OPEN EFFECT

Every Step You Fake

A Comparative Analysis of Fitness Tracker Privacy and Security

Open Effect
Version 0.3
February 2, 2016

[This page intentionally left blank]

Electronic version first published at openeffect.ca in 2016 by Open Effect. Open Effect is a Canadian not-for-profit applied research organization focusing on digital privacy and security.

The Citizen Lab at the Munk School of Global Affairs, University of Toronto contributed expertise and equipment in support of this project. Open Effect and the Citizen Lab are collaborative research partners. Together, the two groups engage in research that investigates the intersection of digital technologies and human rights.

This project is funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC.

Document Version: 0.3

Information presented in this document is for research and educational purposes only. These materials do not constitute solicitation or provision of legal advice. Open Effect makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained in this document. Nothing herein should be used as a substitute for the legal advice of competent counsel.

ABOUT THIS DOCUMENT

Document Version: 0.3

Fitness tracking devices monitor heartbeats, measure steps, sleep, and tie into a larger ecosystem of goal setting, diet tracking, and other health activities. *Every Step You Fake* investigates the privacy and security properties of eight popular wearable fitness tracking systems. We use a variety of technical, policy, and legal methods to understand what data is being collected by fitness tracking devices and their associated mobile applications, what data is sent to remote servers, how the data is secured, with whom it may be shared, and how it might be used by companies.

This research is led Open Effect, with significant contributions from the Citizen Lab at the Munk School of Global Affairs, University of Toronto. The project is funded by the Office of the Privacy Commissioner of Canada's Contributions Program.

NOTE:
This version serves as an early release of two sections of the report, published before the rest of the findings so that consumers can learn sooner about what companies are doing to secure their personal information. The two sections released are the study background, and the technical methodology and findings.

ABOUT THE ORGANIZATIONS

OPEN EFFECT

Open Effect is a Canadian not-for-profit that conducts research and advocacy focused on ensuring that people's personal data is treated securely and accountably. It builds interactive advocacy tools to empower individuals to learn about and exercise their rights online. Open Effect's research on the adoption of has been published in peer-reviewed studies.

`https://openeffect.ca`

CITIZEN LAB

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto, Canada. It focuses on advanced research and development at the intersection of Information and Communication Technologies (ICTs), human rights, and global security.

`https://citizenlab.org`

ABOUT THE AUTHORS

Andrew Hilts is the Executive Director and research lead at Open Effect. His research and software development focuses on empowering citizens to exercise their digital rights online. He is a research fellow at the Citizen Lab at the Munk School of Global Affairs, and has a Master of Information from the University of Toronto.

Dr. Christopher Parsons received his Bachelor's and Master's degrees from the University of Guelph, and his Ph.D from the University of Victoria. He is currently a Postdoctoral Fellow at the Citizen Lab at the Munk School of Global Affairs as well as the Managing Director of the Telecom Transparency Project at the Citizen Lab.

Jeffrey Knockel is a Senior Research Fellow at the Citizen Lab at the Munk School of Global Affairs, and a Ph.D student in Computer Science at the University of New Mexico. He has used reverse engineering techniques to study how digital technologies affect people's freedom to communicate on the Internet in multiple peer-reviewed studies.

CONTENTS

INTRODUCTION

Canadians, and many people around the world,[1] are increasingly purchasing, and using, electronic devices meant to capture and record the relative levels of a person's fitness.

Unlike past fitness devices, such as pedometers, electronic fitness trackers are designed to display aggregate fitness information automatically on mobile devices and, frequently, on websites developed and controlled by the company that makes the given device. This automatic collection and dissemination of fitness data began with simply monitoring the steps a person had taken in a day.

Contemporary consumer fitness wearables collect a broad range of data. The number of floors, or altitudinal changes, a person climbs a day is measured, levels and deepness of sleep, and heart rate activity are all captured by best-of-class consumer-level fitness trackers. And all of this data is of interest to the wearers of the devices, to companies interested in mining and selling collected fitness data, to insurance companies, to authorities and courts of law, and even potentially to criminals motivated to steal or access data retained by fitness companies.

Every Step You Fake explores what information is collected by the companies which develop and sell some of the most popular wearables in North America. Moreover, it explores whether there are differences between the information that is collected by the devices[2] and what companies say they collect, and what they subsequently provide to consumers when compelled to disclose all the personal information that companies hold about residents of Canada. In short, the project asks:

- Were data which are technically collected noted in companies' privacy policies and terms of service and, if so, what protections or assurances do individuals have concerning the privacy or security of that data?
- What of that data is classified by the company as 'personal' data, which is tested by issuing legally compelling requests for the company to disclose all the personal data held on a requesting individual?
- Does the information received by the individual match what a company asserts is 'personally identifiable information' in their terms of service or privacy policies?

Questions of what data a company collects, under what conditions, and how they are treated are critical in this era of big data, and made even more important given the often intimate and personal data captured by fitness trackers and their associated mobile applications. Canadians

[1] This report is funded by the Office of the Privacy Commissioner of Canada. We therefore focus much of our writing on Canadians and Canadian regulations. However, our findings should generally interest persons internationally who are concerned about privacy and security.

[2] Confirmed through technical analyses of data transmissions from devices, to mobile devices, and to the servers of fitness tracker companies.

need to understand what exactly is captured to determine if they are comfortable with their fitness tracker also recording each place they open the company's corresponding fitness application. They need to determine what a company will do with their fitness information in the event of a corporate sale or bankruptcy. And they need to know whether the company that produced the band or watch on their wrist is willing to comply with Canadian law when required. And transparency concerning how these bands operate, and the levels of privacy assured to consumers, is more and more important as insurance companies, government authorities, courts, corporate and academic researchers, and marketers develop an increasing interest in gaining access to fitness data in both bulk and granular form.

In short, this report explores what kinds of data fitness trackers generate and disseminate, and compares this with both what companies state they collect in policy documents, and in disclosures when forced to comply with Canadian privacy legislation.

- **Section 1** provides a background to fitness wearables and a more comprehensive explanation of the project's research questions.
- **Section 2** focuses on the technical research conducted, including the methodologies employed and results obtained. We include discussions of various security vulnerabilities we discovered over the course of our research as well as their relative significance for fitness tracker users.

The following sections will be forthcoming in later versions of this report.

- **Section 3** outlines the methodologies used to collect privacy policies and terms of service which we subjected to analysis, as well as the major findings that emerged from those analyses.
- **Section 4** begins by discussing the methods we when asking consumers to request their personal information from fitness wearable companies as well as the most significant findings that resulted from these requests.
- **Section 5** discusses the extent to which the data companies are collecting from their fitness wearables correlates with information disclosed in their terms of service and privacy policies, and to consumers who request access to all the personal information retained by a given company.
- **Section 6** offers recommendations to companies for improving the transparency of their data collection, the security of data collected and transmitted, and best practices for responding to individuals' requests for their personal information.
- **Section 7**, our conclusion, presents a summary of key points raised in the report.

1 BACKGROUND AND RESEARCH QUESTIONS

Personal health is a pressing issue for many Canadians. They are inundated with advertisements, research reports, and news articles asserting that obesity is a growing and serious problem and, at the same time, are presented with more calorie rich food that is actively designed to induce higher levels of consumption.[3] One of the many 'solutions' to overcoming personal exercise deficits or obesity is for people to wear fitness tracking devices to measure their exercise. The challenge, as noted by experts at a Quantified Self forum, is that the "[m]akers of self-tracking tools are today's de facto stewards of self-collected data" and that many people believe, and find that, "[c]ommercial stewardship creates particular access challenges. From a self-tracker's perspective, access to our data is insecure when it is controlled by commercial stewards with conflicting interests whose corporate lifespan may be brief."[4]

This report focuses on how fitness tracking devices and their associated smartphone and web applications collect, process, and utilize the data collected from users. Its primary focus is on the devices that individuals wear[5] and the mobile applications that individuals typically use to view their aggregate fitness activity.

In this section we provide an overview of fitness tracking itself, the industry, how trackers and companies were chosen for inclusion in the project, as well as some of the reasons why understanding the information collected by fitness tracking companies is important to Canadians. We conclude by discussing the specific research questions that drive all of the research undertaken in Sections 2, 3, and 4.

1.1 WHAT IS FITNESS TRACKING?

Fitness trackers are marketed on the basis that automated and manual data tracking, combined with encouragements to maintain or improve personal states of fitness, will empower wearers to adopt positive health habits. The metrics that are collected by wearables let individuals "find meaningful correlations between diet, exercise, sleep, and mental, physical, and cognitive well-being."[6] Data which is collected is alternately 'owned' by either the individual or company providing the tracker and associated analysis systems.[7]

[3] Michael Moss. (2013). Sugar, Salt, Fat: How the Food Giants Hooked Us. Toronto: Signal.

[4] Gary Wolf and Ernesto Ramirez. (2014). "Quantified Self Public Health Symposium," QS, April 2014, retrieved `http://quantifiedself.com/symposium/Symposium-2014/QSPublicHealth2014_Report.pdf`.

[5] The bands, phones, or bracelets contain a range of sensors that can collect data pertaining to altitudinal changes, number of steps taken in a day, heart rate, to name a few.

