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

Michael Zimmer[2], Priya Kumar[1], Jessica Vitak[1], Yuting Liao[1], and Katie Chamberlain Kritikos[2]

[1]University of Maryland [2]University of Wisconsin-Milwaukee

Project website: https://mobileprivacy.umd.edu

What do we mean by the **quantified self**?

Self-knowledge through self-tracking using technology.

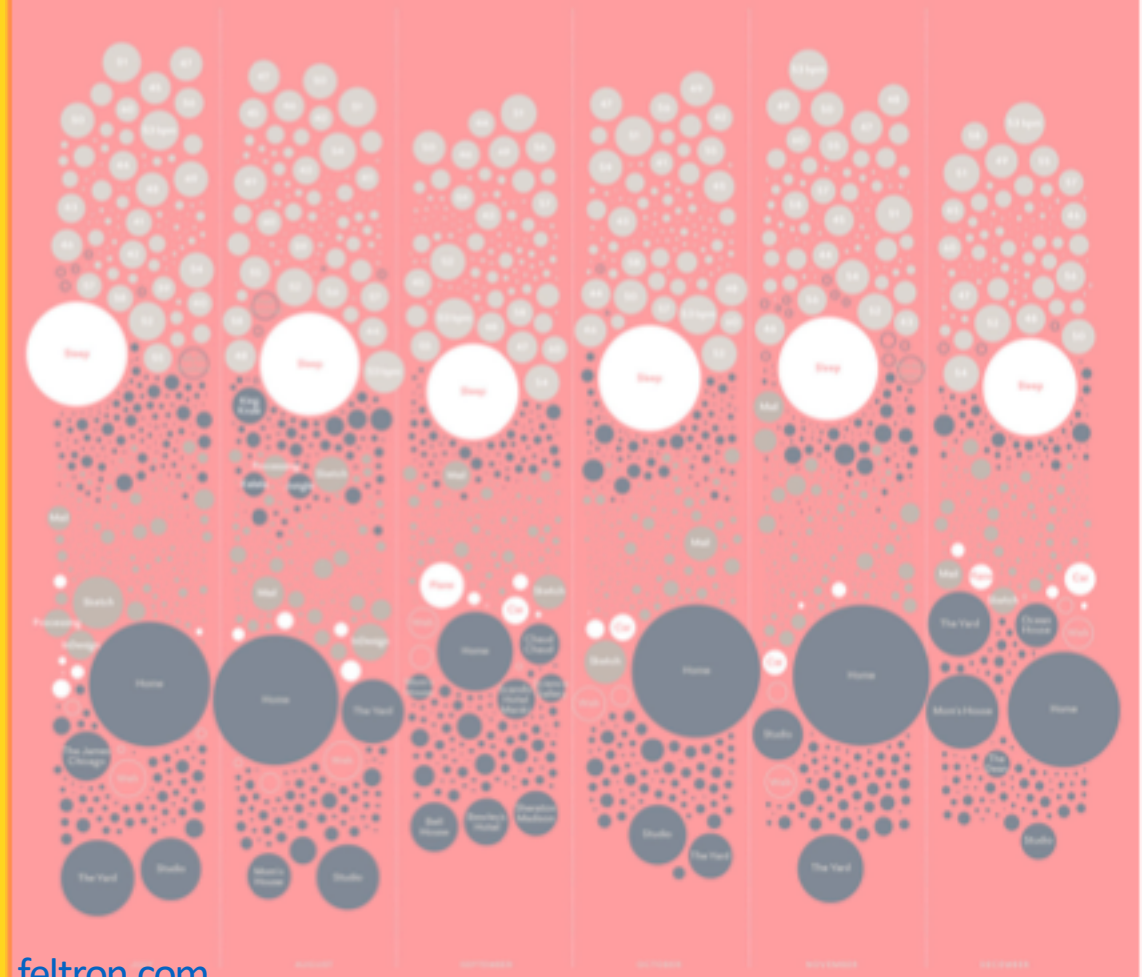
Fitness trackers are increasingly designed to be worn unobtrusively on the body—and to collect data constantly while worn.

