your privacy concerns about collection, storage and sharing of your personal health information using home-monitoring and medical sensing devices

The focus group session will take approximately 90 minutes

Participants will be reimbursed for their time

For more information,
Call: 603-646-3266
Email: tish@cs.dartmouth.edu

Figure 5: Information sheet attached to the flyer



TISH(2) Focus groups regarding privacy in home-based and mobile health monitoring

RESEARCH PROJECT INFORMATION SHEET

This research project is being conducted by David Kotz, Ph.D. from the Department of Computer Science (CS), and the Institute for Security, Technology, and Society (ISTS) at Dartmouth College, Hanover, NH, USA. The purpose of this study is to understand what control patients want over the collection, storage and sharing of their health information, when using home-based and mobile medical sensors.

Your participation in this study is voluntary. You will be involved in an electronically recorded group discussion. The discussion will cover a number of topics related your privacy concerns regarding your health information and how you would want to control the collection, sharing and storage of your information. You will not be asked to give any personally identifying information. We expect the focus-group session to take approximately ninety minutes.

The only inconvenience to you will be the time that it takes to talk with us. Any information you give is completely voluntary and will be kept in strict confidence. Your opinions are important to us. The information you provide will help researchers understand what privacy concerns you have and improve the existing technology to come up with better ways for you to control your health information.

All focus group sessions will be electronically voice recorded. To ensure that your responses remain anonymous, you will not be asked to give your name. No identifying information will be recorded and no identifying information will be included in the professional articles in which written excerpts from these focus group sessions may appear. Only the researchers of this study will have access to the recordings and focus-group material. After the discussions are analyzed and the study is complete, all recording files will be destroyed.

You do not have to be in this study if you do not want to be. If you agree to be in the study, but later change your mind, you may drop out at any time. There are no penalties or consequences of any kind if you decide that you do not want to participate. Your decision whether or not to participate will not affect your current or future relations with Dartmouth College or any of its representatives. If you decide to participate in this study, you are free to withdraw from the study at any time without affecting those relationships.

If you have questions or concerns regarding this study and would like to speak with someone other than the researcher, you may contact the Office of the Committee for the Protection of Human Subjects at Dartmouth College (603) 646-3053 during normal business hours. You will be given a copy of this form to keep for your records. Any questions about this study may be directed to Principal Investigator:

Professor David Kotz
Department of Computer Science
6211 Sudikoff Laboratory
Dartmouth College
Hanover, NH 03755-3510 USA

Email: david.f.kotz@dartmouth.edu
Phone : 1 603 646-1439

Figure 6: Flyer put up on Dartmouth campus

PARTICIPANTS NEEDED

For a focus group session at
Sudikoff Lab, Dartmouth College

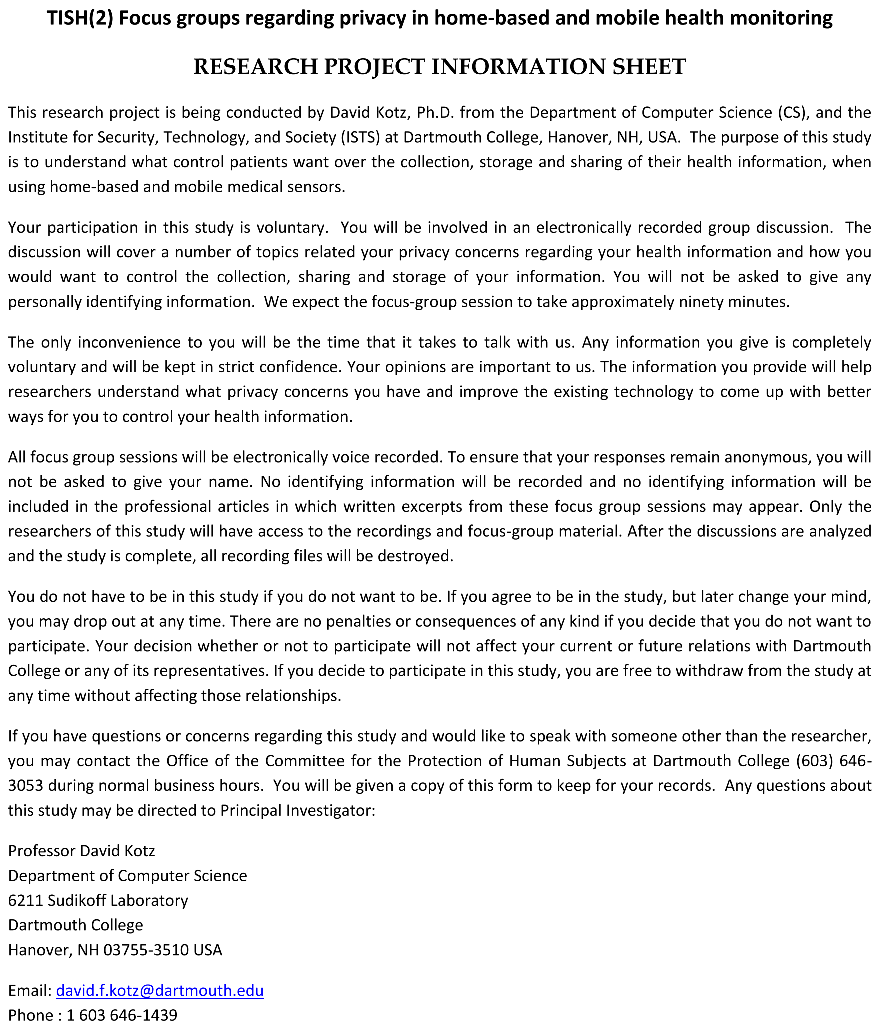
Voice your privacy concerns about collection, storage and sharing of your personal health information using health monitoring devices