[6] Heather Patterson. (2013). "Contextual Expectations of Privacy in Self-Generated Health Information Flows," TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy. Available at SSRN: `http://ssrn.com/abstract=2242144`.

[7] Greg Paul and James Irvine. (2014). "Privacy Implications of Wearable Health Devices," SIN '14 Proceedings of the 7th International Conference on Security of Information and Networks. Pp. 117- ; see also Section

Wearable fitness tracking devices collect varying kinds of data. At their most basic they tend to collect the number of footsteps a person takes in a given period of time and transmits that data either to a mobile phone application exclusively, or to a fitness company's servers by way of an application installed on a mobile phone. The sensors in the wearable, especially when combined with those integrated with mobile phones and which are often accessible by installed fitness tracking mobile applications, can often be used to automatically collect far more information that just footsteps, including:

- altitudinal changes (i.e. floors walked up)
- heartbeat information
- geolocational information
- period of time slept
- quality of sleep
- quality of activity (e.g. light, moderate, vigorous)
- type of activity (e.g. walking, swimming, sports)

Some companies also encourage individuals to manually input information that relates to personal fitness but that cannot be automatically collected by the wearable devices themselves. Examples include:

- specifying all food consumed, its nutritional values, and the time at which it is consumed
- personal moods
- specific type of activity undertaken
- fitness goals (e.g. steps taken, calories burned, amount of sleep)

For companies that offer a 'fitness social network' alongside the device tracking and manual data entry options, individuals can often comment on one another's fitness activities or meals or moods, rank themselves against their 'friends', or even enter into fitness challenges with one another.

1.2 THE FITNESS WEARABLE INDUSTRY

The fitness wearable industry is booming. Analysts valued the market at approximately $2 billion in 2014 and predicted it would increase to as much as $5.4 billion by 2019.[8] Moreover, while

Three of this report (Forthcoming).

[8] Paul Lamkin. (2015). "Fitness tracker market to top $5bn by 2019," Wareable, March 26, 2015, retrieved January 20, 2016, http://www.wareable.com/fitness-trackers/fitness-tracker-market-to-top-dollar-5-billion-by-2019-995.

Vendor	2Q15 Shipment Volume	2Q15 Market Share	2Q14 Shipment Volume	2Q14 Market Share	2Q15/2Q14 Growth
Fitbit	4.4	24.30%	1.7	30.40%	158.80%
Apple	3.6	19.90%	0	0.00%	–
Xiaomi	3.1	17.10%	0	0.00%	–
Garmin	0.7	3.90%	0.5	8.90%	40.00%
Samsung	0.6	3.30%	0.8	14.30%	-25.00%
Others	5.7	31.50%	2.6	46.40%	119.20%
Total	18.1	100.00%	5.6	100.00%	223.20%

Table 1: Top Five Wearables Vendors, Shipments, Market Share and Year-Over-Year Growth, Q2 2015 (Units in Millions)[12]

there are predictions that dedicated fitness trackers might sell only 68 million units in 2016, down from 70 million, some analysts suggest the decrease follows from consumers purchasing smart watches that include fitness tracking functionality.[9] As new products and devices have come to market, such as various smart watches offered by Apple, various Android watches, as well as Withings and Fitbit, other market competitors have exited the space. Most notably this has included Nike, which offered the FuelBand as part of the company's fitness platform, and which was integrated with a range of Nike products.

The most prominent fitness wearable leader has been Fitbit. The company launched itself as a publicly traded company in 2015 and received a $4 billion market capitalization after first issuing shares.[10] The same year, Apple released its Apple Watch. In the second quarter of 2015, market analysts estimate that Fitbit shipped 4.4 million units whereas Apple was estimated to have sold through 3.6 million of their devices.[11] Other markets, such as China, have been dominated by non-Western companies' products. In China and beyond, Xiaomi has aggressively sold fitness trackers with comparable sensors as baseline fitness wearables (e.g. step tracking, altitudinal changes, heart rate monitoring) at prices well below those of Western market leaders. Garmin has also aggressively sought to target "citizen athletes" though its market share decreased between 2014 and 2015. Table 1, reproduced from IDC Research Inc., showcases the relative market positions of major fitness wearable companies as of the second quarter of 2015.

It remains unclear how long consumers actually keep using purchased fitness trackers. Research indicates that trackers are often set aside or taken off, and never used again, after rela-

[9] Nick Statt. (2015). "The rise and fall of fitness trackers," C|Net, January 1, 2015, retrieved January 20, 2016, http://www.cnet.com/news/fitness-trackers-rise-and-fall/.

[10] Jessica Menton. (2015). "Fitbit IPO: Wearable Fitness Tracker Valued At More Than $4B, Begins Trading On NYSE Under 'FIT'," IBT, June 18, 2015, retrieved January 20, 2016, http://www.ibtimes.com/fitbit-ipo-wearable-fitness-tracker-valued-more-4b-begins-trading-nyse-under-fit-1972313.

[11] IDC. (2015). "IDC Worldwide Quarterly Wearable Device Tracker," IDC, August 2015, rerieved January 20, 2016, http://www.idc.com/getdoc.jsp?containerId=prUS25872215.

Company	Wearable	Application and version
Apple	Apple Watch	Watch 2.1
Basis	Basis Peak	Basis Peak 1.14.0
Fitbit	Fitbit Charge HR	Fitbit 2.10
Garmin	Garmin Vivosmart	Garmin Connect 2.13.2.1
Jawbone	Jawbone Up 2	Jawbone UP 4.7.0
Mio	Mio Fuse	Mio GO 2.4.4
Withings	Withings Pulse O2	Withings Health Mate 2.09.00
Xiaomi	Xiaomi Mi Band	Mi Fit 1.6.122

Table 2: Fitness tracking applications and devices studied

tively short periods of use.[13] To overcome this limitation, an analysis of smartphone manufacturers' applications stores, and checking which fitness applications associated with wearable devices were most popular, was the only semi-reliable way for us to determine how popular different companies' devices are within Canada. This analysis cannot, however, predict how many Canadian residents are currently using fitness trackers, whether they were ever owners of such trackers (some of the smartphone applications can use the phone's internal sensors to collect some fitness data), the period of time over which the applications were downloaded, or even the total number of downloads of applications in the case of Apple's store.

1.3 FITNESS TRACKERS STUDIED

Fitness trackers included in this study were selected based on two criteria. First, we identified the most popular fitness tracking applications in the Google Play store as of mid-2015. Second, we included a Canadian fitness tracker, the Mio Fuse, to see how a Canadian product fared relative to market leaders. Table 2 identifies the specific companies and products examined.

1.4 POLICY AND SECURITY RATIONALES FOR STUDY

The rapid integration of fitness-tracking activities into daily life and business has introduced questions about device security, data practices of fitness companies and their cloud services, and the disclosure of personal information to third parties. Moreover, academic studies have showcased how persons who wear fitness trackers are often concerned about the amounts of

[13] Endeavour Partners. (2014). "Inside wearables: How the science of human behavior change offers the secret to long-term engagement," Endeavor Partners, January 2014, retrieved January 20, 2015, http://endeavourpartners.net/assets/Endeavour-Partners-Wearables-White-Paper-20141.pdf; Endeavour Partners. (2014). "Inside wearables: Part 2," Endeavor Partners, July 2014, retrieved January 20, 2015, www.endeavourpartners.net/assets/Endeavour-Partners-Inside-Wearables-Part-2-July-2014.pdf. See also: Amanda Lazar, Christian Koehler, Joshua Tanenbaum, and David H. Nguyen. (2015). "Why We Use and Abandon Smart Devices," UBICOM '15, September 7-11, 2015, Osaka, Japan.

data that are collected by fitness wearable companies, the (in)accessibility of the data once collected, and the ways in which is it subsequently processed, stored, and shared by fitness tracker companies.[14]

Beyond consumers, a range of other actors have become interested in the kinds of data collected by fitness trackers and the ways in which the data can be utilized. There have been situations where fitness tracker-related information has been introduced into cases concerning sexual assault[15] and civil claims pertaining to personal injury.[16] Such data, if it can be manipulated, brings such evidence into question as well as the broader trustworthiness of fitness tracker data. Corporate wellness programs, where individuals or workplaces provide some fitness related information to wellness providers, have shown interest in fitness tracking data as the data can reveal whether health premiums should be reduced or raised in relation to the relative fitness of the monitored persons. Similarly, persons interested in 'cheating' a fitness wearable-based premium system might be motivated to manipulate data that is collected either for themselves or as part of their own fitness tracker 'cheating' service. And there are also concerns that the radios in fitness trackers could be used to monitor their wearers' movements; similar kinds of surveillance, reliant on Bluetooth radios in mobile devices, can be used by retailers to track consumer movements,[17] and have previously been conducted en masse without research subjects ever realizing their movements were being followed.[18]

Worries linked to the range of parties that may be interested in accessing either fitness-related data or other transmissions from the wearable devices are compounded by the relative lack of overt regulation surrounding how fitness tracker data can be collected, processed, retained, or propagated. In the cases of many fitness tracker companies these worries are entirely legitimate. Many of the companies that collect data from devices, from consumers' manual data entry, and from the social networking aspects of their services reserve rights to the data.