Tracking Every Breath You Take & Every Move You Make

Fitness trackers collect **a lot** of data

- Steps taken
- Distance traveled
- Floors climbed
- Calories burned
- Time slept
- Heart rate
- Activity/workout statistics
- Location/GPS (sometimes)

Inferring Behavior from Data



feltron.com

- Dietary habits
- Stress levels
- Alcohol use
- Exposure to pollutants
- Social context
- Movement patterns

…

…

…

- Insurance rates?
- Fidelity?

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: Sampling

Random sample of 6000 university staff invited to participate in study if they owned a Fitbit/Jawbone

- 363 completed surveys
- Survey invited participants to enter email to participate in future studies (141 participants did this)

For analysis of survey results, see:

Vitak, J., Liao, Y., Kumar, P., Zimmer, M., & Kritikos, K. (2018). Privacy attitudes and data valuation among fitness tracker users. Proceedings of the 13th Annual iConference, Lecture Notes in Computer Science, vol 10766. (pp. 229-239). London: Springer. https://doi.org/10.1007/978-3-319-78105-1_27

Method: Interview Participant Selection

Divided potential interviewees into four categories:

- High Skill/High Concern
- High Skills/Low Concern
- Low Skill/High Concern
- Low Skill/Low Concern

Used criterion sampling (Patton, 2005) to select participants evenly across four categories.

Final dataset includes **33 interviews** across were analyzed through iterative coding process by all five authors (Lincoln & Guba, 1985).

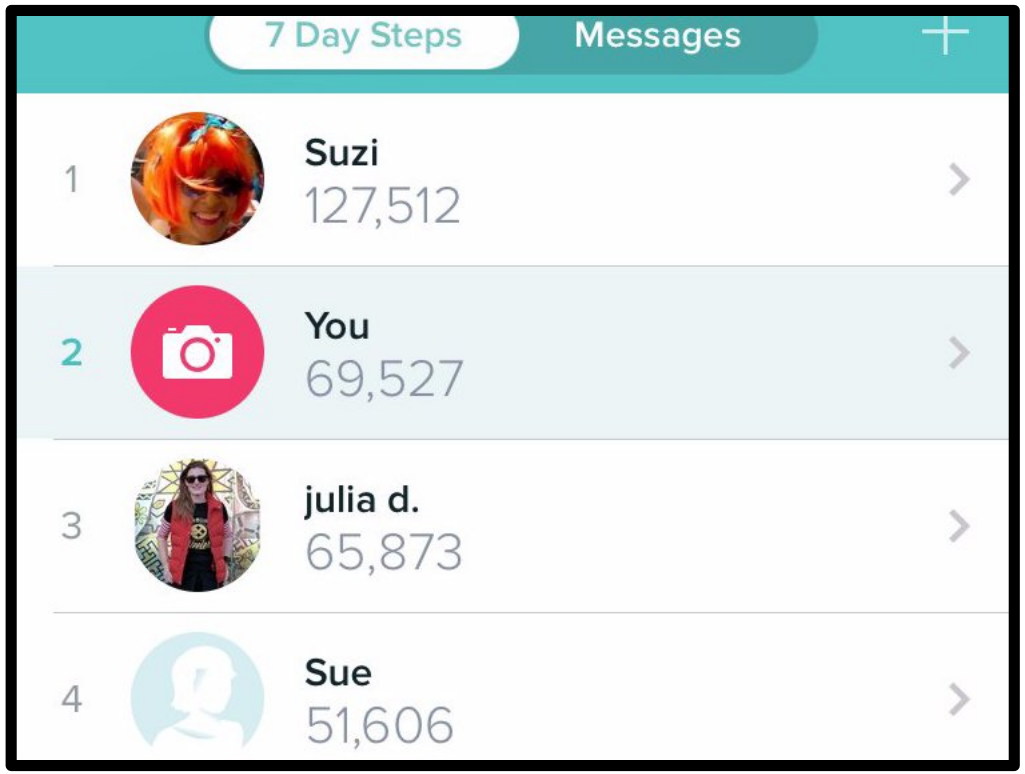
Interview Highlights: Perceived Benefits

- Trackers as part of daily routine
- Trackers as personal motivator
- Benefits beyond step tracking

Look how happy Fitbit makes people!