The focus group session will take approximately 90 minutes

Participants will be reimbursed for their time

For more information,
Call: 603-646-3266
Email: tish@cs.dartmouth.edu

Figure 7: Information sheet attached to the flyer



TISH(2) Focus groups regarding privacy in home-based and mobile health monitoring

RESEARCH PROJECT INFORMATION SHEET

This research project is being conducted by David Kotz, Ph.D. from the Department of Computer Science (CS), and the Institute for Security, Technology, and Society (ISTS) at Dartmouth College, Hanover, NH, USA. The purpose of this study is to understand what control patients want over the collection, storage and sharing of their health information, when using home-based and mobile medical sensors.

Your participation in this study is voluntary. You will be involved in an electronically recorded group discussion. The discussion will cover a number of topics related your privacy concerns regarding your health information and how you would want to control the collection, sharing and storage of your information. You will not be asked to give any personally identifying information. We expect the focus-group session to take approximately ninety minutes.

The only inconvenience to you will be the time that it takes to talk with us. Any information you give is completely voluntary and will be kept in strict confidence. Your opinions are important to us. The information you provide will help researchers understand what privacy concerns you have and improve the existing technology to come up with better ways for you to control your health information.

All focus group sessions will be electronically voice recorded. To ensure that your responses remain anonymous, you will not be asked to give your name. No identifying information will be recorded and no identifying information will be included in the professional articles in which written excerpts from these focus group sessions may appear. Only the researchers of this study will have access to the recordings and focus-group material. After the discussions are analyzed and the study is complete, all recording files will be destroyed.

You do not have to be in this study if you do not want to be. If you agree to be in the study, but later change your mind, you may drop out at any time. There are no penalties or consequences of any kind if you decide that you do not want to participate. Your decision whether or not to participate will not affect your current or future relations with Dartmouth College or any of its representatives. If you decide to participate in this study, you are free to withdraw from the study at any time without affecting those relationships.

If you have questions or concerns regarding this study and would like to speak with someone other than the researcher, you may contact the Office of the Committee for the Protection of Human Subjects at Dartmouth College (603) 646-3053 during normal business hours. You will be given a copy of this form to keep for your records. Any questions about this study may be directed to Principal Investigator:

Professor David Kotz
Department of Computer Science
6211 Sudikoff Laboratory
Dartmouth College
Hanover, NH 03755-3510 USA

Email: david.f.kotz@dartmouth.edu
Phone : 1 603 646-1439

B Scenarios for focus group participants

Figure 8: Scenarios for pilot study

Post-surgery Home Monitoring

Following minor surgery Jane returns home after recuperating in the hospital for one day. Usually patients must go back to see the doctor at 2-days post-surgery, then at 1-week, then again at 2-weeks post-surgery. But Jane has been given the choice to use a device that she wears on her arm with sensors that monitor her vital signs (including body temperature, blood pressure, breathing rate and heart rate). There is no cost to Jane to use the device.

Jane needs to wear the device for 8 hours/day between the hours of 7am and 10pm. The device periodically sends her vital sign readings (via electronic/internet transmission) to her electronic medical record at her doctor's office. A nurse is available to communicate with Jane if any problems are found and if the doctor would like her to come in for a visit.

Post-surgery Home Monitoring

Following minor surgery Jane returns home after recuperating in the hospital for one day. Usually patients must go back to see the doctor at 2-days post-surgery, then at 1-week, then again at 2-weeks post-surgery. But Jane has been given the choice to use a device that she wears on her arm with sensors that monitor her vital signs (including body temperature, blood pressure, breathing rate and heart rate). There is no cost to Jane to use the device.

