

# Privacy Awareness: Zwift User Study

Tess Despres  
University of Washington  
Electrical and Computer Engineering  
tdespres@uw.edu

Tamara Bonaci  
Northeastern University  
Computer Science  
t.bonaci@northeastern.edu

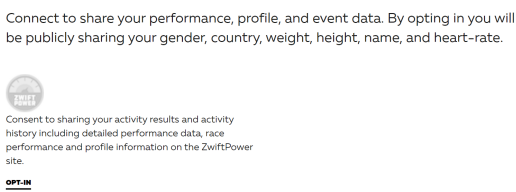
**Abstract**—We propose a research study focusing on human factors related to privacy of fitness trackers. We start our study by demonstrating potential privacy risks, by scraping public-facing data from the Zwift activity platform. We then focus on the question: why do users continue to share fitness data publicly using activity trackers, given the prevalence of documented privacy issues. To answer this question, we propose a survey investigating user mental models, perceived risks, and motivation behind the use of fitness and activity trackers. We, additionally, propose investigating if users attitudes surrounding the usage of activity trackers changed in the face of the COVID-19 pandemic.

## I. INTRODUCTION

Fitness tracking devices and services such as Strava, Apple Fitness+, and Fitbit are becoming more prevalent despite documented privacy risks [1], [2]. This increase of online fitness activity has been exacerbated by the recent closure of gyms and other fitness facilities due to COVID-19 [3]. We propose a study to investigate privacy awareness through the framework of Zwift, a fitness application built for the cycling and running community. The Zwift application records the users' speed and power output using device sensors which are then applied to make an avatar run or bike.

## II. MOTIVATION

We are motivated to help users understand and mitigate potential privacy risks. To get ranked in Zwift, many racers opt-in to the website ZwiftPower. ZwiftPower is a website that pulls data from Zwift races and posts the results publicly. In 2018 the site was briefly shut down due to violating GDPR compliance [4]. After user outcry, Zwift and ZwiftPower collaborated to restore the ZwiftPower platform [6]. In doing so, they have made ZwiftPower an opt-in service, with the message depicted in Fig. 1.



Connect to share your performance, profile, and event data. By opting in you will be publicly sharing your gender, country, weight, height, name, and heart-rate.

Consent to sharing your activity results and activity history including detailed performance data, race performance and profile information on the ZwiftPower site.

OPT-IN

Fig. 1. ZwiftPower Opt-in Message [6]

While the opt-in message clearly conveys to users that data will be shared publicly, many still choose to share identifying

information on ZwiftPower. In fact, we were able to scrape users' names, weights, heights, and countries from ZwiftPower profiles at scale. If users understand that their private data will be shared publicly, do they realize there could be associated privacy risks? If so, what motivates them to use this particular service? We believe examining this question could help to reduce privacy risks in the future design of fitness applications.

## III. PROJECT DESCRIPTION

This project focuses on our overarching question: “To what extent are users aware of potential privacy risks associated with fitness trackers? If they are aware why do they continue to share fitness data publicly?”. We aim to investigate the mental models that users hold of fitness trackers, as well as their motivation to use the technology. We are additionally interested in the users' awareness of the possible risks of these services, and their strategies for dealing with those risks. Lastly, we aim to investigate if and how perceived usages of these services changed during the COVID-19 pandemic. Guiding our investigation are the following research questions:

### A. Research Questions:

- 1) *Q1*: Are Zwift users currently aware of privacy risks and if so are they concerned about sharing data?
- 2) *Q2*: Has there been a perceived change in the amount of time users spend on Zwift due to the pandemic?
- 3) *Q3*: Do users predict a behavior change if they became aware that their data was being used for something they were not originally comfortable with?

### B. User Survey

To answer these questions we designed a user survey that is currently pending IRB approval.

## REFERENCES

- [1] Vitak, Jessica, Yuting Liao, P. Kumar, M. Zimmer, and Katherine Kritikos. “Privacy Attitudes and Data Valuation Among Fitness Tracker Users.” In IConference, 2018.
- [2] Hassan, Wajih Ul, S. Hussain, and Adam Bates. “Analysis of Privacy Protections in Fitness Tracking Social Networks -or- You Can Run, but Can You Hide?” In USENIX Security Symposium, 2018.
- [3] Etherington, Darrell. “Strava Raises 110 Million, Touts Growth Rate of 2 Million New Users per Month in 2020,” November 16, 2020. <https://techcrunch.com>
- [4] Zwift Insider. “All About ZwiftPower’s Temporary GDPR Shutdown,” May 31, 2018. <https://zwiftinsider.com/zwiftpower-and-gdpr/>.
- [5] Zwift Insider. “ZwiftPower Is Back,” July 5, 2018. <https://zwiftinsider.com/zwiftpower-is-back/>.
- [6] “Connections — My Zwift.” Accessed November 28, 2020. <https://my.zwift.com/profile/connections>.