"There's nothing really they can do with this information": Unpacking How Users Manage Privacy Boundaries for Personal Fitness Information

Abstract

Fitness trackers are an increasingly popular tool for tracking one's health and physical activity. While research has evaluated how these mobile devices can improve health and well-being, few studies have empirically evaluated users' privacy concerns that stem from the collection, aggregation, and sharing of personal fitness information (PFI). In this paper, we endeavor to gain a more complete picture of users' experiences with fitness trackers and how they manage the privacy of personal fitness information. Using Communication Privacy Management (CPM) as a theoretical framework, we describe findings from survey and interview data regarding the benefits and drawbacks users perceive from using a fitness tracker, as well as how privacy concerns and behaviors map onto user strategies for managing privacy boundaries related to personal fitness information. We conclude by discussing how our findings contribute to theory and future information policy related to user-generated data from smartphones, wearables, and other mobile devices.

Keywords: fitness trackers, personal fitness information, privacy, communication privacy management, quantified self

"There's nothing really they can do with this information": Unpacking How Users Manage Privacy Boundaries for Personal Fitness Information

Fitness trackers are increasingly popular. A 2012 Pew Research Center survey found that just 5.4% of Americans use a mobile app or online tool to track their weight, diet, or exercise routine (Fox & Duggan, 2013). By 2016, Accenture reported that 21% of Americans owned a wearable device and 33% used one or more health apps on their mobile device (Safavi, K. & Webb, K., 2016). Fitness trackers may provide numerous benefits to users, ranging from an increased awareness about their daily (in)activity to helping them better monitor their food intake and to use the social features to stick to a fitness plan. These devices are a major part of the "quantified self" movement, which focuses on empowering individuals to measure and evaluate metrics about their bodies.

Designed to be worn unobtrusively on the body, fitness trackers collect data in an ambient manner with little effort from the user. The miniaturization and ubiquity of smartphone and mobile sensors allow people to use one device to track several aspects of their bodies (e.g., steps taken, floors climbed, distance traveled, calories burned, time slept, heart rate, location). These data points, known as "personal fitness information" (PFI), may seem innocuous; however, over time, PFI may reveal insights about people's health and habits, and especially when combined with other data sources (Christovich, 2016; Peppet, 2014; Raij, Ghosh, Kumar, & Srivastava, 2011).

Since fitness trackers are designed to facilitate pervasive tracking of PFI, many of their benefits hinge on constant data collection. One study of 21 Fitbit users found that they wear their devices continuously, even while sleeping or showering (Patterson & Nissenbaum, 2013). That study suggests that people who use fitness trackers have adopted the mentality of the quantified self and acquiesced to the device's requisite automated collection of detailed fitness and health. Yet, the PFI generated from fitness trackers can contain sensitive

information, and it is increasingly accessed by third parties in contexts other than users simply checking their step count on their smartphone. Court cases now regularly include evidence gleaned from fitness trackers (Alba, 2016; Snyder, 2015; Crawford, 2014) and medical and insurance providers increasingly seek access to fitness tracker data (Farr, 2017a, 2017b), leading privacy advocates to warn of an emerging "medical surveillance system" (Farr, 2015).

Despite such growing occurrences of third-party access to PFI, little research has considered how users balance the benefits of wearable devices with the privacy risks of sharing highly detailed data streams about their physical activity. In this paper, we endeavor to gain a more complete picture of users' experiences with fitness trackers and how they manage the privacy boundaries surrounding personal fitness information. Using Communication Privacy Management theory (CPM) (Petronio, 2002) as a theoretical framework, we describe findings from survey and interview data regarding the benefits and drawbacks that users perceive from using a fitness tracker, as well as how privacy concerns and behaviors map onto user strategies for managing privacy boundaries related to personal fitness information. We conclude by discussing how our findings contribute to theory and future information policy related to user-generated data from smartphones, wearables, and other mobile devices.

Research on Personal Fitness Information (PFI)

The mobile and networked nature of fitness trackers means that they constantly collect data and transmit it to others (Crawford, Lingel, & Karppi, 2015). Many devices connect to partner mobile apps (e.g., Fitbit, Jawbone's UP, Garmin's Connect and Vivofit Jr., Misfit, and Samsung Gear) or to other third parties. As of late 2017, Fitbit's website lists nearly forty compatible third-party apps and links to Fitbit's API guidelines for those who want to develop an app that integrates with Fitbit's data (Fitbit, 2017). Data sharing can

happen automatically, such as when a fitness tracker syncs with a partner mobile app and sends the user's data to the company's servers. It can also happen when users actively share their data, such as syncing their fitness tracker with a social network site. Further, companies may share or sell users' data with third parties (Fitbit, 2016; Ho, Novick, & Yeung, 2014; Jawbone, 2014).

While a fitness tracker may collect multiple forms of PFI, people's privacy concerns differ based on the type of data collected. Studies show that people express concerns about the collection of video or audio data, location data, mood or stress level data, and data related to conversational behavior (Klasnja, Consolvo, Choudhury, Beckwith, & Hightower, 2009; Motti & Caine, 2015; Patterson & Nissenbaum, 2013). Fitbit users do not want the device to collect detailed health information like glucose level or blood pressure (Patterson & Nissenbaum, 2013). These concerns may be tempered, however, by certain factors related to data management. For example, one user study found that people were more willing to provide GPS and audio data to a tracker if the system deleted the data after a predetermined period of time (Klasnja et al., 2009).

In general, users of fitness trackers do not express many privacy concerns about data collection of PFI (Gorm & Shklovski, 2016). Motti and Caine (2015) surmise that users' lack of concern with fitness trackers stems from a lack of awareness of how companies' collection of granular data about users over a long period of time can compromise privacy. Few regulations exist to constrain companies from sharing user data with third parties, and the FDA recently announced it would lower some regulatory barriers for several technology companies – including those who design fitness trackers—that wish to develop platforms for medical uses, such as screening PFI for medical conditions, and potentially share that data with doctors (Farr, 2017a).