Jane needs to wear the device for 24 hours/day. The device periodically sends her vital sign readings (via electronic/internet transmission) to her electronic medical record at her doctor's office. A nurse is available to communicate with Jane if any problems are found and if the doctor would like her to come in for a visit.

Managing your medications

James has a chronic condition (e.g., heart disease, high blood pressure, arthritis) that requires he take two different medications each day at specific times. Sometimes James forgets to take his medication, or has an activity that makes it difficult to take it as recommended. Each medication has side effects that make James sometimes not want to take it.

James' doctor has offered him the option to use a new wearable device that will monitor whether he takes his medication as recommended. It will give feedback to James so he can monitor himself, and to his doctor so the doctor can monitor how consistently he takes his medication. There is no cost to James to use the device. James needs to wear the device every day. The device periodically sends data about his medication use (via electronic/internet transmission) to a private website that both he and his doctor can access to see how he is doing. His doctor typically checks the website when James comes in for a visit to review how well the medication is working.

Diet and Exercise

Jonah had a heart attack and is now working with his doctor and others to change his diet and exercise patterns so that he can lose weight. In addition to working with a nutritionist and taking an exercise class, his doctor has offered him the option to use a new wearable device that will monitor both his daily calories and his level of movement each day. It will give feedback to Jonah so he can monitor himself, and to his care givers so they can monitor how consistently he sticks to his diet and exercise plan (and when and why he might deviate from the plan). There is no cost to Jonah to use the device.

Jonah needs to wear the device every day. The device periodically sends data about his calories and exercise (via electronic/internet transmission) to a private website that both he and his caregivers can access to see how he is doing. Jonah can look at the website to see how his behavior this week compares to previous weeks. If he chose to do so, he can also compare his progress with those of others like himself. His nutritionist typically checks the website when Jonah comes in for a visit.

Figure 9: Scenarios for young participants

Managing your medications

James has a chronic condition (e.g., diabetes, ADHD, allergies) that requires he take two different medications each day at specific times. Sometimes James forgets to take his medication, or has an activity that makes it difficult to take it as recommended. Each medication has side effects that make James sometimes not want to take it.

James' doctor has offered him the option to use a new wearable device that will monitor whether he takes his medication as recommended. It will give feedback to James so he can monitor himself, and to his doctor so the doctor can monitor how consistently he takes his medication. There is no cost to James to use the device.
James needs to wear the device every day. The device periodically sends data about his medication use (via electronic/internet transmission) to a private website that both he and his doctor can access to see how he is doing. His doctor typically checks the website when James comes in for a visit to review how well the medication is working.

Diet and Exercise

Jane has been diagnosed with diabetes and wants to lose weight. She is now working with her doctor and others to change her diet and exercise patterns. In addition to working with a nutritionist and taking an exercise class, her doctor has offered her the option to use a new wearable device that will monitor both her daily calories and her level of movement each day. It will give feedback to Jane so she can monitor herself, and to her doctor so he can monitor how consistently she sticks to her diet and exercise plan (and encourage her not to when she might deviate from the plan). There is no cost to Jane to use the device.

Jane needs to wear the device every day. The device periodically sends data about her calories and exercise (via electronic/internet transmission) to a private website that both she and her caregivers can access to see how she is doing. Jane can look at the website to see how her behavior this week compares to previous weeks. If she chose to do so, she can also compare her progress with those of others like herself. Her nutritionist typically checks the website when Jane comes in for a visit.

Allergies

As spring approaches, Joan worries about allergies. She is not sure what she is allergic to and what place she should stay away from. Her doctor advises her to use a device that would record all the places she goes to. It will check for allergy symptoms and track their onset as well. The mobile health device is free of cost.