Interview Highlights: Perceived Drawbacks

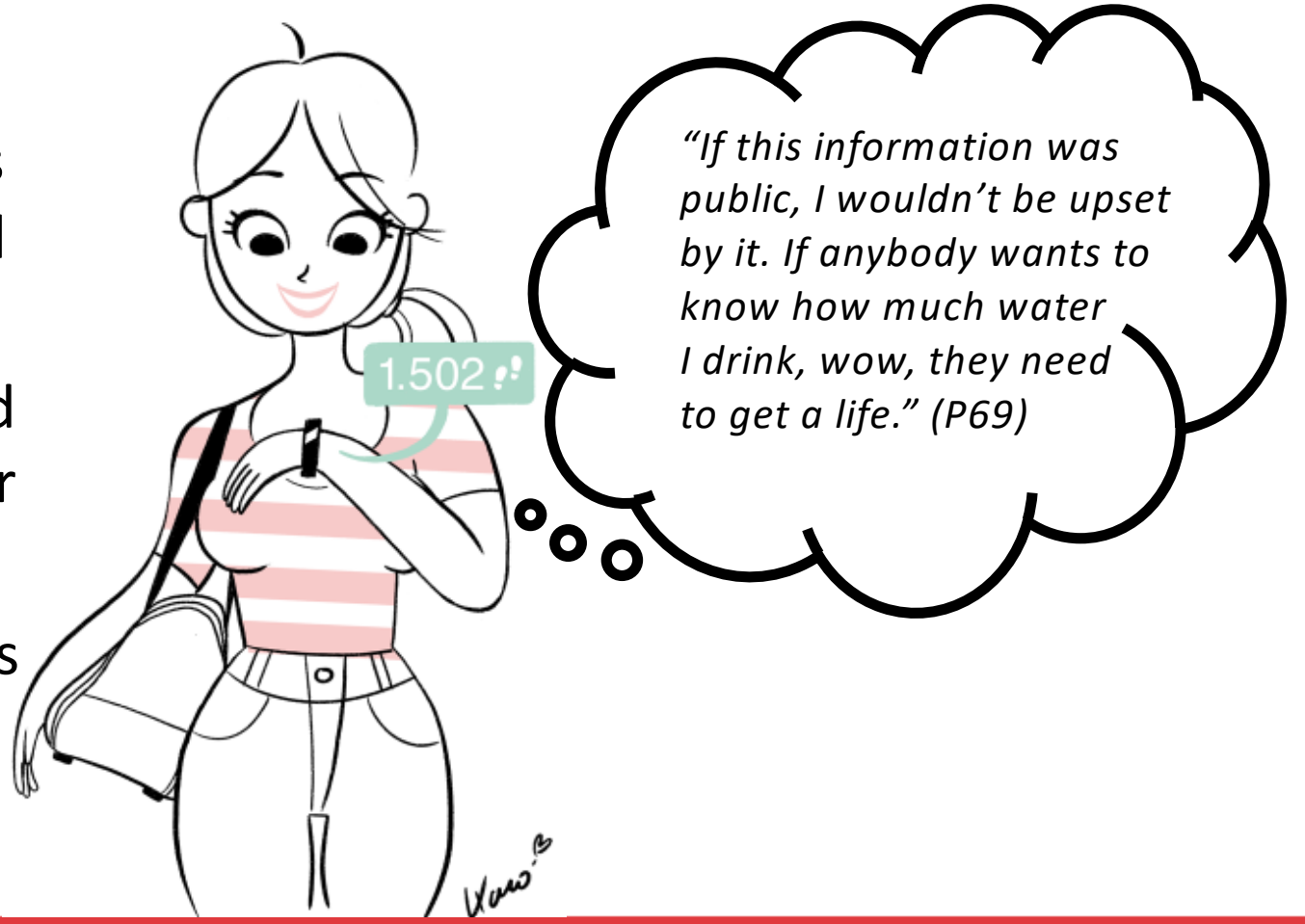
- In general, users perceived few drawbacks to these devices
- Lack of interest in social and gamification aspects
- Social comparison can be problematic



Do you ever even sleep, Suzi?