Theoretical Framework: Communication Privacy Management

Derlega and Chaikin describe privacy as a "process of boundary regulation that controls the degree of contact an individual maintains with others" (1977, p. 1). Individuals frequently regulate these boundaries in social relationships through adjustments to the transmission and sharing of personal information. This control of information exchange typically defines the amount of privacy present in a relationship both theoretically and pragmatically. Elaborating on the notion of privacy as regulated by boundaries, Petronio (2002) presents a theory of Communication Privacy Management (CPM) to explain the decisions people make when disclosing (or concealing) private information. As a boundary management theory, CPM argues that individuals engage in a "mental calculus" when making decisions about whether to disclose a piece of personal information, with ongoing interplays between pressures to reveal and to conceal information.

Petronio (2013, 2002) suggests that individuals manage the tensions between public and private disclosures by establishing boundaries that are constantly negotiated and coordinated depending upon contextual factors. These boundaries are negotiated within CPM through three core elements: (1) ownership, (2) information control via privacy rules, and (3) turbulence. First, Petronio notes that individuals maintain "ownership" of their private information, even after it is shared with others. She provides the concept of thick versus thin boundaries to unpack this ownership. For example, personal secrets such as one's sexual history might have very thick boundaries, while personal information frequently shared with others, such as one's home address, may have thinner boundaries.

Individuals control how their personal information is shared by actively negotiating "privacy rules" with others who might have (or wish to have) access to a piece of personal information. The goal of these rules is to help people understand when, where, and with whom it is acceptable to share a piece of private information. Privacy rules vary based on the

particular relationship, as well as on cultural and contextual factors, as well as risk-benefit calculations (Petronio, 2002).

Finally, CPM theory assumes that privacy rules might break down, leading to "privacy turbulence" between the owners of a piece of information and a breakdown of trust between the original owner of the information and those who violated a privacy rule (Petronio & Durham, 2008). When this happens, individuals must recalibrate their privacy rules to avoid future turbulence—or dissolve the relationship if the violation was severe enough, assuming dissolution is even possible.

Communication researchers have applied CPM in various contexts where privacy negotiations occur between two parties, including romantic partners (Durham, 2008; Steuber & Solomon, 2011), families (Toller & McBride, 2013), healthcare providers and patients (Petronio & Kovach, 1997), and victims of sexual abuse (Petronio, Reeder, Hecht, & Ros-Mendoza, 1996). More recently, CPM is being applied to contexts where privacy boundaries are managed within mobile, online, and social media environments (Child, Haridakis, & Petronio, 2012; Jin, 2013; Metzger, 2007; Waters & Ackerman, 2011; Yang & Pulido, 2016).

CPM, then, offers a useful framework for exploring how fitness tracker users manage boundaries around the sharing of personal fitness information. Consequently, we can use CPM to identify users' perceptions and behaviors regarding data ownership, privacy rules, and turbulence to gain insights into how users negotiate the disclosure and sharing of PFI.

Current Study: Unpacking How Users Manage Privacy Boundaries with PFI

In this study, we endeavor to gain a more complete picture of users' experiences with fitness trackers and how they manage privacy boundaries regarding the sharing and disclosure of personal fitness information. As noted above, little research on fitness trackers has focused on data privacy; in the few studies that have addressed privacy issues, users

expressed little concern about their PFI (Gorm & Shklovski, 2016; Motti & Caine, 2015). However, these studies did not evaluate how privacy concerns fit into the wider ecosystem of device benefits and drawbacks, or the strategies users may employ to minimize privacy risks. Therefore, we guide our analyses with the following research questions:

RQ1: What benefits and drawbacks do users experience from using fitness trackers?

RQ2: How do users of fitness trackers perceive concerns over privacy and personal fitness information?

RQ3: What actions, if any, do users take to manage the privacy of their personal fitness information?

Method

To address our RQs, we used a mixed-method approach involving a survey and semi-structured interviews. In this paper, we focus primarily on the qualitative data gathered through interviews with 33 Fitbit and Jawbone users and only include quantitative data when it complements or contextualizes the interviews. Participants were first recruited through emails to a random sample of 6,000 university employees across two American public universities. They were invited to complete an online survey if they were at least 18 years old, owned a smartphone, and currently used a Fitbit or Jawbone device. At the end of the survey, respondents could provide contact information to participate in a follow-up interview and to enter a drawing for one of five $50 Amazon gift cards.

From 363 completed surveys, 141 participants stated they would be willing to participate in an interview. We used criterion sampling (Patton, 2005)to identify a subset to invite to interviews. We first looked at survey items that captured participants' privacy concerns, using a measure of internet privacy concerns (Vitak, 2016), mobile privacy concerns (Xu, Gupta, Rosson, & Carroll, 2012), internet skills (Hargittai & Hsieh, 2012), and fitness tracker use (both frequency of use and engagement in social features). We then

created four categories of users along two axes: skills and concerns. This led to pools of participants who self-reported as (1) high skills, high concerns, (2) high skills, low concerns, (3) low skills, high concerns, and (4) low skills, low concerns. We excluded anyone who fell into the midpoint for both categories or who reported rarely using their fitness tracker.

During March and April 2017, we invited potential interviewees in batches, starting with those who most strongly represented each of the four categories. As interviews were scheduled and conducted, we invited additional participants and tried to ensure we had a similar number of participants across each group. At the conclusion of data collection, we had interviewed 33 people across the two universities, with 8 had High Skills/Low Concerns, 11 had High Skills/High Concerns, 6 had Low Skills/Low Concerns, and 8 had Low Skills/High Concerns. See Table 1 for descriptive data on each of the 33 participants and Figure 1 for general mapping of participants across skill and concern measures. Each participant received a $15 Amazon gift card upon completion of the interview.

Data Analysis

Following data collection, each interview was transcribed and uploaded to the qualitative analysis program Dedoose to enable iterative coding by multiple research team members (Lincoln & Guba, 1985). The authors first discussed a set of potential codes to include in the codebook based on the theoretical framing, interview protocol, and research goals of the project. They then independently coded two interviews and met to update the codebook. Once the codebook was finalized, two authors coded each transcript to ensure consistency and validate results. Finally, we exported excerpts from each code to Excel and further analyzed them to identify trends in the data (Miles, Huberman, & Saldaña, 2013).