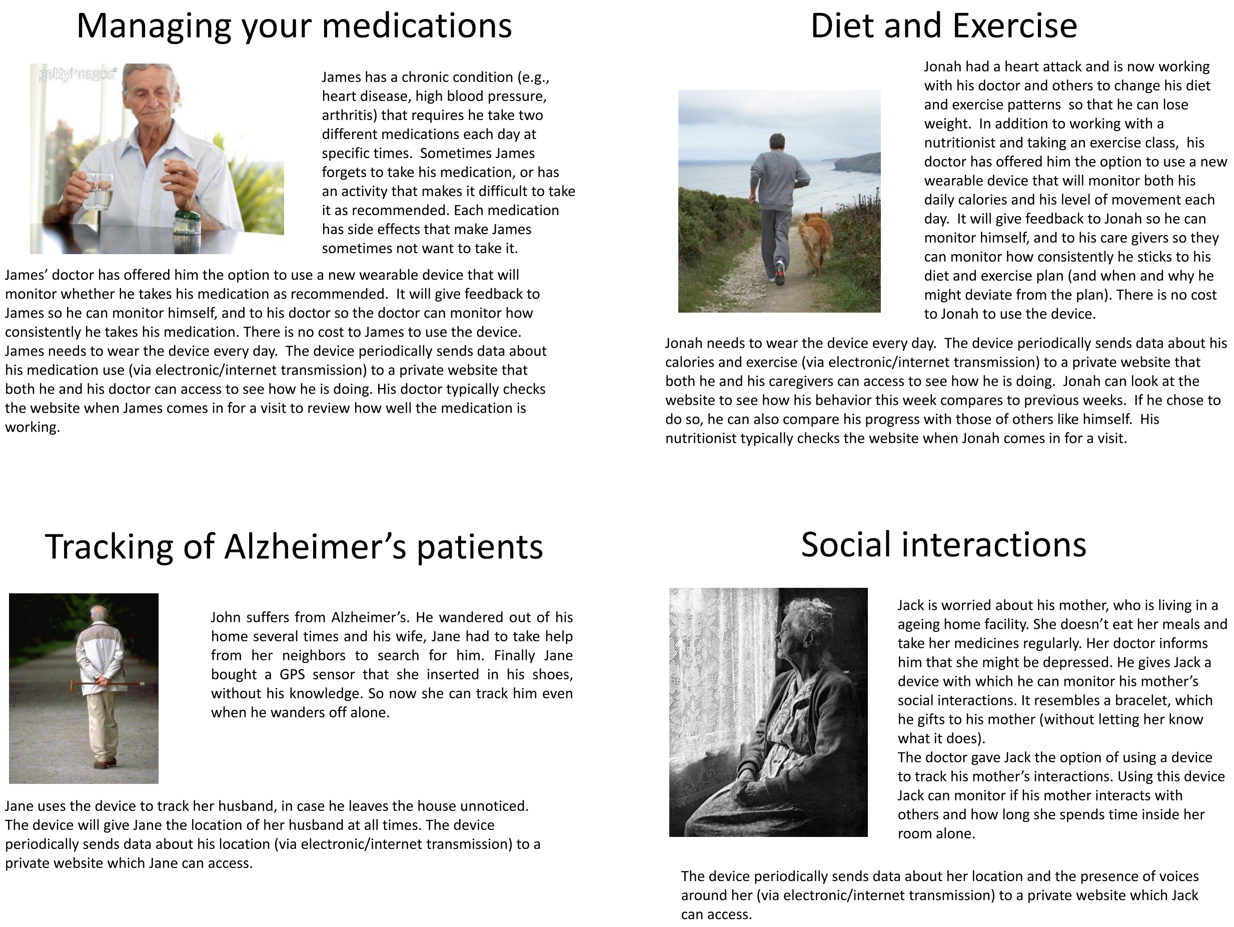
Joan's doctor gives her the option to use the device to track the onset of her allergy symptoms and hopefully determine their cause. It will give feedback to Joan so she can monitor herself. Joan needs to wear the device every day and at all times, till the source of her allergies is discovered. The device periodically sends data about her location and allergy symptoms (via electronic/internet transmission) to a private website that both she and her doctor can access. Her doctor typically checks it only if Joan wants a second opinion.

Social interactions

Jack is caught taking drugs at school. His parents take him to a therapist and she tells them that Jack could be depressed about something. She asks Jack's parents to ask Jack to use a device with which they can monitor if he interacts with others or if he is depressed and shying away from interactions. It can also detect when Jack takes off the device.

The doctor has offered Jack the option to use a new wearable device that will monitor the frequency of interactions he has with others. It will give feedback to Jack's doctor so that they can know whom he interacts with and where he goes. There is no cost to Jack to use the device.
Jack needs to wear the device every day and at all times. The device periodically sends data about his interactions(via electronic/internet transmission) to a private website that his doctor can access to see how he is doing. His doctor typically checks the website when Jack comes in for his therapy session, to check if he interacts more with others.

Figure 10: Scenarios for elderly participants



Managing your medications

James has a chronic condition (e.g., heart disease, high blood pressure, arthritis) that requires he take two different medications each day at specific times. Sometimes James forgets to take his medication, or has an activity that makes it difficult to take it as recommended. Each medication has side effects that make James sometimes not want to take it.