[14] Heather Patterson. (2013). "Contextual Expectations of Privacy in Self-Generated Health Information Flows," TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy. Available at SSRN: http://ssrn.com/abstract=2242144; Vivian Genaro Motti and Kelly Caine. (2015). "Users' Privacy Concerns About Wearables: impact of form factor, sensors and type of data collected" in Financial Cryptography and Data Security: FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, January 30, 2015. Michael Brenner, Nicolaw Christin, Benjamin Johnson, and Kurt Rohloff (Eds.). New York: Springer. 231-244.

[15] Unknown Author. (2015). "Police charge woman for making up a rape after she was exposed by her own FitBit," News.Com.Au, June 24, 2015, retrieved June 25, 2015, http://www.news.com.au/lifestyle/police-charge-woman-for-making-up-a-rape-after-she-was-exposed-by-her-own-fitbit/story-fneszs56-1227412671705.

[16] Christina Bonnington. (2014). "Data From Our Wearables Is Now Courtroom Fodder," Wired, December 12, 2014, retrieved December 15, 2014, http://www.wired.com/2014/12/wearables-in-court/.

[17] McCarthy, Bill (2015). Using Location-Based Analytics to Understand the Customer Journey. ShopperTalk. http://www.shoppertrak.com/using-location-based-analytics-to-understand-the-customer-journey/.

[18] Paul Lewis. (2008). "Bluetooth is watching: secret study gives Bath a flavour of Big Brother," The Guardian, July 21, 2008, retrieved January 20, 2015, http://www.theguardian.com/uk/2008/jul/21/civilliberties.privacy.

Such rights can include commercially sharing it, conducting data analyses of it, providing it to government authorities, and disposing of it as an asset in the case of bankruptcy or merger processes. Data may also be shared either on an individual or aggregate basis, though companies often 'anonymize' data prior to providing it to third parties. We discuss this in more depth in Section 3 (forthcoming).

United States-based companies can engage in many of the aforementioned practices with the data collected from the wearable devices on the basis that fitness tracker data is not classified as 'health' data. Companies can more freely analyze and share fitness information as compared to formally classified 'health' data as a result.[19] In contrast, Health Canada has avoided asserting that wearables must, or do not need to, comply with strict health data laws; in an report published by the Office of the Privacy Commissioner of Canada (OPC) the authors write that the "scope of wearable devices that could be subject to [health] regulations could broaden as the line between health monitoring and interventionist medical devices becomes less defined."[20] Though the same authors avoid engaging in a detailed analysis of how Canadian commercial privacy legislation[21] applies to wearables they instruct wearable companies that recommendations the OPC has released concerning mobile application developers, gaming consoles, and online behavioural advertising "are relevant in the context of wearable computing as well."[22] And even without specific guidance on what wearable companies must do to remain compliant with Canadian law, broadly companies can examine guidance concerning the application of PIPEDA to develop lawful practices concerning the collection, processing, retention, and dissemination of fitness-related information.

Europe, in contrast to either the United States or Canada, has provided clearer guidance to fitness tracker companies. Specifically, the European Data Protection Supervisor (EDPS) has asserted that 'lifestyle' information associated with fitness trackers constitutes personal information when the collected data enables inferences about a person's health, "especially when the purpose of the application is to monitor the health or well-being of the individual (whether in a medical context or otherwise)."[23] Given that many fitness companies provide health-related

[19] Heather Patterson. (2013). "Contextual Expectations of Privacy in Self-Generated Health Information Flows," TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy. Available at SSRN: `http://ssrn.com/abstract=2242144.`; Greg Paul and James Irvine. (2014). "Privacy Implications of Wearable Health Devices," SIN '14 Proceedings of the 7th International Conference on Security of Information and Networks. Pp. 117

[20] Office of the Privacy Commissioner of Canada. (2013). "Wearable Computing: Challenges and opportunities for privacy protection," retrieved from `https://www.priv.gc.ca/information/research-recherche/2014/wc_201401_e.asp.`

[21] As captured through the Personal Information and Protection of Electronic Documents Act (PIPEDA)

[22] Office of the Privacy Commissioner of Canada. (2013). "Wearable Computing: Challenges and opportunities for privacy protection," retrieved from `https://www.priv.gc.ca/information/research-recherche/2014/wc_201401_e.asp.`

[23] European Data Protection Supervisor. (2015). "(Opinion 1/2015) Mobile Health: Reconciling technological innovation with data protection," EDPS, May 21, 2015.

advice as part of their algorithmic analysis of activity, sleep, and food consumption logs, the EDPS effectively maintains that companies cannot treat ‘fitness’ data as non-personal information and, as such, must treat the data with a degree of sensitivity that stands in contrast to data that does not intrude into a person’s life.

1.5 CORE RESEARCH QUESTIONS

Broadly, this report exposes the relationship between the data collection and transmission practices of fitness tracking devices and associated applications, cloud services offered by device manufacturers, and how third parties may obtain access to personal information collected by these devices. We hypothesize that there will be variation in how technically secure the commercial products are, in their commitments to individual control of personal data, and in company responsiveness to right to information requests. Specifically, more established companies or those that have encountered parliamentary/congressional questions of device data integrity will offer more secure and privacy-protective products. In contrast, we hypothesize that younger companies will be be less effective in protecting users’ data or communicating privacy risks.

To investigate the veracity of these hypotheses we ask the following questions:

1. What technical security mechanisms are in place for each device with regard to data collection, storage, and transmission practices, and as a result what sort of data could an attacker obtain by targeting each of those practices?
2. What categories of data does each device’s privacy policy state they collect, and what categories does technical analysis reveal devices to collect?
3. What data can Canadians obtain through right to information requests sent to each device manufacturer?

In responding to these questions it will become apparent which devices and companies offer more privacy protective products and services, as well as evaluate whether there are commonalities (e.g. engagement with regulators or parliaments) that have led some companies to provide such protective products.

2 TECHNICAL RESEARCH AND FINDINGS

Our investigation looks into the relationship between the data collection and transmission practices of fitness tracking devices, cloud services offered by device manufacturers, and how third parties may obtain access to personal information collected by these devices. To learn about this relationship, we adopted a mixed-methods approach that involved technical analysis, document and policy analysis, and legal compliance tests. In aggregate these methods let us understand the actual data that are collected, transmitted, and processed by companies, what data companies publicly state they collect and how they use it, as well as the ability for Canadian residents to compel companies to disclose information. By contrasting all three methods, and as discussed in Section 5 (Forthcoming), it will become apparent just how much data is collected, its security, as well as the ability for individuals to learn about practices or access data that has already been collected.

This section focuses exclusively on the technical testing conducted over the course of the project. Specifically, it:

- Outlines the specific methodologies used to investigate how data was transmitted over Bluetooth radios that are embedded in the wearables, over the Internet, and how mobile applications secured or processed data sent to them by wearables and received from company servers;
- Presents the findings of our tests, in the same sequence as the methodology, along with the broader significances of such findings;
- Concludes by identifying common technical deficits that applied across a range of wearables and brief summations of how technical findings either confirm, or refute, concerns that individuals have about fitness tracking surveillance as noted in Section 1.4.

2.1 TEST DEVICES

We purchased our test devices from various online stores in the summer of 2015. We purchased fitness tracking devices from from Apple, Amazon.ca, Best Buy, and AliExpress. We additionally obtained a test iPhone 6 directly from Apple and a Google Nexus 5 from Amazon.ca.

2.2 TECHNICAL METHODOLOGY

We use several technical research methods to identify the data that fitness trackers transmit to mobile applications, that mobile applications send to and receive from the Internet, as well as the security practices employed to safeguard fitness information. In what follows we first discuss the techniques used to examine Bluetooth transmissions, then Internet-based transmissions, and finally the extent to which mobile device applications are developed to secure and maintain the integrity of individuals' fitness data.

2.2.1 TRANSMISSIONS OVER BLUETOOTH

Fitness bands routinely communicate with mobile device applications using the Bluetooth communications protocol. This protocol is designed to exchange data over short distances and has been updated numerous times since it was introduced as an Institute of Electrical and Electronics Engineers (IEEE) standard.

Fitness wearables establish connections with mobile devices using the Bluetooth protocol. Creating these connections involves the trackers making themselves discoverable to devices, such as mobile devices, by publicly broadcasting advertising packets. Devices that are listening for such packets can discover the unique Media Access Controller (MAC) address broadcast within these packets; this address is included in the advertising packets so that a mobile phone or other connecting device knows which device it should pair with.

In some cases data may be accessible when the Bluetooth radio emits information; this is true in cases where a Bluetooth radio was released before the contemporary privacy features were built into the protocol, or where the developer does not activate the private protective characteristics in the current Bluetooth protocol. Where such emitted data contains content (e.g. fitness information) a third party might be able to intercept the data. Where the data contains addressing information a third party might be able to monitor the location of where a device is physically positioned; over time, such monitoring might be used to track an individual's movements. For our research, we focused exclusively on whether addressing information was accessible to third parties and did not examine whether Bluetooth payloads transmitted between fitness wearables and mobile devices were encrypted.