Findings

Benefits of Fitness Tracker Use

The survey revealed that 70% of respondents use their fitness trackers every day, and they perceived the physical fitness-related features to be more important than the non-fitness features. Using a five-point scale ranging from not important at all to very important, respondents said the most important features were the step counter (*M*=4.81, *SD*=0.53), calorie tracker (*M*=4.34, *SD*=1.01), and workout/activity tracker (*M*=4.02, *SD*=1.14), and the least important features were the ability to compete with others (*M*=2.90, *SD*=1.41) and engage with social features (e.g., messaging, groups, chat) (*M*=2.10, *SD*=1.16). See Table 2 for a full listing of survey respondents' perceived importance of fitness tracker features.

Follow-up interviews with fitness tracker users confirmed the usage patterns and benefits suggested by the survey responses. Eighty percent (N=27) of interviewees reported using their fitness tracker every day, typically removing the device only to shower or charge the battery. For example, P324 said, "I'm always wearing my fitness tracker, except for the things you can't, like taking a shower, swimming, that sort of thing. … Last year, I think there was one day when I didn't have it." P194 justified her constant use—only taking it off to shower—because she wanted "to get credit for every step."

Along these lines, fitness tracking devices acted as strong motivators in many interviewees' lives, where the presence of the device encouraged greater physical activity. Many participants noted how the devices made them more aware and more accountable regarding their level of activity, particularly when the devices "nudged" them into action—some, but not all devices come equipped with reminder functions to prompt regular physical activity throughout the day. P123 described this perception of accountability by saying, "I thought by getting a Fitbit, it would keep me accountable with the steps and being able to be aware of approximately how many calories I'm burning, things like that. It definitely helps to

keep me accountable." P324 echoed this sentiment, saying his Fitbit served as a mental reminder to get up and move more often: "It's sort of the nice friend that tells you, 'Hey, let's go out and do something.'"

Many fitness trackers can collect a variety of fitness data beyond steps, and some interview participants cited sleep tracking as a benefit of owning these devices. P439 noted she has "really bad sleeping patterns" and wanted to use her Fitbit to get data on her sleep quality. While some interviewees opted to charge their device overnight, several indicated that sleep tracking was their primary use of the device. P299 indicated that his device had significantly improved his sleep quality, which was suffering due to working off-hour shifts: "I'm pretty dialed into my sleep and that's because of this. The step part of it, nicety but not ... just cause I'm pretty active otherwise." Survey responses revealed that sleep tracking was the fifth most important feature out of ten features (see Table 2). This suggests that sleep tracking was more popular with interview participants than with survey respondents as a whole.

Other benefits interviewees expressed included weight loss, increased endurance, feeling healthier, and a sense of making positive life choices. And while survey respondents rated the social aspects of fitness trackers of lowest importance (M=2.10, SD=1.16), numerous interview participants noted that the social functions help motivate them to exercise more. For example, P71 noted: "I have a couple of friends who do a lot, a lot of steps so it kinda motivates me to do more too. 'Cause sometimes I'll look and I'm like, 'Yeah, I didn't take a morning walk today. I should probably do something.'"

Drawbacks of Fitness Tracker Use

While some of our participants expressed minor technological frustrations with their fitness tracker—including (what they perceived as) imprecise step counts, skin irritations, lack of waterproofing, battery issues, or the fact their tracker lacks features available in more current models—only a few mentioned any real drawbacks from owning a device. A few

participants expressed frustration with the tracker's ability to "nudge" you to get up and move each hour, feeling it was a bit intrusive at times.

Other drawbacks centered on the social and competitive functions of their fitness trackers. Overall, our survey respondents rated the social functionality of fitness trackers as the least important feature. And while many interviewees had positive experiences with the social aspects of their fitness devices, a few complained about the small size of their social network through the app, while others expressed wariness of the shaming and over-competitive elements of sharing personal fitness information across social networks. For example, P371 described why she stopped engaging with the social and competitive features of the app, saying:

> *I stopped looking at [other people's stats] because it makes me feel bad. I have a lot of [Ultimate] Frisbee friends that use a Fitbit and they walk a lot more than I do. ... I have stopped looking at that out of slight embarrassment, even though I know I don't wear my Fitbit all the time. ... If anything, it's just the interconnected sharing my data with other people feels slightly shaming sometimes, which I guess is the point. I'm not the hugest fan of that necessarily. (P 371)*

P194 described the activity comparisons and competition features in similar terms, saying she sometimes felt a "backlash" from not doing as well as friends she followed through the app. Still others expressed an overall distaste for the social aspects of owning a fitness tracker and consciously chose not to share their PFI with anyone. P216 said she turns down any connection requests she receives because, "I don't care about sharing. I'm not a 'share' person. This is mine. I don't care what they do and I don't want them to care what I do." Likewise, P439 described her Fitbit data in terms of ownership, saying, "Fitness stuff is for me, not for everybody else." For her, the kinds of data generated through her device had a thick boundary, and thus she was less likely to share ownership with others.

Privacy Concerns Regarding Fitness Trackers and Personal Fitness Information

Most participants expressed only minimal privacy concerns related to their use of a personal fitness tracker. When first asked if they had any privacy concerns related to their tracker, one-third of the interviewees quickly and simply said no.

A few participants admitted being largely unaware of any broader privacy issues related to using a fitness tracker. For example, P257 had heard about a woman using Fitbit data in a lawsuit and thought, "Oh. This information could be used, really, beyond myself. Is this information that I would like to have tracked?" P261 feels she "should be more concerned about" the data she shares with Fitbit, but then ignores such feelings:

> *It has crossed my mind what if this information were shared with an insurance company or it impacted my health care in some way, or my ability to obtain health care in some way? It's crossed my mind, and then I dismiss it. (P261)*

Others expressed general ambivalence, stating, "I know there are some issues with like privacy, but I'm not as concerned about that" (P96). Participants recognized that their PFI may need a boundary, but they did not feel the information was so sensitive that it required them to take time and define the contours and rules to govern such a boundary.

