Selected Papers of #AoIR2018:
The 19th Annual Conference of the
Association of Internet Researchers
Montréal, Canada / 10-13 October 2018

PRIVACY BOUNDARIES AND INFORMATION FLOW SOLIPSISM IN THE PERSONAL FITNESS INFORMATION ECOSYSTEM

Michael Zimmer[1], Katherine Kritikos[1], Jessica Vitak[2], Priya Kumar[2], and Yuting Liao[2]
[1]University of Wisconsin, USA
[2]University of Maryland, USA

Introduction

Fitness trackers are an increasingly popular tool for tracking health and physical activity (Safavi & Webb, 2016). The miniaturization and ubiquity of smartphone and mobile sensors mean that a single device can track several aspects of a user's behavior (e.g., steps taken, floors climbed, heart rate, and calories burned). These data points, referred to as "personal fitness information" (PFI), reveal novel insights about users' physical activity, health, and personal habits (Crawford, Lingel, & Karppi, 2015).

The benefits of these devices hinge on ubiquitous data collection and the algorithmic processing of PFI. One early study found that Fitbit users wear their devices continuously, even while sleeping or showering, and have seemingly acquiesced to the device's requisite automated collection of PFI (Patterson, 2013). The PFI generated from fitness trackers, however, also contains potentially sensitive information that third parties may access in contexts that users do not anticipate. For example, court cases now regularly include evidence gleaned from fitness trackers (Alba, 2016) and medical and insurance providers increasingly seek access to fitness tracker data (Farr, 2017), leading privacy advocates to warn of an emerging "medical surveillance system" (Farr, 2015).

Given increased occurrences of third-party access to PFI, researcher have begun exploring how users balance the benefits of using fitness trackers with the privacy risks of sharing highly detailed data streams about their physical activity. In general, fitness tracker users do not express many privacy concerns about PFI collection (Gorm & Shklovski, 2016). Motti and Caine (2015) surmise users' lack of concern stems from a

Suggested Citation (APA): Zimmer, M, Kritikos, K, Vitak, J, Kumar, P, and Liao, Y. *Privacy Boundaries and Information Flow Solipsism in the Personal Fitness Information Ecosystem*. (2018, October 10-13) Paper presented at AoIR 2018: The 19th Annual Conference of the Association of Internet Researchers. Montréal, Canada: AoIR. Retrieved from http://spir.aoir.org.

lack of awareness regarding 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 U.S. Food and Drug Administration (FDA) recently announced it would lower some regulatory barriers for several technology companies – including those who design fitness trackers – to develop platforms for medical uses, such as screening PFI for medical conditions and potentially sharing that data with doctors (Farr, 2017).

This paper generates a more complete picture of users' experiences with fitness trackers and how they manage PFI privacy boundaries. Specifically, we argue while fitness tracker users take steps to manage privacy boundaries (Petronio, 2002), they also succumb to "information flow solipsism" (Proferes, 2017), meaning that while users might understand the primary technical functions and features of their fitness trackers, they are broadly unaware of "how the technology operates at a broader techno-cultural or socioeconomic level" (Proferes, 2017, p. 10). Our findings suggest that, largely due to the affordances of fitness tracker user interfaces and platforms, users are broadly unaware of how companies might collect and aggregate their PFI.

Methodology

Our mixed-methods approach involved a survey and semi-structured interviews. Participants were recruited through emails to a random sample of 6,000 employees at two American public universities. They were invited to complete an online survey if they were at least eighteen years old, owned a smartphone, and currently used a Fitbit or Jawbone device. Respondents could also indicate their willingness to participate in a follow-up interview. We received 363 valid completed surveys.

From the completed surveys, we used criterion sampling (Patton, 2005) to identify a subset of interviewees, and created four categories of users based on their relative (high vs. low) internet technology skills and their (high vs. low) general privacy concerns. During spring 2017, we interviewed 33 people across the two universities, with six to 11 people from each of the four possible categories. Interview transcripts went through multiple levels of coding in the qualitative analysis program Dedoose.