In the course of analyzing Bluetooth communications between fitness wearables and our test mobile devices we monitored for how, and whether, unique identifiers such as MAC address of wearables were accessible using RamBLE.[24] RamBLE is an Android application that scans the Bluetooth wireless spectrum for advertising devices and saves the found MAC addresses in a timestamped database. We initiated RamBLE scans daily for 3 days to determine whether the same addresses could be collected by RamBLE. For these tests, we disconnected each fitness tracker from our test phones by disabling Bluetooth on the phones, as a user might do in order to conserve battery life. We then repeated these tests at later dates to confirm our findings. To determine if unique identifiers were accessible to Bluetooth scanning techniques we monitored for whether any of the following types of identifiers were emitted:

- Static MAC address: the same address is persistently used by the device
- Non-resolvable private MAC address: the address is randomly generated and used as temporary addresses

[24] Version 1.5.4, available in the Google Play Store: `https://play.google.com/store/apps/details?id=com.contextis.android.BLEScanner&hl=en`.

- Resolvable private MAC address: these can be changed often and are cryptographically derived when two devices pair with one another. This mode of (re)generating MAC addresses forms the basis of the Bluetooth Low Energy privacy features that were introduced in version 4.0 and improved in version 4.2 of the Bluetooth protocol.[25]

Publicly-discoverable static MAC addresses enable third parties to track devices persistently, whereas the use of private MAC addresses foils such surveillance. RamBLE was used to ascertain whether fitness wearable devices had implemented the BLE Privacy feature and used resolvable private addresses.

2.2.2 TRANSMISSIONS OVER THE INTERNET

Fitness applications installed on mobile devices often act as proxies to send fitness data onto fitness companies' servers as well as to retrieve data from those servers to display in the application. In some cases, such retrievals may involve the company sending new versions of the operating code, or firmware, to the wearable device itself. Such firmware can modify how long devices operate before needing to be charged, modify or calibrate the accuracy of sensors embedded in fitness devices, or potentially even update the Bluetooth privacy options associated with a fitness device's Bluetooth radio.

PACKETS AND PACKET CAPTURE

To transmit information over the Internet, computers break information up into data packets. Packets are ostensibly routed independently of one another when transmitted to the intended recipient that, upon receiving all of the packets in question, reassembles them. Each packet contains a 'header' and a 'payload'. The header possesses routing information – such as where the packet came from and where it is destined for – whereas the payload holds the actual content of the communication – such as the sensor data collected by a fitness tracker or the firmware code being sent from a company server to the fitness band.

Examining the headers and payloads of packets transmitted to and from fitness devices' associated mobile applications can reveal what data is sent to servers and the extent to which it is protected. In effect, by examining the packets that are sent to and from fitness companies' servers we can determine precisely what information is collected by, and disseminated to, the

[25] Resolvable private addresses have been a part of Bluetooth Low Energy since the original 4.0 specification, and have been improved in version 4.2. See: Bluetooth SIG. Security, Bluetooth Smart (Low Energy), Bluetooth Developer Portal. Retrieved From `https://developer.Bluetooth.org/TechnologyOverview/Pages/LE-Security.aspx`; Andrew Cunningham. (2014). "New Bluetooth 4.2 spec brings IPv6, better privacy, and increased speed [Updated]," Ars Technica, December 3, 2014, retrieved January 20, 2016, `http://arstechnica.com/gadgets/2014/12/new-Bluetooth-4-2-spec-brings-ipv6-better-privacy-and-increased-speed/`.

company: is a fitness device, or its corresponding application, sending contact information, or geolocational information without a user's explicit knowledge, or other information?

To determine what data was sent between the fitness band application and companies' servers we captured the packets that were emitted from the mobile applications. The captures took place on a wireless network we established in a controlled laboratory setting. Only authorized users and devices could connect to the network.

BYPASSING HTTPS

Prior to connecting to our test network we installed a custom certificate on the mobile devices we were monitoring on our test network. This test network was configured to route all wireless traffic through a computer running the mitmproxy software. This software intercepts connections made between one device, such as our mobile phones, and another, such as a fitness company's server.

Specifically, when a device on our network tried to establish a connection with a server on the Internet, mitmproxy intercepted the request and replaced the certificate for the given server with one created automatically by mitmproxy. The certificate provided by mitmproxy was signed by our custom certificate authority. Since our test devices trusted our custom certificate authority, all certificates issued by mitmproxy were in turn trusted by our test devices. This configuration let us conduct a 'man-in-the-middle' attack, or view packets that otherwise would be cryptographically secured as they were transmitted to fitness company servers.

Using Wireshark, we analyzed the captured packets exchanged between fitness company applications and the companies' servers. We specifically used Wireshark to reassemble packets into the source data. Doing so let us identify the IP addresses that each fitness tracking application communicated with, look at the security mechanisms used to the transmission of packets, and peer into the actual payloads of the reassembled communications. We furthermore configured Wireshark to use our custom certificate authority's private key and used temporary session keys collected by mitmproxy to also decrypt encrypted communications.[26]

DATA COLLECTION

We performed a predefined series of tasks on each fitness tracker mobile phone application and observed the resultant HTTP connections. We performed additional tasks particular to each application if the user interface encouraged us to do so, such as inputting food consumption or water intake. We performed the following common tasks:

- Signing up for app

[26] For more information on the development and configuration of our test network, consult: Hilts, Andrew (2015). Snifflab: An environment for testing mobile devices. Open Effect. `https://openeffect.ca/snifflab-an-environment-for-testing-mobile-devices/`.

- Logging out of app
- Logging into app
- Syncing with cloud
- Editing profile
- Editing privacy settings
- Editing other settings
- Sharing / Adding friends
- Pairing device with phone
- Syncing with device
- Logging activities manually

After performing each of the tasks denoted above, we captured packets transferred between the mobile device and company's servers and looked for keywords, key/value pairs, or other structured data.[27] These examinations let us identify the kind(s) of the data being transmitted. In some cases, we explicitly searched through the captured network traffic for particular text strings, such as our test phone's MAC address, International Mobile Subscriber Identity (IMSI) number, and several other identifiers on the basis that they could be used to monitor individuals when sent in an unencrypted format, and because such identifiers and oftentimes used as 'hooks' to aggregate disparate datasets into comprehensive profiles of individuals.[28] We recorded the identified data types in a spreadsheet.

2.2.3 APPLICATION CODE ANALYSIS

We employed reverse engineering techniques on the Android applications in cases where the content of transmissions observed over our wireless network were unclear, or where a mobile application was employing encryption that was not undone using the aforementioned self-signed certificate and mitmproxy software.

When Android programs are compiled their source code is converted into Android bytecode. We used a software tool called apktool to extract the Android packages and disassemble the

[27] To identify these data we used mitmproxy's graphical interface to view explore collected data. This interface lets users interactively explore HTTP transmissions in real time as the data packets traversed from the device through the proxy and to the Internet. While Wireshark let us reconstruct HTTP communications from captured packets the process was generally less user-friendly than working directly at the HTTP level with mitmproxy.

[28] The Citizen Lab (2015). The Many Identifiers in Our Pockets: A primer on mobile privacy and security. Citizen Lab Research Brief. Retrieved: `https://citizenlab.org/2015/05/the-many-identifiers-in-our-pocket-a-primer-on-mobile-privacy-and-security/`.

Android bytecode into smali instructions. Since smali instructions are not easily human readable we also used jadx, an Android bytecode decompiler, to convert the bytecode into higher level Java code on the basis that it is much easier to analyze.

In the case of Basis Peak's Android application we also modified the smali bytecode to remove its use of certificate pinning. Certificate pinning hard-codes the certificates that a piece of software uses to communicate with a server and prevented us from employing mitmproxy to capture unencrypted packets between the mobile device and company's servers. After removing the certificate pinning[29] we used apktool to reassemble the modified application. We were subsequently able to capture packets sent between our modified version of the Basis Peak mobile application and company servers.

2.3 TECHNICAL FINDINGS

We divide our technical findings into three major categories. Please consult Table 3 at the end of this section for a high-level overview.

First, we examined how transmissions were secured between the fitness application and the Internet and found that most applications use HTTPS to encrypt communications. The large exception is the Garmin Connect applications for both Android and iOS, which did not encrypt the transmission of fitness data over the Internet. Garmin Connect only employed HTTPS for account creation and sign on purposes. Withings Health Mate uses HTTPS for most functions save for when a user attempts to share their fitness dashboard with a contact. As a result, important user login session information to Withings' servers is transmitted insecurely.

Second, we examined whether the data being sent from a fitness application to the respective company responsible for the application was susceptible to tampering. We found that Garmin Connect and Withings Health Mate were vulnerable to third parties observing and tampering with fitness data as it was transmitted. In the cases of Jawbone UP and Withings Health Mate, we found that a user could use their own credentials to send false fitness device reports to the companies; these reports were then downloaded to their respective applications and treated as legitimately generated fitness data.

Third, we examined whether fitness devices implemented Bluetooth LE Privacy. This feature randomizes a Bluetooth device's unique MAC address periodically in order to make persistent monitoring of that device more difficult. We found that only the Apple Watch implements Bluetooth LE Privacy; all other devices do not.