Regarding the relative sensitivity of personal fitness information, survey respondents expected that they would feel only average levels of concern (evaluated on a scale of 0 to 100) if their fitness tracker data were compromised in something like a security breach (M=54.44, SD=29.26). Nearly half of our interviewees did not perceive PFI to be valuable and did not sense that sharing such data could potentially harm them. For example, P371 felt that Fitbit was "fairly innocuous." Others did not express concern at the idea of someone seeing the data.

> *If this information was public, I wouldn't be upset by it. If anybody wants to know how much water I drink, wow, they need to get a life. (P69)*

These participants did not feel that disclosure of their PFI could result in boundary turbulence. However, a few interviewees exhibited a qualified version of this "who cares?" perspective. They preferred that PFI was not shared with others, but they also did not perceive such sharing to be a concern.

> *I guess if anybody were to see it, they're not going to ... There's nothing really they can do with that information, but I just like knowing that I have it set and only a few people can see it. (P56)*

These participants appear to maintain a thin boundary around PFI, preferring for it to remain within, but still not feeling that its disclosure could result in turbulence.

Numerous interviewees noted, however, that privacy concerns would emerge if their fitness tracker was collecting or sharing personal information beyond just steps taken, such as personal or location data. P123 "wouldn't really mind" if data about her steps, calories, or sleep was "out there." But she felt concerned about this data including her email or physical address because this would give people a way to contact her. For P65, concerns arose depending on the specificity of the data shared. He was "happy to share basic information" such as name, general location, or steps, but did not want more granular information, such as birth date or address, to be shared. P75 felt that sharing data that was so granular that it could be used to infer other details about his life was "crossing the a line."

> *I think, essentially, if you had exactly the number of steps someone took at which time, like, minute or something, you can actually work out exactly what they did and it kinda gets into the personal space where they got up in the morning and then went to the bathroom ... I don't want it to be that granular level. I think that, kind of, invades my personal space where something personal to me being exposed to someone else. (P75)*

Other interviewees clearly stated that it would be a privacy concern if the tracker collected specific, GPS-based, location data. For example, P408 said, "If it's connecting to the servers in the cloud and pinpointing my location, then I would be worried." P326 seemed unsure about whether her device captured her location, but acknowledged it would be "super creepy... especially because I walk a lot at night by myself."

Various interviewees took a utilitarian perspective when considering privacy concerns related to the collection and use of their personal fitness information, suggesting that concerns would be minimized if they could realize some benefit of the data collection.

> *It all depends on what their purpose is for collecting it. If it benefits me by them collecting it, like if they can collect it and then show me how it impacts my life or relates with other things, then it's useful. Then I have no problem with that. But if it's just so they can build and sell the data, I don't agree with that. (P65)*

And some interviewees noted they trusted their fitness tracker company, which tended to alleviate any potential privacy concerns.

> *I don't have any reason to not trust [Fitbit]. I haven't heard anything bad about them. There hasn't been any information out there about any breach of the data that they collect. I'm sure that when I did the set-up it had a whole privacy statement and all that kind of stuff on it. If I had had any concerns about it, I probably wouldn't have set it up. (P69)*

They did not, however, report thinking actively about questions of trusting the company. For example, P82 acknowledged that Fitbit had a lot of data about her, and she wondered, "how susceptible it is to a hack or something," but she hadn't "really thought about how it could be potentially used against me." P96 wasn't sure if this was a "matter of trust or just, like, not worrying as much about [Fitbit] because they're smaller" than companies like Google and Facebook, which "touch everything on the internet."

Some interviewees appeared to have basic privacy rules surrounding their PFI, identifying that turbulence could arise if certain types of information were collected at an unexpected level of granularity. They appeared to be giving the companies that manage their PFI the benefit of the doubt, withholding concern until they had a reason to fear boundary turbulence.

Privacy Behaviors Regarding Fitness Tracker Devices and Personal Fitness Information

In line with the general lack of strong privacy concerns regarding their personal fitness information reported above, our interview participants reported limited specific actions taken to manage privacy on their device. While a few participants noted taking steps to protect their privacy on their device—for example, P96 said, "First time I sign up for anything I go through all the privacy settings and make sure they're pretty locked down"—many interviewees recalled examining the privacy settings of their device when first setting it up, but they haven't checked or adjusted the settings since.

For example, several participants said they didn't think they'd checked the settings since first setting up the device. Others could not even remember changing the settings upon receiving the device and assumed the default settings were still in place. Finally, P65 noted that while he regularly checks and adjusts privacy settings on other internet platforms, such as Facebook, he doesn't for his fitness tracking device.

Of those participants who reported making adjustments to their fitness tracker privacy settings, most took steps that limited the flow of personal fitness information. P56 said she went through her Fitbit settings when she set up the device and made everything private so only she could see the data; she has subsequently connected with three other users whom she knows offline. Other participants noted difficulties in adjusting privacy settings due to the limited features on the fitness tracker's mobile application compared to the settings on the fitness tracker company's web site. For example, Fitbit's mobile app only offers one general

privacy setting while its web site lets users set privacy levels for at least 14 different types of information This is especially problematic because many users exclusively use the mobile app to interact with their PFI; however, the app's privacy settings do not allow for granular control and can be hard to locate. For example, P323 noted:

> *I can't remember [having any privacy concerns when setting up my Fitbit] and I wouldn't have checked what they were collecting. Again, if it's not very front-facing about it, I'm bad about going in and looking at it. I know I should, but I just get lazy about it, so I don't think so. And if there was, I may have gone in and changed the settings to say, "No, I don't want you actually doing this," or I may have tried and got annoyed and then forgot.*

P259 described a similar experience when setting up a replacement device and reviewing the privacy settings for his account. He expressed frustration that users have to log onto the website to view and change the full set of privacy settings.