James' doctor has offered him the option to use a new wearable device that will monitor whether he takes his medication as recommended. It will give feedback to James so he can monitor himself, and to his doctor so the doctor can monitor how consistently he takes his medication. There is no cost to James to use the device. James needs to wear the device every day. The device periodically sends data about his medication use (via electronic/internet transmission) to a private website that both he and his doctor can access to see how he is doing. His doctor typically checks the website when James comes in for a visit to review how well the medication is working.

Diet and Exercise

Jonah had a heart attack and is now working with his doctor and others to change his diet and exercise patterns so that he can lose weight. In addition to working with a nutritionist and taking an exercise class, his doctor has offered him the option to use a new wearable device that will monitor both his daily calories and his level of movement each day. It will give feedback to Jonah so he can monitor himself, and to his care givers so they can monitor how consistently he sticks to his diet and exercise plan (and when and why he might deviate from the plan). There is no cost to Jonah to use the device.

Jonah needs to wear the device every day. The device periodically sends data about his calories and exercise (via electronic/internet transmission) to a private website that both he and his caregivers can access to see how he is doing. Jonah can look at the website to see how his behavior this week compares to previous weeks. If he chose to do so, he can also compare his progress with those of others like himself. His nutritionist typically checks the website when Jonah comes in for a visit.

Tracking of Alzheimer's patients

John suffers from Alzheimer's. He wandered out of his home several times and his wife, Jane had to take help from her neighbors to search for him. Finally Jane bought a GPS sensor that she inserted in his shoes, without his knowledge. So now she can track him even when he wanders off alone.

Jane uses the device to track her husband, in case he leaves the house unnoticed. The device will give Jane the location of her husband at all times. The device periodically sends data about his location (via electronic/internet transmission) to a private website which Jane can access.

Social interactions

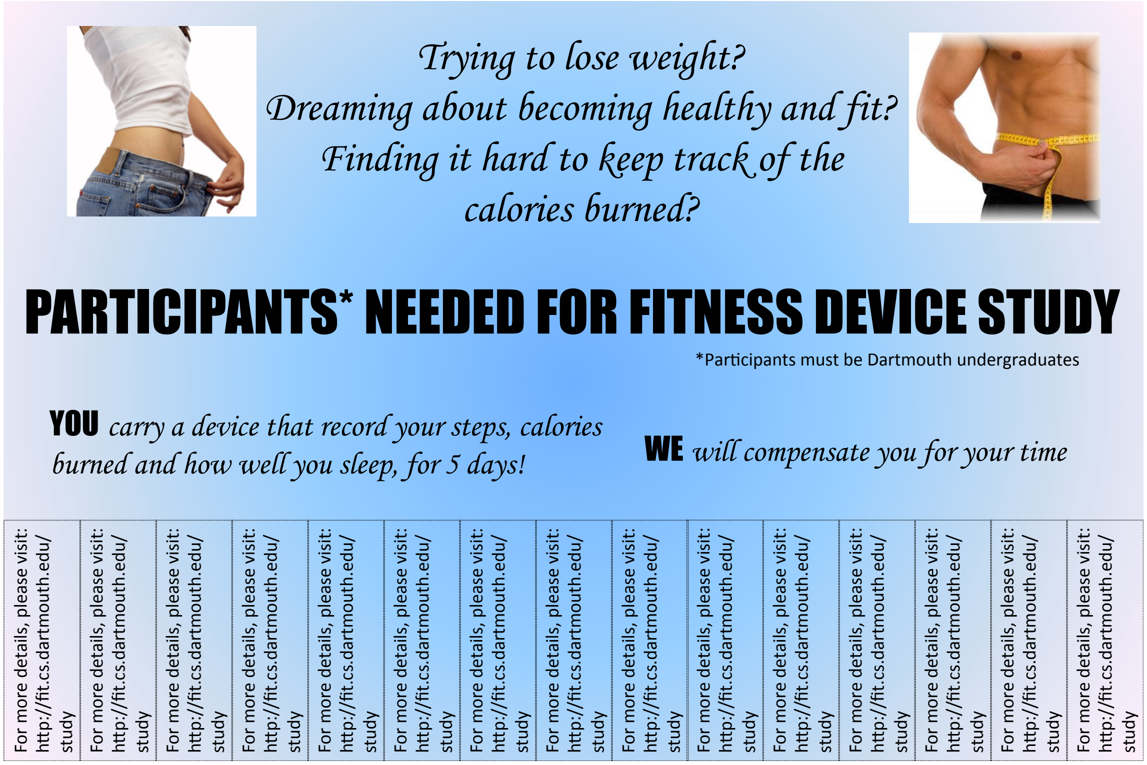
Jack is worried about his mother, who is living in a ageing home facility. She doesn't eat her meals and take her medicines regularly. Her doctor informs him that she might be depressed. He gives Jack a device with which he can monitor his mother's social interactions. It resembles a bracelet, which he gifts to his mother (without letting her know what it does).
The doctor gave Jack the option of using a device to track his mother's interactions. Using this device Jack can monitor if his mother interacts with others and how long she spends time inside her room alone.