[29] More specifically, we modified Basis Peak's code to not pass in a custom "X509TrustManager," an implementation of a Java class that would have otherwise performed certificate pinning.

Device	App	Transmission Security	Data Integrity	Bluetooth surveillance
Apple Watch	Watch	✓ Uses HTTPS; ✓ Certificate Pinning	No test performed	✓ LE Privacy
Basis Peak	Basis Peak 1.14.0	✓ Uses HTTPS; ✓ Certificate Pinning	No test performed	X No LE Privacy
Fitbit Charge HR	Fitbit 2.10	✓ Uses HTTPS	✓ Takes steps to prevent data tampering by user	X No LE Privacy
Garmin Vivosmart	Garmin Connect 2.13.2.1	X No HTTPS besides signup/login	XX MITM can read / write fitness data	X No LE Privacy
Jawbone UP 2	Jawbone UP 4.7.0	✓ Uses HTTPS	X Technically sophisticated user can inject false generated fitness data.	X No LE Privacy
Mio Fuse	Mio GO 2.4.4	✓ No user data sent	✓ No user data sent	X No LE Privacy
Withings Pulse O2	Withings Health Mate 2.09.00	✓ Uses HTTPS; X Security hole (Android)	XX MITM can read / write fitness data (Android). Technically sophisticated user can inject false generated fitness data.	X No LE Privacy
Xiaomi Mi Band	Mi Fit 1.6.122	✓ Uses HTTPS	? Tampered data sent successfully to server, not updated in-app	X No LE Privacy

Table 3: Summary of Technical Findings

Company	Email sent to company	Reminder sent to company	Security contact received	Security report sent	Security team response
Apple	N/A	N/A	N/A	N/A	N/A
Basis	11/26/2015	N/A	11/29/2015	12/1/2015	12/3/2015
Fitbit	11/26/2015	N/A	12/1/2015	12/2/2015	12/16/2015
Garmin	11/26/2015	12/11/2015	–	–	–
Jawbone	11/26/2016	1/15/2016	–	–	–
Mio	11/26/2015	N/A	11/26/2015	11/27/2015	11/27/2015
Withings	11/26/2015	12/11/2015	–	–	–
Xiaomi	11/26/2015	1/20/2016	–	–	–

Table 4: Security vulnerability disclosure timeline by company

2.3.1 NOTIFICATION AND RESPONSIBLE DISCLOSURE

We contacted each fitness tracking company in advance of this report's release. In each case we attempted to inform the respective company about any security vulnerabilities that we discovered in their products. Our goal was to provide companies with a reasonable window within which they could develop fixes for the identified problems. We contacted companies in November 2015, and stated we had security issues to discuss with their security teams. We also informed the comapnies that we intended to publish our findings at the end of January 2016.

Table 4 identifies when we contacted companies and the times of subsequent engagements with them.

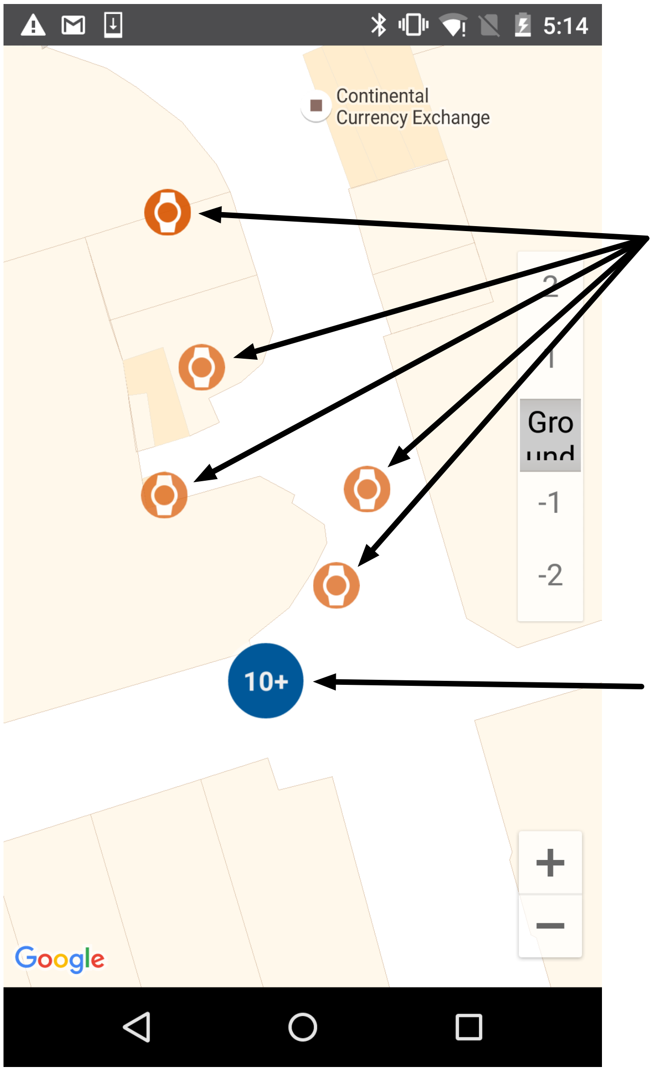
2.3.2 BLUETOOTH PRIVACY

MAC ADDRESS PERSISTENCE

We collected the Bluetooth MAC addresses that our fitness tracking devices broadcast within advertising packets when the devices were not connected to a mobile phone. We monitored our test devices over a period of several months and found the MAC addresses remained fixed in almost all cases. These packets are not sent while the device is paired and connected to a mobile device with the relevant company's associated mobile application. We found that only the Apple Watch randomized the Bluetooth MAC address it uses in Bluetooth advertising packets. Specifically, Apple Watch changes its Bluetooth MAC address when rebooted and at an approximately 10 minute interval.

> Only the Apple Watch randomized the MAC address it uses in Bluetooth advertising packets. It changes its MAC address when rebooted, and at an approximately 10 minute interval.

We performed these tests using the RamBLE Android application. RamBLE records the geographic location at which a device's Bluetooth MAC address is detected by the software. Using this data the application plots those locations on a map to visualize the device's location. More sophisticated tracking software that uses multiple scanners placed in different geographic locations could use such methods to plot a device wearer's movement over space and time. Figure 1 shows how RamBLE plots Bluetooth-enabled devices on a map based on MAC address broadcasts.



Places where the Garmin vivoactive was detected.

10 instances where the vivoactive was detected.

Figure 1: Screenshot from the RamBLE application showing a map of a shopping centre. Icons indicate locations where RamBLE scans detected the presence of a particular Garmin vivoactive fitness wearable over a period of 40 minutes.

ANALYSIS

Fitness trackers that change their Bluetooth MAC address on a regular basis eliminate one way

Device	Test 1	Test 2	Test 3
Apple Watch	46:CF:99:10:D0:DF	51:E5:71:EA:F1:03	7D:D6:E6:18:7D:95
Basis Peak	E6:D0:D6:F8:F2:06	E6:D0:D6:F8:F2:06	E6:D0:D6:F8:F2:06
Fitbit Charge HR	DC:67:77:FA:A5:98	DC:67:77:FA:A5:98	DC:67:77:FA:A5:98
Garmin Vivosmart	E4:D2:5B:2E:EA:2D	E4:D2:5B:2E:EA:2D	E4:D2:5B:2E:EA:2D
Jawbone UP 2	E4:DD:95:B2:DF:AA	E4:DD:95:B2:DF:AA	E4:DD:95:B2:DF:AA
Mio Fuse	D7:FC:11:83:37:FF	D7:FC:11:83:37:FF	D7:FC:11:83:37:FF
Withings Pulse O2	00:24:E4:2F:9D:0F	00:24:E4:2F:9D:0F	00:24:E4:2F:9D:0F
Xiaomi Mi Band	88:0F:10:26:9F:E3	88:0F:10:26:9F:E3	88:0F:10:26:9F:E3

Table 5: Fitness Device Bluetooth MAC addresses. Note changing Apple Watch address.

by which the wearer's presence could be persistently monitored. Most fitness tracking companies do not design their devices to change their MAC addresses.

We disclosed the risks introduced by a fixed MAC address to all companies save Apple (whose Apple Watch device does change its address). Of the companies that engaged with this disclosure, Fitbit and Basis provided notable responses. Fitbit stated it was interested in implementing LE Privacy and that their wearable devices could support it. However, the company asserted that the fragmented Android ecosystem, in which some devices do not support LE Privacy, prevented them from implementing the feature. The security team at Intel (the owners of Basis) stated that the primary use case for the Peak involved the device being continually connected over Bluetooth to the user's phone, and they provided no indication that they intended to fix the emission of a persistent MAC address through advertising packets when the device was not connected to a mobile device.

SIGNIFICANCE

Our findings directly relate to the case of shopping centres that scan for Bluetooth devices to monitor customer journeys as they move from store to store. As an example, a mall visitor wearing a Fitbit Charge HR might have turned off their phone's Bluetooth radio to save power, or forgotten their phone at home or in the car. In either case, the Fitbit device would emit advertising packets detectable by the shopping centre's scanning. Since the Fitbit does not change its MAC address the shopping centre can monitor the presence of the MAC address relative to its scanners and pinpoint the customer's location. The shopping centre could record all this location data for future study. Where the shopping centre is part of a conglomerate of similar venues, or where the scanning system is provided to the mall by a third party, location records derived from Bluetooth scans from a variety of different venues might be stored together to provide an overview of all the places the organization has 'seen' a particular MAC address.