This suggests that participants who want to change the privacy rules surrounding their PFI may struggle to navigate the fitness tracker's app and website to do so. However, their general sense that only a thin boundary needs to surround the information may de-motivate them from trying to figure out how to adjust the privacy settings.

Discussion

Our exploratory research questions were designed to gain insights into users' experiences with fitness trackers and how they manage privacy boundaries related to personal fitness information.

RQ1 sought to understand the benefits and drawbacks users perceive from using a fitness tracker, and our interview results revealed that benefits far outweighed any perceived drawbacks. Our interviewees wear their devices nearly constantly and see the device as a motivating presence in their lives. Contrary to many news reports that fitness trackers might

not improve one's health (Carroll, 2017; Ross, 2016), our participants expressed a variety of (perceived) benefits including weight loss, increased endurance, feeling healthier, and a sense of making positive life choices. Few participants expressed any significant drawbacks, with some mentioning irritation over the social features of their device, including both frustration about the limited size of the social network as well as a general distaste of making one's personal fitness information visible to anyone outside a close network of friends. Thus, while fitness tracker companies highlight the social aspects of their ecosystem—ranging from competing with other users, following friends' fitness goals and activities, and automatically posting daily statistics to one's social media account—our findings suggest that users preferred to keep their personal fitness information relatively close to themselves. As P439 noted: "Fitness stuff is for me, not for everybody else."

RQ2 and RQ3 focused on assessing interviewees' privacy concerns and behaviors related to their fitness trackers and personal fitness information, generally. Overall, our participants expressed low levels of privacy concerns, with many suggesting that personal fitness information did not to rise to a level of sensitivity that would trigger privacy concerns or privacy-protecting activities. Notably, few participants noted making changes to privacy settings after initially setting up their fitness tracker. Those who did make adjustments tended to limit the flow of personal fitness information.

If we consider our findings within the framework of Communication Privacy Management (CPM), we can see how users' conceptualizations of ownership, privacy rules, and turbulence surrounding their personal fitness information influence how they manage the privacy boundaries around such information.

Ownership

CPM argues that individuals strive to maintain "ownership" of their private information, even when sharing it with others, and that they frequently erect thick or thin

boundaries to manage this ownership. In the context of fitness trackers, our participants noted a strong urge to own their personal fitness information: most felt little need to actively share their fitness activities beyond a close social circle. A few participants did construct thick boundaries around this information.

However, participants largely did not see PFI as sensitive, and most appeared to be satisfied with a much thinner boundary. Few participants noted making changes to their default privacy settings, which might be a result of the limited privacy controls provided on the mobile apps most frequently used by participants to manage their PFI. Thus, while participants sought to maintain ownership of their PFI, they varied in the degree to which they felt thick boundaries were necessary. For those who do seek to articulate a boundary, the affordances of the platform might limit their ability to do so.

Privacy Rules

Within the CPM framework, individuals control how their personal information is shared by actively negotiating "privacy rules" with others who might have (or wish to have) access to a piece of personal information. While participants engaged in social aspects of their fitness device (e.g., messaging, groups, chat), their established privacy rules appeared to focus on sharing only the most basic fitness data with only close friends. Few were willing to share more detailed information, such as location or weight, and no one suggested that rules might exist to allow broadcasting PFI beyond a close circle of known friends. Interviewees created distinct privacy rules for different types of PFI, seeing some types of information as more acceptable for the device to collect and share than others. Interviewees saw steps, sleep, and general fitness data as acceptable, but GPS or other location data clearly fell outside what was allowed.

Many of our participants expressed an inherent trust with their fitness tracker company, assuming that the company already had privacy rules in place to properly limit the

flow of their personal fitness information. Many could not remember adjusting their privacy settings or assumed the default settings were still in place. Furthermore, participants appeared to give the company the benefit of the doubt because they had not heard negative news about the company, (e.g., a security breach, PFI used in inappropriate ways). More media coverage on the ways that PFI can be used to infer other information about users, as well as additional scrutiny of the data practices of such companies, may help raise awareness of the privacy concerns that such pervasive data collection poses.

Turbulence

CPM suggests that privacy rules eventually break down, leading to "privacy turbulence" between the owners of a piece of information and to reduced trust between the original owner of the information and those who disrupted a privacy rule. The potential for privacy turbulence was apparent in our interviewees' concerns that PFI might be combined with more personal data, comingled with location data, or shared outside the expected contexts. However, this concern was tempered for many participants by the fact that they had not heard of such cases or were not aware if such activities were occurring. Again, this suggests that media coverage of the practices of fitness tracker companies could help inform users about how their PFI is being used. Our findings also reveal a potential for unexpended privacy turbulence, since most respondents reported limited engagement with the privacy settings for their fitness tracker. This suggests that unanticipated data sharing might very well be prevalent.

Conclusions and Future Work

Our study sought to identify benefits and drawbacks from the use of personal fitness trackers and to leverage Communication Privacy Management theory to gain a better understanding of how fitness tracker users manage privacy boundaries related to personal fitness information (PFI). Our findings revealed that the perceived benefits of using fitness

trackers greatly outweigh drawbacks. They also show how users do (or do not) exert control over their PFI and establish basic privacy rules to govern how PFI might flow to other individuals. Yet, limited engagement with privacy settings for fitness trackers, combined with fear over PFI being co-mingled with other personal information, leads to the potential for privacy turbulence to emerge related to PFI. A consequence of such turbulence might be reduced engagement in fitness tracking activities.

Our findings suggest that the potential for privacy turbulence could be mitigated if fitness tracking companies like Fitbit take cues from other internet companies like Facebook and Google, which have taken steps to spotlight privacy features more clearly within the user experience. For example, Facebook introduced its Privacy Checkup features in 2014 to alert users when they are about to share content publicly and to provide a walkthrough of the site's many privacy settings (Schaar, 2010). Likewise, Google has implemented a Security Checkup that takes the user through connected accounts, authorizations, and two-factor authentication (Whitney, 2017). Fitness tracking companies could embrace a more transparent stance on how they use the data they collect from users, as has been shown in design-based mockups like the "privacy nutrition label" (Kelley, Bresee, Cranor, & Reeder, 2009).