The device periodically sends data about her location and the presence of voices around her (via electronic/internet transmission) to a private website which Jack can access.

C User Study

C.1 Flyer

Figure 11: Flyer to recruit Dartmouth students



Trying to lose weight?
Dreaming about becoming healthy and fit?
Finding it hard to keep track of the calories burned?

PARTICIPANTS* NEEDED FOR FITNESS DEVICE STUDY

*Participants must be Dartmouth undergraduates

YOU *carry a device that record your steps, calories burned and how well you sleep, for 5 days!*

WE *will compensate you for your time*

For more details, please visit: http://fit.cs.dartmouth.edu/study

For more details, please visit: http://fit.cs.dartmouth.edu/study

For more details, please visit: http://fit.cs.dartmouth.edu/study

For more details, please visit: http://fit.cs.dartmouth.edu/study

For more details, please visit: http://fit.cs.dartmouth.edu/study

For more details, please visit: http://fit.cs.dartmouth.edu/study

For more details, please visit: http://fit.cs.dartmouth.edu/study

For more details, please visit: http://fit.cs.dartmouth.edu/study

For more details, please visit: http://fit.cs.dartmouth.edu/study

For more details, please visit: http://fit.cs.dartmouth.edu/study

For more details, please visit: http://fit.cs.dartmouth.edu/study

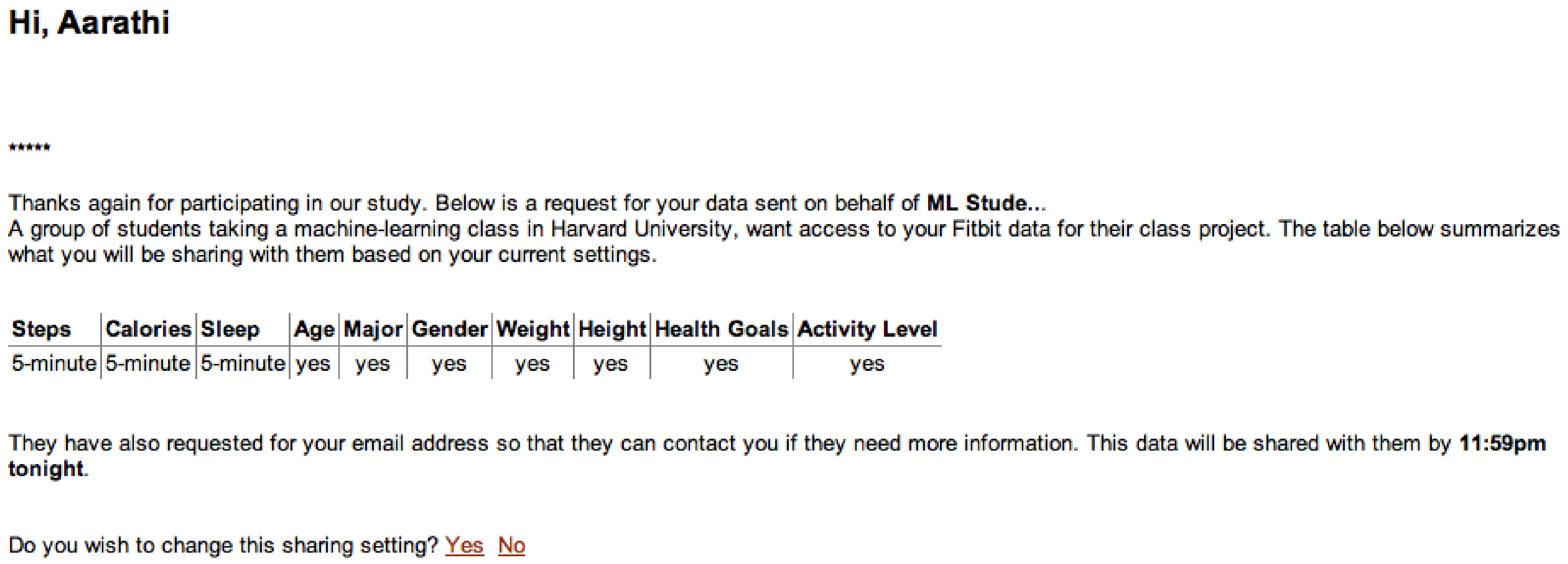
For more details, please visit: http://fit.cs.dartmouth.edu/study

For more details, please visit: http://fit.cs.dartmouth.edu/study

For more details, please visit: http://fit.cs.dartmouth.edu/study

For more details, please visit: http://fit.cs.dartmouth.edu/study

Figure 12: Example request-for-data email sent to study participants



Hi, Aarathi

*****

Thanks again for participating in our study. Below is a request for your data sent on behalf of **ML Stude...**
A group of students taking a machine-learning class in Harvard University, want access to your Fitbit data for their class project. The table below summarizes what you will be sharing with them based on your current settings.