Summary of Findings

The majority of survey respondents (96%) used a Fitbit device, and most (71%) reported wearing it every day. Most respondents, however, had very limited knowledge of the companies' data tracking and retention policies: 73% did not know whether Fitbit or Jawbone sold their data and 66% were not sure who owned their data. Further, 85% of respondents did not know how long companies stored the data, and 89% were unsure where their data was stored besides the device.

Viewing our broader results through Petronio's (2002) Communication Privacy Management (CPM) theory, we see how users' conceptualizations of ownership, privacy rules, and turbulence surrounding their PFI influence how they manage privacy boundaries. Participants largely did not see PFI as sensitive, and most interviewees expressed only minimal privacy concerns related to their PFI: one-third of interviewees

simply responded “no” when asked whether they had any tracker-related privacy concerns. Some admitted to being largely unaware of any broader privacy issues related to using a fitness tracker, while others recognized they may need boundaries to manage the flow of their PFI, but they did not think PFI was sensitive enough to require them to define the contours and rules of such boundaries. Many interviewees expressed general ambivalence about the flow of their PFI, such as:

> I don’t think there’s that much information out there that really would hurt me if anybody knew about it. I don’t think there’s anybody that’s going to take my pattern of heart rate and go with and do anything to me. Where are you going to get that? Maybe that’s just I’m a trusting person or maybe that’s I’m naïve, but unless I have a reason for thinking or knowing that something’s going to hurt me, I don’t care.

As a result, few respondents noted making changes to their default privacy settings, perhaps a result of the limited privacy controls provided on the mobile apps most participants used to interact with the fitness tracking ecosystem. While some participants may have sought to maintain ownership of their PFI and establish “thicker” privacy boundaries, the platform’s affordances limited their ability to do so as granular control of data flows and visibility is only possible via the web interface, yet few respondents indicated ever visiting the platform’s web site to view data or adjust settings. Many could not remember adjusting their privacy settings at all, and assumed the default settings were still in place and trusted that their privacy was sufficiently protected as a result. For example, “I just assume I think that the protections are in place, the firewalls are in place that are going to protect me. I don't know why.”

As Proferes (2017) notes in his study of Twitter users, “[i]nformation flow solipsists may … be more broadly unaware of what happens to the information they produce beyond the ‘real-time’” (p. 10). Our findings suggest the dangers of information flow solipsism extends to fitness tracker users, where users might feel content with their management of privacy boundaries related to their PFI, while failing to understand how personal fitness information flows beyond their device lead to unanticipated privacy risks.

Acknowledgements
This research was funded by the National Science Foundation under Grant No 1640640.

References

Alba, A. (2016, April 19). Police, attorneys using fitness trackers as court evidence. New *York Daily News*. Retrieved October 27, 2017, from http://www.nydailynews.com/news/national/police-attorneys-fitness-trackers-court-evidence-article-1.2607432.

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.

Farr, C. (2015, April 9). Weighing privacy vs. rewards of letting insurers track your fitness. *NPR.org*. Retrieved October 27, 2017, from http://www.npr.org/sections/alltechconsidered/2015/04/09/398416513/weighing-privacy-vs-rewards-of-letting-insurers-track-your-fitness.

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

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.

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). Retrieved from http://fc15.ifca.ai/preproceedings/wearable/paper_2.pdf.

Patterson, H. (2013). Contextual expectations of privacy in self-generated health information flows (pp. 1–48). Presented at the TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy, Arlington, VA: TPRC. Retrieved from http://dx.doi.org/10.2139/ssrn.2242144.

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.

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.

Proferes, N. (2017). Information flow solipsism in an exploratory study of beliefs about Twitter. *Social Media + Society*, *3*(1), 1–17. https://doi.org/10.1177/2056305117698493.