Further, our initial findings urge us to explore additional implications for the CPM model in the context of fitness tracking and personal fitness information. As suggested by Vitak's (2016) discussion of how best to apply CPM to technologically mediated interactions, future work should focus on the role of particular contexts related to sharing PFI. For example, there is growing interest in using fitness trackers as part of workplace wellness programs (Gorm & Shklovski, 2016), and it would be useful to investigate whether users manage their privacy boundaries differently when sharing PFI with employers or health insurance companies compared to sharing it within their social networks. Further work can

also explore how the affordances of the fitness tracker platforms themselves – including differences across wearable device designs, mobile app interfaces, and website layout – might affect users' ability to manage privacy boundaries.

Wearable devices, including fitness trackers, are likely to become even more pervasive in everyday life. Understanding how users manage privacy boundaries around the information these devices generate is crucial to ensuring that increased adoption of the devices does not also result in increased privacy risks for the people who use them.

References

Alba, A. (2016, April 19). Police, attorneys using fitness trackers as court evidence. *New York Daily News*. Retrieved from http://www.nydailynews.com/news/national/police-attorneys-fitness-trackers-court-evidence-article-1.2607432.

Child, J. T., Haridakis, P. M., & Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior*, *28*(5), 1859–1872. https://doi.org/10.1016/j.chb.2012.05.004.

Christovich, M. M. (2016). Why should we care what Fitbit shares: A proposed statutory solution to protect sensitive personal fitness information. *Hastings Communications and Entertainment Law Journal*, *38*(11), 91-145.

Crawford, K. (2014, November 19). When Fitbit is the expert witness. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936/.

Crawford, K., Lingel, J., & Karppi, T. (2015). Our metrics, ourselves: A hundred years of self-tracking from the weight scale to the wrist wearable device. *European Journal of Cultural Studies*, *18*(4–5), 479–496. https://doi.org/10.1177/1367549415584857.

Derlega, V. J., & Chaikin, A. L. (1977). Privacy and self-disclosure in social relationships. *Journal of Social Issues*, *33*(3), 102–115. https://doi.org/http://dx.doi.org/10.1111/j.1540-4560.1977.tb01885.x.

Durham, W. T. (2008). The rules-based process of revealing/concealing the family planning decisions of voluntarily child-free couples: A communication privacy management perspective. *Communication Studies*, *59*(2), 132–147. https://doi.org/10.1080/10510970802062451.

Farr, C. (2015, April 9). Weighing privacy vs. rewards of letting insurers track your fitness. *NPR.org*. Retrieved from http://www.npr.org/sections/alltechconsidered/2015/04/09/398416513/weighing-privacy-vs-rewards-of-letting-insurers-track-your-fitness.

Farr, C. (2017a, September 27). FDA helps Apple, Alphabet and Samsung in long-term health care bets. *CNBC.com*. Retrieved from https://www.cnbc.com/2017/09/27/fda-helps-apple-alphabet-and-samsung-in-long-term-health-care-bets.html.

Farr, C. (2017b, October 23). You can get an Apple Watch for only $25 ... with one small catch. *CNBC.com*. Retrieved from https://www.cnbc.com/2017/10/23/apple-watches-offered-to-all-john-hancock-life-insurance-customers.html.

Fitbit. (2016, August 9). Fitbit Privacy Policy. *Fitbit*. Retrieved from https://www.fitbit.com/legal/privacy-policy.

Fitbit. (2017). Work with us. *Fitbit*. Retrieved from https://www.fitbit.com/partnership.

Fox, S., & Duggan, M. (2013, January 28). Tracking for health. *Pew Research Center: Internet, Science & Tech*. Retrieved from http://www.pewinternet.org/2013/01/28/tracking-for-health/.

Gorm, N., & Shklovski, I. (2016). Sharing steps in the workplace: Changing privacy concerns over time. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 4315–4319). New York, NY, USA: ACM. https://doi.org/10.1145/2858036.2858352.

Hargittai, E., & Hsieh, Y. P. (2012). Succinct survey measures of web-use skills. *Social Science Computer Review*, *30*(1), 95–107. https://doi.org/10.1177/0894439310397146.

Ho, J.-J., Novick, S., & Yeung, C. (2014). A snapshot of data sharing by select health and fitness apps. Presentation at Consumer Generated and Controlled Health Data. Federal

Trade Commission Spring Privacy Series. Retrieved from https://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf.

Jawbone. (2014, December 16). Jawbone privacy policy. *Jawbone*. Retrieved from https://jawbone.com/privacy.

Jin, S.-A. A. (2013). Peeling back the multiple layers of Twitter's private disclosure onion: The roles of virtual identity discrepancy and personality traits in communication privacy management on Twitter. *New Media & Society*, *15*(6), 813–833. https://doi.org/10.1177/1461444812471814.

Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009). A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (p. 4:1–4:12). New York, NY, USA: ACM. https://doi.org/10.1145/1572532.1572538.

Klasnja, P., Consolvo, S., Choudhury, T., Beckwith, R., & Hightower, J. (2009). Exploring privacy concerns about personal sensing. In *Pervasive Computing* (pp. 176–183). Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-642-01516-8_13.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry* (1st edition). Beverly Hills, CA: SAGE Publications.

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, *12*(2), 335–361. https://doi.org/10.1111/j.1083-6101.2007.00328.x.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2013). *Qualitative data analysis: A methods sourcebook* (3rd edition). Thousand Oaks, CA: SAGE Publications.

Motti, V. G., & Caine, K. (2015). Users' privacy concerns about wearables: Impact of form factor, sensors and type of data collected. In *1st Workshop on Wearable Security and*

Privacy (pp. 1–15). Financial Cryptography and Data Security 2015. Retrieved from http://fc15.ifca.ai/preproceedings/wearable/paper_2.pdf.