Interview Highlights: Privacy Concerns & PFI

- Most participants had minimal privacy concerns about their PFI (one-third said they had none)
- Some had not considered how PFI could be used for broader purposes
- Data is seen as innocuous and not sensitive



Interview Highlights: Privacy Concerns & PFI

Boundaries did exist for problematic data collection and sharing.

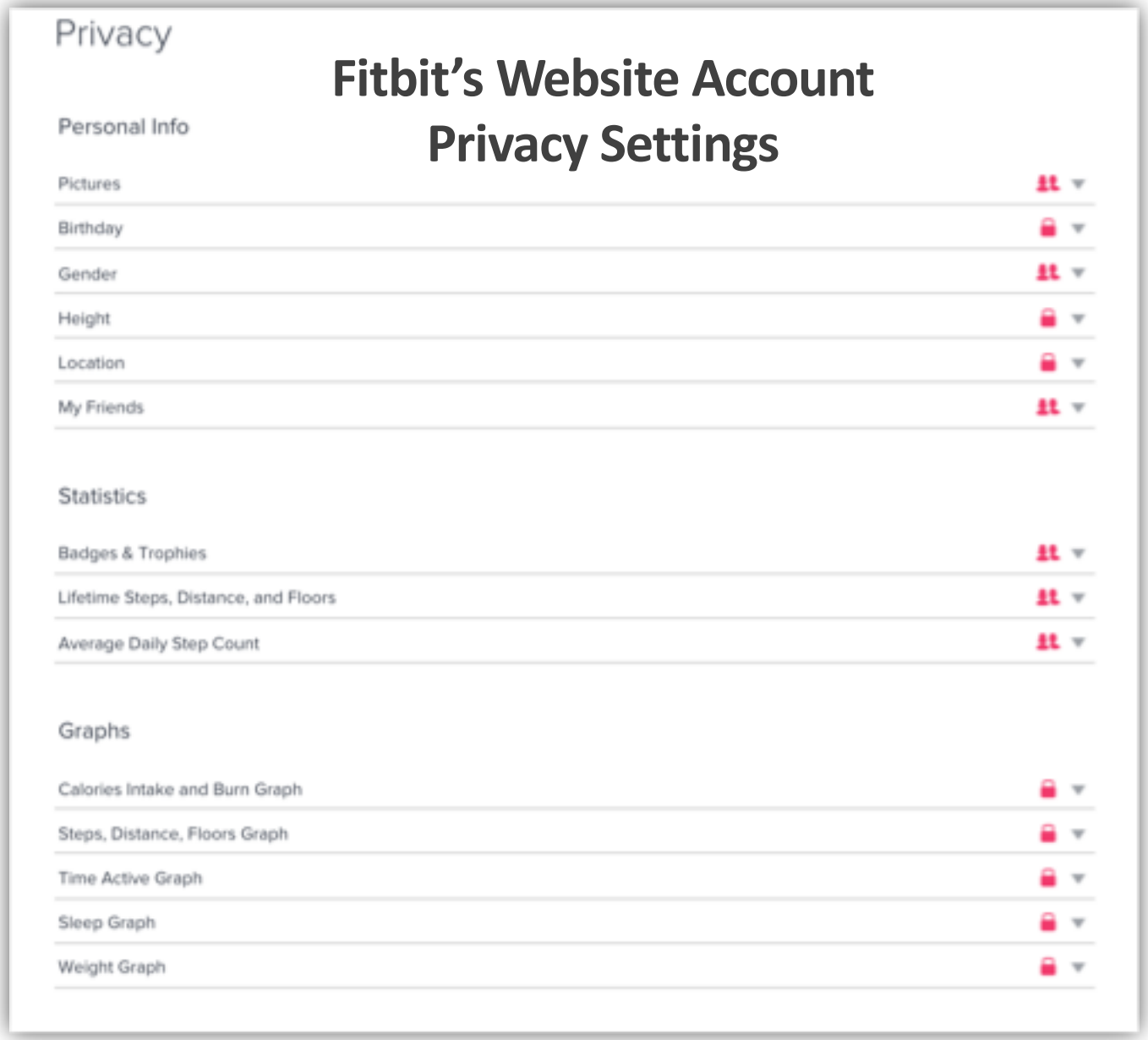
- Name: Probably OK
- Steps: OK
- Sleep: Maybe OK
- Location: Not OK
- DOB: Not OK
- Granular data: Not OK