Steps	Calories	Sleep	Age	Major	Gender	Weight	Height	Health Goals	Activity Level
5-minute	5-minute	5-minute	yes	yes	yes	yes	yes	yes	yes

They have also requested for your email address so that they can contact you if they need more information. This data will be shared with them by **11:59pm tonight**.

Do you wish to change this sharing setting? Yes No

C.2 Post-study Interview

1. How was your experience with the Fitbit?
2. Did wearing the device affect how you thought about your sleep, steps or calories? (Were you more aware of these?)
3. Were there instances when you took off the device to prevent it from recording any information? If so:
   (a) What type of information did you not want the device to record?
   (b) Was there a specific person(s) that you did not wish to see any data? Why?
4. Were there instances when you took off the device to hide information about
   (a) Your sleep?
   (b) Your physical activities?
5. Did you ever feel the need to change your habits when you were carrying the device with you? If yes:
   (a) Were there instances when you changed your habits to hide your normal routine?
   (b) What influenced you to change your habits?
   (c) Did you ever feel the need to lie about your habits?
6. Did you change the sharing controls on the interface at any point?
   (a) If so, what influenced that decision?

    (b) Did you change the sharing controls for a particular person(s)? Why?

7. Did your choice of sharing recipients (family/friends) affect how you shared the recorded information?

    (a) If so, how?

8. Did the sharing controls on the interface allow you to set your sharing preferences easily? If no:

    (a) Why not?

    (b) What changes/omissions/additions would you suggest to make the interface more usable?

    (c) If it had been easier to change the privacy preferences, would you have shared differently?

9. Do you want any more control over your information? If so:

    (a) Over which types of information-all, or some?

    (b) Was there information that you felt was more important to control the privacy settings for than others.

10. On a scale of 1 to 10 (1 being highly unlikely and 10 being highly likely), how likely is it that you would use an mHealth device, if it gave you similar sharing controls?

References

[1] Electrodermal Testing and Face Expression Recognition Tools - Affectiva. Online at http://www.affectiva.com/, visited January 2011.

[2] Fitbit. Online at https://www.fitbit.com/, visited January 2011.

[3] Google Health. Online at http://www.google.com/intl/en-US/health/about/, visited January 2011.

[4] Microsoft HealthVault. Online at http://www.healthvault.com/personal/index.aspx, visited January 2011.

[5] Monica Healthcare. Online at http://www.monicahealthcare.com/, visited February 2011.

[6] WakeMate - Wake up fresh; sleep smarter. Online at http://wakemate.com/, visited January 2011.

[7] Body media fit. Online at http://www.bodymedia.com/Products/Learn-More/What-is-BodyMedia-FIT, visited January 2012.

[8] Harris interactive survey. Online at http://www.truste.com/why_TRUSTe_privacy_services/harris-mobile-survey/, visited January 2012.

[9] D. Anthony, T. Henderson, and D. Kotz. Privacy in location-aware computing environments. *IEEE Pervasive Computing*, 6:64–72, 2007. DOI 10.1109/MPRV.2007.83.

[10] M. Benisch, P. G. Kelley, N. Sadeh, T. Sandholm, J. Tsai, L. F. Cranor, and P. H. Drielsma. The Impact of Expressiveness on the Effectiveness of Privacy Mechanisms for Location-Sharing. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM, 2009. DOI 10.1145/1572532.1572561.

[11] J. Birnholtz and M. Jones-Rounds. Independence and Interaction: Understanding Seniors' Privacy and Awareness Needs for Aging in Place. In *Proceedings of the 28th International Conference on Human Factors In Computing Systems (CHI)*, pages 143–152. ACM, 2010. DOI 10.1145/1753326.1753349.

[12] M. T. Britto, T. L. Tivorsak, and G. B. Slap. Adolescents' Needs for Health Care Privacy. *Pediatrics*, 126(6):e1469–1476, December 2010. DOI 10.1542/peds.2010-0389.