Patterson, H., & Nissenbaum, H. (2013). Context-dependent expectations of privacy in self-generated mobile health data. Presentation at Privacy Law Scholars Conference.

Patton, M. Q. (2005). Qualitative research. In *Encyclopedia of Statistics in Behavioral Science*. Hoboken, NJ: John Wiley & Sons, Ltd. https://doi.org/10.1002/0470013192.bsa514.

Peppet, S. R. (2014). Regulating the Internet of Things: First steps toward managing discrimination, privacy, security, and consent. *Texas Law Review*, *83*, 85–176. Retrieved from http://www.texaslrev.com/wp-content/uploads/2015/08/Peppet-93-1.pdf.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany, NY: SUNY Press. Retrieved from http://www.sunypress.edu/p-3659-boundaries-of-privacy.aspx.

Petronio, S. (2013). Brief status report on communication privacy management theory. *Journal of Family Communication*, *13*(1), 6–14. https://doi.org/10.1080/15267431.2013.743426.

Petronio, S., & Durham, W. T. (2008). Communication privacy management theory: Significance for interpersonal communication. In *Engaging Theories in Interpersonal Communication: Multiple Perspectives* (pp. 309–322). Thousand Oaks, CA: SAGE Publications. https://doi.org/10.4135/9781483329529.

Petronio, S., & Kovach, S. (1997). Managing privacy boundaries: Health providers' perceptions of resident care in Scottish nursing homes. *Journal of Applied Communication Research*, *25*(2), 115–131. https://doi.org/10.1080/00909889709365470.

Petronio, S., Reeder, H. M., Hecht, M. L., & Ros-Mendoza, T. M. (1996). Disclosure of sexual abuse by children and adolescents. *Journal of Applied Communication Research*, *24*(3), 181–199. https://doi.org/10.1080/00909889609365450.

Raij, A., Ghosh, A., Kumar, S., & Srivastava, M. (2011). 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* (pp. 11–20). New York, NY, USA: ACM. https://doi.org/10.1145/1978942.1978945.

Safavi, K., & Webb, K. (2016). Digitally enabled healthcare experience for the patients in the US: Accenture 2016 consumer survey on patient engagement. *Accenture Consulting*. Retrieved from https://www.accenture.com/us-en/insight-research-shows-patients-united-states-want-heavy.

Schaar, P. (2010). Privacy by Design. *Identity in the Information Society*, *3*(2), 267–274. https://doi.org/10.1007/s12394-010-0055-x.

Snyder, M. (2015, June 19). Police: Woman's fitness watch disproved rape report. *ABC27*. Retrieved from http://abc27.com/2015/06/19/police-womans-fitness-watch-disproved-rape-report/.

Steuber, K. R., & Solomon, D. H. (2011). Factors that predict married partners' disclosures about infertility to social network members. *Journal of Applied Communication Research*, *39*(3), 250–270. https://doi.org/10.1080/00909882.2011.585401.

Toller, P. W., & McBride, M. C. (2013). Enacting privacy rules and protecting disclosure recipients: Parents' communication with children following the death of a family member. *Journal of Family Communication*, *13*(1), 32–45. https://doi.org/10.1080/15267431.2012.742091.

Vitak, J. (2016). A digital path to happiness?: Applying communication privacy management theory to mediated interactions. In Reinecke, L. & Oliver, M. B. (Eds.), *The*

Routledge Handbook of Media Use and Well-Being: International Perspectives on Theory and Research on Positive Media Effects (pp. 274–287). London: Routledge.

Waters, S., & Ackerman, J. (2011). Exploring privacy management on Facebook: Motivations and perceived consequences of voluntary disclosure. *Journal of Computer-Mediated Communication*, *17*(1), 101–115. https://doi.org/10.1111/j.1083-6101.2011.01559.x.

Whitney, L. (2017, April 5). How to run a security checkup on your Google account. *PCMag*. Retrieved from https://www.pcmag.com/article2/0,2817,2515751,00.asp.

Xu, H., Gupta, S., Rosson, M., & Carroll, J. (2012). Measuring mobile users' concerns for information privacy. In *Proceedings of the International Conference on Information Systems 2012 on Digital Innovation in the Service Economy*. Retrieved from http://aisel.aisnet.org/icis2012/proceedings/ISSecurity/10.

Yang, K. C., & Pulido, A. (2016). Exploring the relationship between privacy concerns and social media use among college students: A communication privacy management perspective. *Intercultural Communication Studies*, *25*(2), 46–62. Retrieved from http://web.uri.edu/iaics/files/K.-YANG-A.-PULIDO-Y.-KANG.pdf.

Figure 1.