"If you had exactly the number of steps someone took at which time, 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 think that invades my personal space where something personal to me being exposed to someone else." (P75)

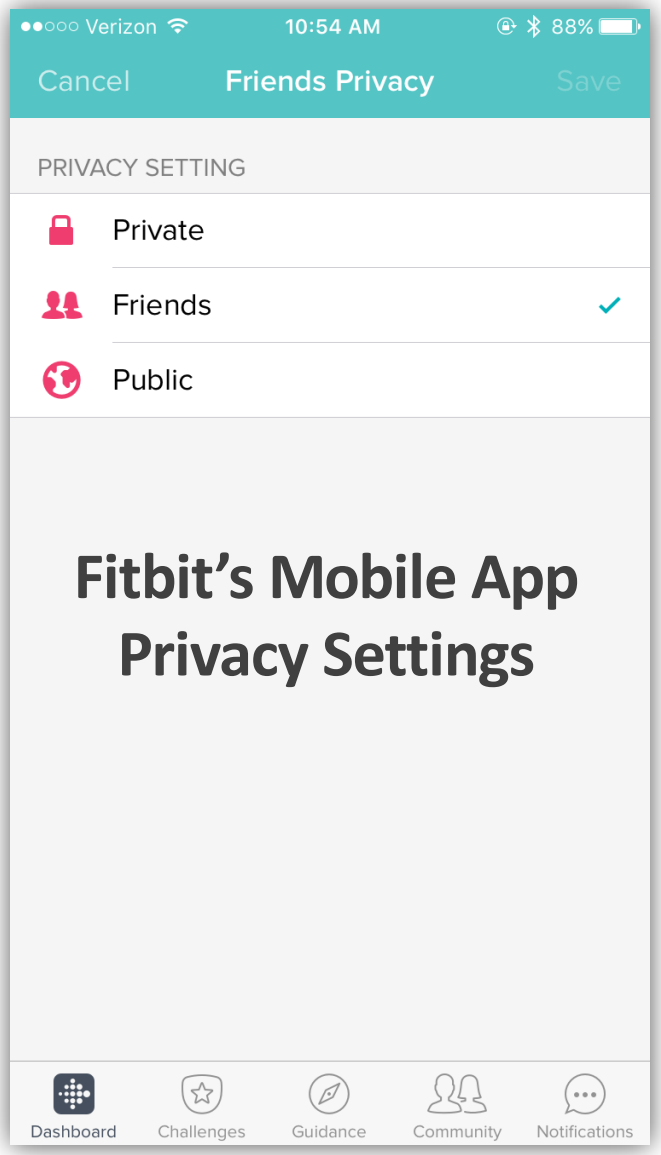
Interview Highlights: Privacy Behaviors

- ✓Low privacy concerns → minimal engagement with privacy features
- ✓Rely on default settings
- ✓Differences between app and web dashboard settings

Fitbit's Website Account Privacy Settings



Fitbit's Mobile App Privacy Settings



Theoretical Implications

We considered these interviews in light of Petronio's (2002) Communication Privacy Management (CPM) theory.

1. **Ownership**
   - ✓Thick boundary: Users want to own their PFI
   - ✓Thin boundary: Users do not change default privacy settings
2. **Privacy rules**
   - ✓Users share only basic PFI and only share with known social ties
   - ✓Users inherently trust fitness tracker companies
3. **Turbulence**
   - ✓Unaware of unanticipated sharing PFI with third parties

Conclusions and Future Research

We hypothesize that fitness tracker users:

- View the devices as a personal utility (even a toy)
- Do not engage in social activities, thus don't include trackers within set of concerns about social media privacy
- Don't concern themselves with how data is being collected, aggregated, shared

This leads to a normalization of data collection and aggregation, with little concern over data sensitivity.

Thanks!

Jessica Vitak

College of Information Studies
University of Maryland

jvitak@umd.edu
https://pearl.umd.edu
https://jessicavitak.com

This material is based upon work supported by the National Science Foundation under Grant Number 1640640.