Law enforcement agencies might also be interested in databases holding Bluetooth MAC addresses. In the case of the shopping mall, authorities might request access to a subset, or all of, the retained records. This has the effect of the collection of Bluetooth MAC information being used far in excess of the reason the devices were emitting advertising packets: to pair with a phone, in order for the user to track their fitness behaviours. The shopping centre could also decide to sell its customer data to a marketing agency or other data broker without first notifying customers. These agencies could collate multiple data sets together to weave a portrait about customer movements – all based on this MAC address and other uniquely identifying device identifiers. Few customers are likely to consider, to consent to, these scenarios as they enter shopping centres and begin invisibly broadcasting their location to small sensors throughout their built environment.

2.3.3 TRANSMISSION SECURITY

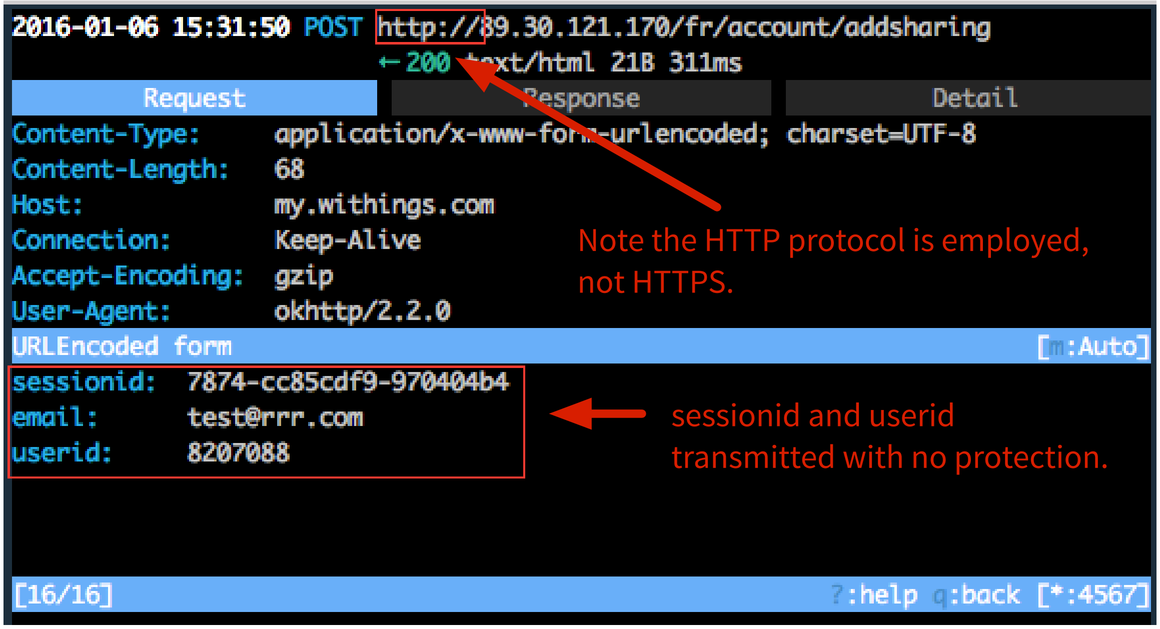
Our research revealed that most fitness devices' mobile applications encrypted their communications with remote servers using HTTPS. Encryption is generally used for signing up, logging in, as well as transmitting fitness and other application data to fitness companies' servers. By adopting HTTPS, fitness device companies are helping to shield consumers from third parties' monitoring or tampering of fitness data exchanged between users' mobile applications and company servers. This security practice was not employed in two notable cases.

GARMIN CONNECT

The Garmin Connect Android and iOS applications do not use HTTPS for routine data transmission, such as fitness event creation notices, downloading daily fitness summaries, and the modification of privacy settings. Consequently all fitness data transmitted using the company's mobile applications can be monitored by a third party that stands between the consumer's mobile device and Garmin's servers; this is referred to conducting a 'man-in-the-middle' (MITM) attack. Garmin's fitness data transmissions typically include the end user's userid in the transmission payload, which makes it very simple to identify and profile the captured data. The only instance where we observed HTTPS being employed by Garmin Connect was during the account creation and user login and log out processes. Securing the login and log out processes helps protect accounts from being fully taken over (i.e by stealing passwords) but does not help against surveillance of routine fitness data transmissions.

WITHINGS HEALTH MATE

The Withings Health Mate Android application generally employs HTTPS and the Health Mate iPhone application appears to use it consistently. However, HTTPS is not used for the Android version's "Share my dashboard" feature. This feature lets the user input a friend's email address with whom to share the user's fitness activity. When the user submits the email address to Withings the resulting plaintext HTTP request includes the application's sessionid and userid. As a result, an unauthorized third party (i.e a MITM attacker) can collect the userid and sessionid. These identifiers can subsequently be used to make new requests to Withings for access to that user's data. While the sessionid seems to expire after an interval of approximately 15 minutes an attacker with knowledge of Withings API could download a wide variety of fitness information about that particular user within the time period.[30] Figure 2 provides visual confirmation that we could identify the sessionid and userid in plaintext communications between the mobile device and Withings' servers.



```
2016-01-06 15:31:50 POST http://89.30.121.170/fr/account/addsharing
                         ← 200 text/html 21B 311ms
        Request              Response              Detail
Content-Type:      application/x-www-form-urlencoded; charset=UTF-8
Content-Length:    68
Host:              my.withings.com
Connection:        Keep-Alive
Accept-Encoding:   gzip
User-Agent:        okhttp/2.2.0
URLEncoded form                                              [m:Auto]
sessionid:   7874-cc85cdf9-970404b4
email:       test@rrr.com
userid:      8207088



[16/16]                                    ?:help q:back [*:4567]
```

Note the HTTP protocol is employed, not HTTPS.

sessionid and userid transmitted with no protection.

Figure 2: Screenshot from mitmproxy showing an intercepted plaintext HTTP request originating from the Withings Health Mate Android application that contains the sessionid and userid (as well as a contact's email address).

SIGNIFICANCE

Employing encryption to prevent eavesdroppers from collecting and tampering with other people's data is a basic technical security mechanism for protecting the transmission of personal information. That Garmin Connect failed to employ the basic safeguard of HTTPS means that all of the app's transmissions of sensitive data about the fitness habits of its users are, at the time of writing, vulnerable to third party surveillance or modification. The vulnerability in the Withings Health Mate Android application exposes its users to similar risk. The difference between the two vulnerabilities is that while Garmin data can be passively collected by someone controlling the network, an attacker must wait for the particular HTTP request discussed above to exploit the Withings Health Mate Android application. Only once the attacker received the aforementioned request could they exploit the vulnerability.

[30] We suspect that this deficiency is an accidental programming error as opposed to a deliberate decision to not secure all data transmissions.

Neither Garmin nor Withings responded to our attempts to contact their security teams about these issues.

> All of Garmin Connect's transmissions of sensitive data about the fitness habits of its users are, at the time of writing, vulnerable to third party surveillance or modification.

2.3.4 DATA INTEGRITY

The data sent by fitness tracking applications over the Internet can fall into two general categories:

- **Manual fitness data** is created by the user through the user interface of the mobile application. This can involve inputting data related to setting goals, logging diet, and logging mood. Three fitness applications are susceptible to spoofed manual data being accepted by fitness tracker servers and presented in the mobile application interface as fitness events that a user themself had input.
- **Generated fitness data** is sent immediately following the user syncing their fitness device with the application. Generated fitness data is a structured format that usually describes how many steps were taken, how much sleep occurred, or how many stairs were climbed, and typically within a series of time intervals (e.g. per minute, per hour, or per day). There is no user interface to create this data in the application. Instead, the data is treated as though it originated from the fitness tracker itself. Two applications are vulnerable to generated fitness data being accepted by fitness tracker servers and presented in the mobile application interface as legitimate fitness events.