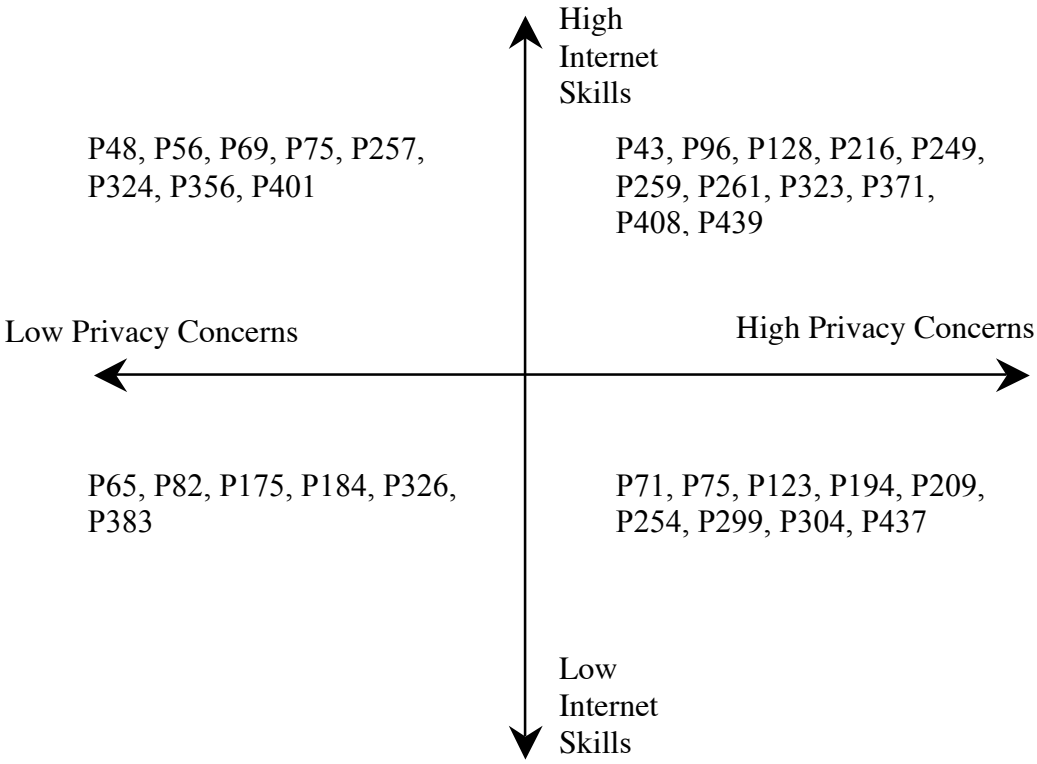
High Internet Skills
P48, P56, P69, P75, P257, P324, P356, P401
P43, P96, P128, P216, P249, P259, P261, P323, P371, P408, P439
Low Privacy Concerns
High Privacy Concerns
P65, P82, P175, P184, P326, P383
P71, P75, P123, P194, P209, P254, P299, P304, P437
Low Internet Skills

Table 1. Descriptive data of 33 interview participants

ID	Internet Skills Scale[1]	General Privacy Concern[2]	Mobile Data Concern[3]	Tracker Frequency of Use	Sex	Age	User Category[4]
P43	4.4	5	5	Everyday	F	39	High Skill/High Concern
P48	4.8	2.55	2.75	Most days	M	26	High Skill/Low Concern
P56	5	3.18	3.88	Everyday	F	46	High Skill/Low Concern
P65	3.2	1.36	3.13	Everyday	M	33	Low Skil/Low Concern
P69	4.8	1.45	4	Everyday	F	55	High Skill/Low Concern
P71	3.5	4.27	4.25	Everyday	F	27	Low Skill/High Concern
P75	5	2.82	2.88	Everyday	M	34	High Skill/Low Concern
P82	3.3	1.73	4	Everyday	F	30	Low Skil/Low Concern
P96	4.7	3.09	5	Most days	F	35	High Skill/High Concern
P123	3.1	4	3.25	Most days	F	23	Low Skill/High Concern
P128	4.1	5	5	Everyday	F	52	High Skill/High Concern
P175	3.9	2.27	2.25	Everyday	F	50	Low Skil/Low Concern
P184	3.6	2.27	4.75	Everyday	F	23	Low Skil/Low Concern
P194	2.89	4.09	4	Everyday	F	57	Low Skill/High Concern
P209	2.4	3.45	3.5	Everyday	F	57	Low Skill/High Concern
P216	5	4.27	4	Everyday	F	66	High Skill/High Concern
P249	5	4.55	4.13	Everyday	F	30	High Skill/High Concern
P254	2	3.27	4	Everyday	M	42	Low Skill/High Concern
P257	4.7	1.45	3.25	Everyday	F	41	High Skill/Low Concern
P259	1.6	1.45	2.88	Everyday	M	26	High Skill/High Concern
P261	4.9	4.82	4.88	Everyday	F	56	High Skill/High Concern
P299	3.1	4.27	4.63	Everyday	M	51	Low Skill/High Concern
P304	2.8	4.91	4	Most days	F	33	Low Skill/High Concern
P323	5	4.27	4.13	Most days	M	34	High Skill/High Concern
P324	5	1.91	3.5	Everyday	M	33	High Skill/Low Concern
P326	3.9	2.91	4.25	Everyday	F	38	Low Skil/Low Concern
P356	3.2	1.64	3.63	Everyday	F	35	High Skill/Low Concern
P371	4.9	4.45	3.38	Most days	F	25	High Skill/High Concern
P383	3	1.27	2.25	Everyday	F	61	Low Skil/Low Concern
P401	5	1.18	4	Everyday	F	51	High Skill/Low Concern
P408	5	5	4.38	Everyday	F	45	High Skill/High Concern
P437	2.5	4	4.63	Everyday	F	64	Low Skill/High Concern
P439	5	4.82	4.63	Everyday	F	34	High Skill/High Concern
	Mean (SD)= 3.95 (1.05)	Mean (SD)= 3.24 (1.33)	Mean (SD)= 3.88 (0.76)		F (80%) M (20%)	Mean (SD= 41 (12.7)	

1. Internet Skills Scale (perceived): 10 items averaged, 1=Low Skill; 5=High Skill

2. Privacy Concerns Scale: 12 items averaged, 1=Low Concerns, 5=High Concerns

3. Mobile Data Concerns: 9 items averaged, 1=Less Agreement, 5=More agreement with items about data loss on mobile

4. Skill/Privacy Concerns Category: A=High Skill/Low Concerns, B=High Skill/High Concerns, C=Low Skill/Low Concerns, D=Low Skill/high Concerns.

Table 2. Perceived Importance[1] of Fitness Tracker Features (N=360).

	Mean	SD	Median
Steps Counter	4.8	0.52	5
Workout/Activity Tracking	4.3	0.99	4
Clock	4.05	1.33	5
Calories Burned	3.96	1.11	3
Sleep Tracking	3.68	1.34	4
Alarm	3.3	1.43	3
Weight Tracking	3.19	1.28	3
Syncing with Other Apps	3.19	1.43	2
Competition Features (who can get the most steps in a week)	2.9	1.42	5
Social Features (messaging, groups, chat)	2.1	1.16	4

1. Perceived Importance: 1=Not at all important; 2=Not that important; 3=Neutral; 4=Important;5=Very important.