[13] K. Connelly, A. Khalil, and Y. Liu. Do I Do What I Say?: Observed Versus Stated Privacy Preferences. In C. Baranauskas, P. Palanque, J. Abascal, and S. Barbosa, editors, *Human-Computer Interaction – INTERACT 2007*, volume 4662 of *Lecture Notes in Computer Science*, chapter 61, pages 620–623. Springer, 2007. DOI 10.1007/978-3-540-74796-3_61.

[14] 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)*, pages 81–90. ACM, 2005. DOI 10.1145/1054972.1054985.

[15] 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. DOI 10.2196/jmir.1053.

[16] HHS. HIPAA website. Online at http://www.hhs.gov/ocr/privacy/., visited March 2010.

[17] HIPAA Survival Guide. The HITECH Act and HIPAA. Online at http://www.hipaasurvivalguide.com/hipaa-survival-guide-21.php, visited November 2009.

[18] 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. Online at http://ssrn.com/abstract=1589864.

[19] G. Iachello and J. Hong. End-user Privacy in Human-Computer Interaction. *Foundations and Trends in Human Computer Interaction*, 1, January 2007. DOI 10.1561/1100000004.

[20] G. Iachello, I. Smith, S. Consolvo, M. Chen, and G. D. Abowd. Developing Privacy Guidelines for Social Location Disclosure Applications and Services. In *Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS)*, pages 65–76. ACM, 2005. DOI 10.1145/1073001.1073008.

[21] M. C. Julie Maitland. Designing for peer involvement in weight management. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, 2011. DOI 10.1145/1978942.1978988.

[22] J. King, A. Lampinen, and A. Smolen. Privacy: Is there an app for that? In *Proceedings of the Symposium On Usable Privacy and Security (SOUPS)*, 2011. DOI 10.1145/2078827.2078843.

[23] P. Klasnja, S. Consolvo, T. Choudhury, and R. Beckwith. Exploring Privacy Concerns about Personal Sensing. In *Proceedings of the International Conference on Pervasive Computing (Pervasive)*. Springer-Verlag, May 2009. DOI 10.1007/978-3-642-01516-8_13.

[24] D. Kotz, S. Avancha, and A. Baxi. A Privacy Framework for Mobile Health and Home-Care Systems. In *Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS)*, pages 1–12, November 2009. DOI 10.1145/1655084.1655086.

[25] B. Krishnamurthy and C. E. Wills. Characterizing Privacy in Online Social Networks. In *Proceedings of the First Workshop on Online Social Networks*, pages 37–42. ACM, 2008. DOI 10.1145/1397735.1397744.

[26] M. Lesk. Reading Over Your Shoulder. *IEEE Security & Privacy Magazine*, 7(3):78–81, May 2009. DOI 10.1109/MSP.2009.74.

[27] O. Nov and S. Wattal. Social Computing Privacy Concerns: Antecedents and Effects. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pages 333–336. ACM, 2009. DOI 10.1145/1518701.1518754.

[28] 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)*, pages 1985–1988. ACM, 2005. DOI 10.1145/1056808.1057073.

[29] A. Prasad, J. Sorber, T. Stablein, D. Anthony, and D. Kotz. Exposing Privacy Concerns in mHealth Sensing. In *USENIX Workshop on Health Security (HealthSec)*, August 2011. Position paper, Online at http://www.cs.dartmouth.edu/~dfk/papers/prasad-healthsec11.pdf.

[30] 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)*, 2011. DOI 10.1145/1978942.1978945.

[31] P. Sankar and N. L. Jones. To Tell or Not to Tell: Primary Care Patients' Disclosure Deliberations. *Archives of Internal Medicine*, 165(20), November 2005. DOI 10.1001/archinte.165.20.2378.

[32] J. A. Tamada, S. Garg, L. Jovanovic, K. R. Pitzer, S. Fermi, R. O. Potts, and the Cygnus Research Team. Noninvasive Glucose Monitoring. *Journal of the American Medical Association*, 282(19):1839–1844, Nov. 1999. DOI 10.1001/jama.282.19.1839.

[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)*, 2009. Online at http://cups.cs.cmu.edu/LBSprivacy/files/TsaiKelleyCranorSadeh_2009.pdf.

[34] W. Wilkowska, S. Gaul, and M. Ziefle. A Small but Significant Difference - The Role of Gender on Acceptance of Medical Assistive Technologies. In G. Leitner, M. Hitz, and A. Holzinger, editors, *HCI in Work and Learning, Life and Leisure*, volume 6389 of *Lecture Notes in Computer Science*, chapter 6, pages 82–100. Springer, 2010. DOI 10.1007/978-3-642-16607-5_6.

[35] Withings blood pressure cuff. Online at http://www.withings.com/en/bloodpressuremonitor, visited November 2011.