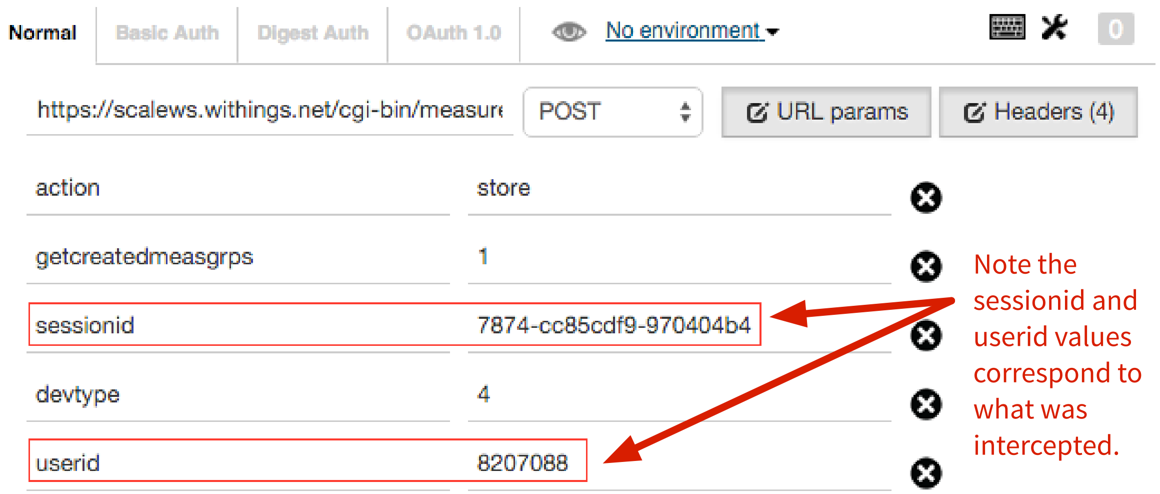
We distinguish between manual fitness data and generated fitness data because the data generated by the wearable are the product of continual and passive measurements, as opposed to the end user self-reporting manual fitness entries.

DATA TAMPERING BY A "MAN-IN-THE-MIDDLE"

Garmin Connect does not use HTTPS for most application functions. In addition to not using transport security the application uses OAuth 1.0 for user server request authentication. OAuth 1.0 verifies that requests originate from an authorized user by generating a cryptographic signature that combines a secret key and a request base string that combines the destination Uniform Resource Locator (URL) with some other metadata about the request. OAuth 1.0 does not verify the actual data contained in HTTP POST requests; such requests are typically used for uploading data to a server over the Internet.[31]

In practice, Garmin's decision to use OAuth 1.0 without HTTPS for its mobile applications enables third parties to collect user requests and subsequently modify them. Such modifications let third parties inject false fitness data or even delete fitness events from a user's profile. It would also be possible for this third party to alter a user's privacy settings, stated gender, or other profile information.

As described above, Withings' Android Health Mate application includes a function that makes an unencrypted HTTP request. In the process of making these requests the user session credentials are exposed to third parties who can intercept the data traffic between the mobile application and Withings' servers. An attacker with knowledge of Withings Application Programming Interface (API) could utilize this request to create false manual fitness data that is recognized, processed, and incorporated into fitness statistics by Withings servers and the Health Mate application, as demonstrated in Figures 3, 4, 5, and 6.



https://scalews.withings.net/cgi-bin/measure POST

action	store
getcreatedmeasgrps	1
sessionid	7874-cc85cdf9-970404b4
devtype	4
userid	8207088

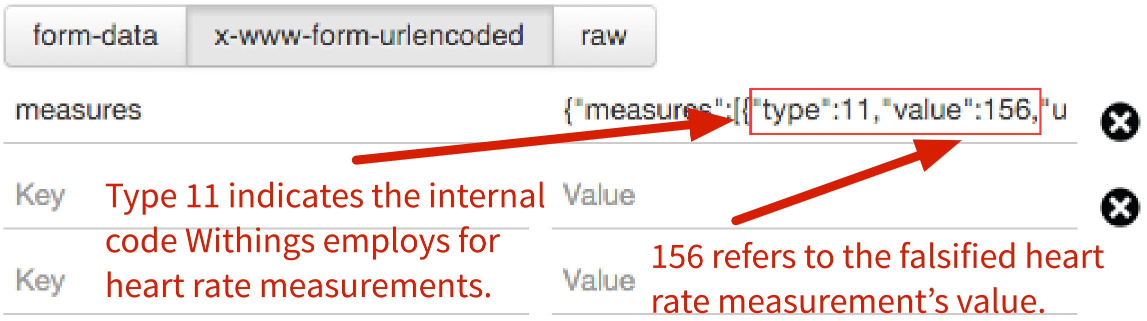
Note the sessionid and userid values correspond to what was intercepted.

Figure 3: Attacker using intercepted Withings Health Mate user's sessionid and userid values in a preconstructed request to create new fitness data.

FITNESS BAND TAMPERING BY THE USER

The Jawbone UP and Withings Health Mate fitness data transmissions we observed between the mobile application and respective companies' servers were generally secured using HTTPS. However, the applications (for both Android and iOS) were vulnerable to a motivated user creating false generated fitness data for their own account, effectively tricking servers that the fake

[31] The OAuth 1.0 specification notes that HTTP request components that are excluded from the signature base string cannot be verified without the use of transport-layer security. Since, in Garmin's case, the POST data is excluded from server verification a third party can tamper with the data. See: `http://tools.ietf.org/html/rfc5849`.

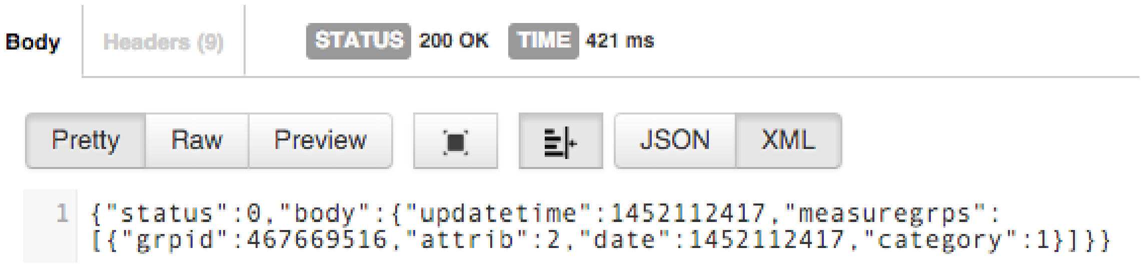


measures {"measures":[{"type":11,"value":156,"u

Type 11 indicates the internal code Withings employs for heart rate measurements.

156 refers to the falsified heart rate measurement's value.

Figure 4: Inputting false heart rate data into a form to send to Withings. "Type: 11" refers to the fitness event type, in this case a heart rate measurement. "Value: 156" refers to the value of the falsified heart rate measurement.



STATUS 200 OK TIME 421 ms

```
{"status":0,"body":{"updatetime":1452112417,"measuregrps":
[{"grpid":467669516,"attrib":2,"date":1452112417,"category":1}]}}
```

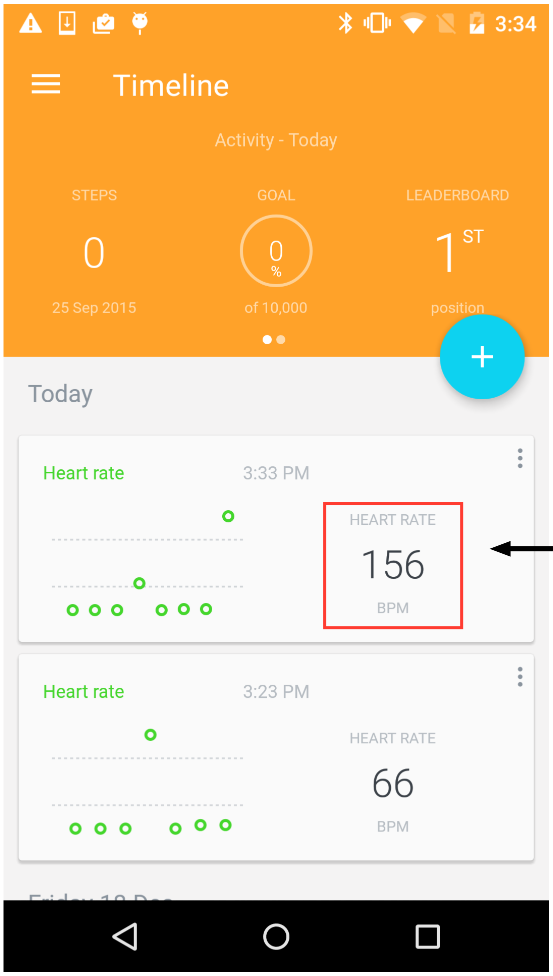
Figure 5: The Withings server responding to the HTTP request containing a falsified heart rate measurement. "Status: 0" indicates the server accepted the data. Other information present include the time at which the server accepted the request and the time associated with the heart rate measurement.

data originated from the Jawbone or Withings fitness wearables. HTTPS only secures the communications channel between user and server; it does not offer protection from end users abusing a service.

We created proof-of-concept applications that tricked Jawbone and Withings servers into accepting false fitness band information. As an extreme example, we sent a request to Jawbone stating that our test user took ten billion steps in a single day, shown in Figure 7. This request was accepted by the server and displayed as normal in the Jawbone application. Our proof of concept application evenly distributes the desired step count into fixed intervals within the desired timeframe and this causes the resulting step graph to appear to be noticeably artificial, as shown in Figure 8. A more sophisticated approach would randomly allocate steps to establish a more realistic-looking distribution.

> We sent a request to Jawbone stating that our test user took ten billion steps in a single day.

Neither Jawbone nor Withings responded to our attempts to contact their security teams about these issues.



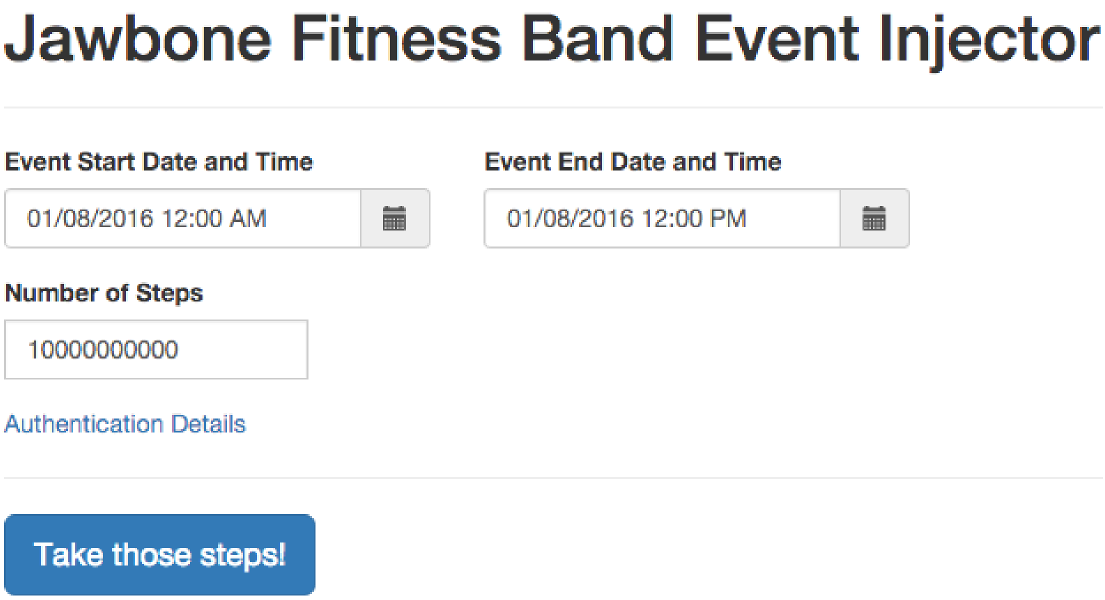
Note the heart rate value displayed in the app corresponds to the value sent to the Withings server.

Figure 6: The false heart rate data appearing in the user's Withings Health Mate application.

MEASURES TO HINDER GENERATED FITNESS DATA TAMPERING

We found that Fitbit takes steps to prevent generated fitness data tampering by encrypting its generated fitness data on the Fitbit Charge HR wearable itself, and then routing that encrypted data through the company's mobile application to Fitbit's servers. The servers then presumably decrypt the data into a structured format and store it. The Fitbit mobile application then downloads the data from the server for display. In this model, Fitbit's servers and the device hold the authority over the integrity of the band's data; the application is not trusted.

Encryption was performed by software on the Charge HR, and as a result we could not determine exactly how data transmissions are encrypted. However, we analyzed 22 Bluetooth transmissions generated by the device and found some consistencies. Each transmission includes a 16-byte header containing the wearable's 6-byte serial number followed by what is likely an encrypted payload. The bytes in the encrypted payload are uniformly distributed at random. Moreover, the number of bytes is always divisible by 8 but not necessarily by 16, suggesting encryption with an 8-byte block cipher such as DES or Blowfish. The encrypted payload is fol-



Jawbone Fitness Band Event Injector

Event Start Date and Time
01/08/2016 12:00 AM

Event End Date and Time
01/08/2016 12:00 PM

Number of Steps
10000000000

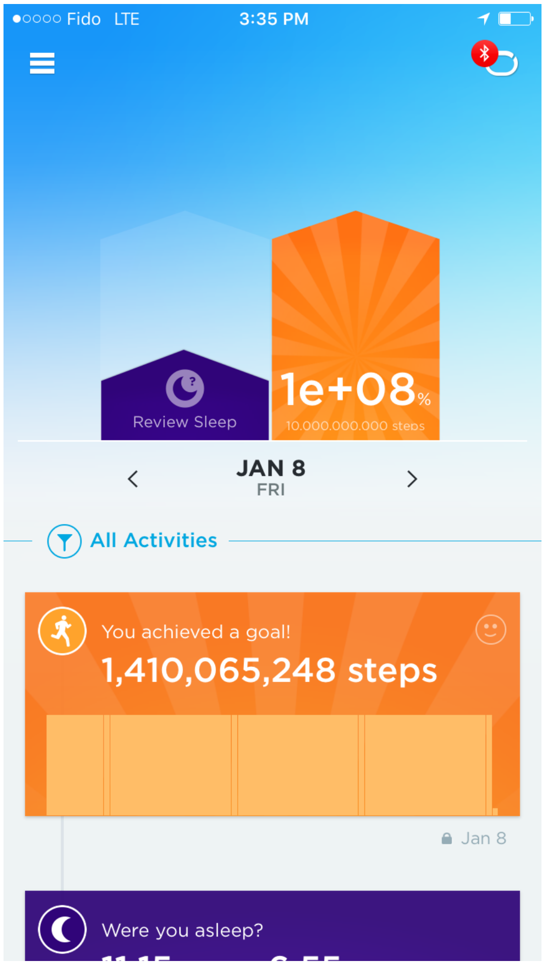
Figure 7: Screenshot of proof-of-concept application to feed false generated fitness data to Jawbone.

lowed by a two-byte value and a zero byte. The two-byte value may refer to the length of the unencrypted transmission, as the value was always observed to be between 22 and 32 less than the number of bytes of the encrypted payload.

Since other devices we analyzed did not perform end-to-end encryption from the device to the server, they were vulnerable to data tampering. In order to create our fake Jawbone and Withings generated fitness data we established a proxy server that replaced the respective company's fitness device's server's encryption with our own. We used this vantage point to understand the structure of Jawbone and Withings generated fitness data formats, and study the URLs, authentication details, and HTTP headers required to create a successful request to the companies' servers.

We could study the fitness applications in this manner because the applications accepted the security certificates issued by the proxy and signed by a certificate authority we had added to our test mobile phones (as described in Section 2.2.2). To analyze Basis Peak's traffic we had to remove the application's certificate pinning functionality.

Certificate pinning involves an application relying on its own set of trusted certificates when communicating with other servers using transport layer encryption (i.e. TLS). By using its own set of certificates the application does not inherently trust certificates identified as being legitimate by the device operating system. Therefore, if a third party installs additional certificate authorities (which we did for our tests) and attempts to modify communications issued by the application to use their own certificate the application will flag that communication as untrusted and cease processing the HTTP request. However, to analyze the application's traffic



You achieved a goal!

1,410,065,248 steps

Were you asleep?

Figure 8: Jawbone UP application accepting falsified generated fitness data from our application. Note the uniformly distributed time-series graph.

we successfully circumvented certificate pinning in the Basis Peak Android application by removing the certificate pinning code from our reverse engineered application and reassembling the application (as discussed in Section 2.2.2).

ANALYSIS

Our ability to successfully issue falsified requests to Jawbone and Withings calls into question the integrity of generated fitness data for these two companies. These companies do not seem to use mechanisms to verify that generated fitness data originates from the wearable devices themselves. We must note that we crafted generated fitness data exploits for Jawbone and Withings because of the relatively simple data formats that each company used for their generated fitness data. It is possible that, with additional time and resources, equivalent vulnerabilities might be found in other companies' applications.

SIGNIFICANCE

These findings concerning fitness tracker data integrity could call into question several real-world uses of fitness data. Fitess tracking data has been introduced as evidence in court cases, as discussed in Section 1.4, meaning that at least some attorneys are relying upon generated fitness data as a possibly objective indicator of a person's activities at a given point in time. For Jawbone and Withings we created fraudulent fitness data which indicated that a passive measuring device, the fitness device, recorded a person taking steps at a specific time when no such steps occurred. For this reason we believe that the provenance of fitness tracking data needs to be carefully assessed when utilizing the data for non-personal fitness tracking purposes, such as when the data is introduced in courts or used to increase or reduce a person's insurance premiums.

2.4 CONCLUSION

In the course of our technical investigations into transmission security, data integrity, and Bluetooth privacy, we discovered several issues that confirm concerns about the potential uses of fitness tracking data beyond the typical case of a user monitoring their own personal wellness.

The unique identifiers broadcast by all studied devices except for the Apple watch are fixed. These static identifiers enable third parties, such as shopping malls, to persistently monitor where fitness wearables are located at a given point in time. These findings confirm concerns described in Section 1.4 relating to the privacy of Bluetooth emissions and geolocating fitness trackers more generally.

Garmin Connect's lack of HTTPS encryption exposes its customers to the risk that their sensitive fitness data is being collected or tampered by unauthorized third parties, as does a security vulnerability in the Withings Health Mate application. Our findings confirm concerns described in Section 1.4 about the potential for unknown parties to access fitness data.

Finally, the fitness data generated by several wearable devices can be falsified by motivated parties, calling into question the degree to which this data should be relied upon for insurance or legal purposes. This confirms the concerns described in Section 1.4 that people could fraudulently input device data are grounded in reality.

3 POLICY FINDINGS

[Forthcoming]

4 PIPEDA FINDINGS

[Forthcoming]

5 DATA EXPECTATIONS VERSUS REALITY

[Forthcoming]

6 RECOMMENDATIONS AND BEST PRACTICES

[Forthcoming]

7 CONCLUSION

[Forthcoming]