OPEN EFFECT

Every Step You Fake

A Comparative Analysis of Fitness Tracker Privacy and Security

[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.

Document Version: 1.5

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

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.

ABOUT THIS VERSION

April 18, 2016: This report has been updated with factual corrections and clarifications raised in recent communication from Fitbit.

RECOMMENDED CITATION

Andrew Hilts, Christopher Parsons, and Jeffrey Knockel, *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security*. Open Effect Report (2016). Available at: `https://openeffect.ca/reports/Every_Step_You_Fake.pdf`.

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 HTTPS among websites and advertising trackers 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

PREFACE

Consumers are bombarded with advertisements for products that will enhance, extend, or enable a healthier life. One class of health product is fitness wearables, usually small bands that are worn on the wrist and collect a range of data to help visualize how (in)active a person is in their daily life. This is a booming industry, with millions of the devices sold each year.

Given the number of these devices that are in use, we asked: is the data on these devices secured from misuse by third parties? What data are being collected and transmitted back to fitness companies? And how transparent is this data collection when individuals examine companies' privacy policies and terms of service documents, or file requests for access to all the data a company has collected about the user and their activities?

Over the past year we have conducted in-depth technical and policy research to respond to these questions. And quite often the results have been troubling: basic technical safeguards have sometimes been improperly established, or not established at all. In other situations it became apparent that users' concerns about their data being sold or made available to third parties are entirely warranted. And quite often the information accessible by individuals who request their personal information varies from the data actually collected by the companies in question.

These results call into question the very nature of self-empowerment that is marketed alongside fitness trackers. Can individuals be truly empowered when their data is not secured? When their data might be sold off without the individual's consent? When they cannot even learn about all the data a company has collected?

While we believe this represents the most comprehensive attempt to determine fitness companies' technical, policy, and legal processes for collecting and disclosing data, the results should not be read as 'Canadian' or even necessarily about just fitness tracking companies. Instead, they showcase how increasingly globalized companies dictate what jurisdictions they will accept complaints from, how technical collection systems are obfuscated by often ambiguous policy language, and the difficulties in exercising binding national law on foreign companies.

These problems, obviously, pertain to certain fitness tracking companies. But the problems are not bound to this industry segment: past research has shown similar difficulties concerning social media companies, and other efforts have showcased how challenging it is to determine what telecommunications companies are doing to collect, process, retain, and disclose customer data. As such, this research should be seen as unpacking some of the practices of the fitness tracker industry but, more broadly, as showcasing the state of contemporary data handling practices in consumer products and services. Citizens, regulators, and politicians alike must actively investigate how data collecting-companies are treating customer data, and where inappropriate activities are identified, regulators and politicians alike must actively seek to prevent such data mishandling.

We hope that this report will outline some of the contemporary data handling issues in this industry segment and offer regulators both a methodology to test other industry categories while also offering sufficient empirical data to let them discuss contemporary practices that members of the fitness tracking industry are engaged in, today. We further hope that the fitness tracking industry and other "internet of things" companies in general, adopt our recommendations in order to strengthen the data protection they offer to consumers.

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. Best-of-class trackers capture the number of floors, or altitudinal changes, a person climbs a day, levels and deepness of sleep, and heart rate activity. 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:

- Are 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

[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.

personal data captured by fitness trackers and their companion mobile applications. Canadians 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. 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. Transparency concerning how these bands operate, and the levels of privacy assured to consumers, is increasingly 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 discuss our observations of the types of personal information transmitted by these devices, multiple security vulnerabilities we discovered, and these findings' relative significance for fitness tracker users.
- **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 these analyses.
- **Section 4** begins by discussing the methods we employed 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 that companies are collecting from their fitness wearables corresponds 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. It also suggests some actions the Office of the Privacy Commissioner of Canada might consider to better guide fitness wearable companies.
- **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 3 of

Fitness wearables 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

this report.

[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, retrieved 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
Bellabeat	Bellabeat LEAF	LEAF 1.7.0
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 several 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. Third, we included the Bellabeat LEAF due to its focus on women's health issues, whereas all other wearable devices omitted women's health features such as menstrual cycle tracking. Table 2 identifies the specific companies and products examined.

[13] Endeavour Partners. (2014). "Inside wearables: How the science of human behaviour 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.

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 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] This data, if it can be manipulated, brings its use as evidence as well as its broader trustworthiness, into question. Corporate wellness programs[17], and insurance firms[18] 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,[19] and have previously been conducted en masse without

[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] Programs in which individuals or workplaces provide some fitness related information to their employers and / or wellness firms

[18] See, for example: Evans, P. (2016). Manulife to offer Canadians discounts for healthy activities. CBC News. Feb 9, 2016. Retrieved from http://www.cbc.ca/news/business/manulife-fitness-insurance-1.3439904.

[19] 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/.

research subjects ever realizing their movements were being followed.[20]

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 disclosed. 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. 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 the rights companies afford to themselves in more depth in Section 3.

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.[21] 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."[22] Though the same authors avoid engaging in a detailed analysis of how Canadian commercial privacy legislation[23] 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."[24] Even without specific guidance on what wearable companies must do to remain compliant with Canadian law, companies can still examine guidance concerning the application of

[20] 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.

[21] 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

[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] As expressed in the Personal Information and Protection of Electronic Documents Act (PIPEDA)

[24] 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.

PIPEDA to develop lawful practices concerning the collection, processing, retention, and dissemination of fitness-related information.

Europe, in contrast to both 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)."[25] Given that many fitness companies provide health-related 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 companion 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.

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.

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

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 access 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, 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 the Internet, over Bluetooth radios that are embedded in the wearables, 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 summaries 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 employed several different types of devices for our research including smartphones, a laptop, wireless router, and of course, fitness wearables. 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 laptop and test iPhone 6 directly from Apple, and a Google Nexus 5 from Amazon.ca.

2.2 TECHNICAL METHODOLOGY

We used several technical research methods to identify the data that fitness trackers transmit to mobile applications, that mobile applications sent to and received 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 Internet-based transmissions, then the extent to which mobile device applications are developed to secure and maintain the integrity of individuals' fitness data, and finally, Bluetooth transmissions.

2.2.1 TRANSMISSIONS OVER THE INTERNET

Fitness applications installed on mobile devices often act as proxies to send fitness data to 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 designed to be 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 the data 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 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 secured 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 the 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
- 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

[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/`.

- 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.

2.2.2 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 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.

[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 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/`.

[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.

2.2.3 TRANSMISSIONS OVER BLUETOOTH

Fitness bands routinely communicate with mobile device applications using the Bluetooth Low Energy (BLE) 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 used RamBLE[30] to monitor how and whether, unique identifiers such as MAC address of wearables were accessible. 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

[30] 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.[31]

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

2.3 DATA TRANSMISSIONS

The fitness tracking applications that we examined transmitted five major categories of data to remote servers over the Internet, summarized in Table **??**. Those categories include: basic personal information, fitness information, location information, social information, and device identifiers. The types of basic personal information that were transmitted were relatively consistent across applications, while the other categories exhibited more variance and were largely dependent on the specific features of the devices and applications.

This inventory of data types is not necessarily exhaustive or complete. We identified these types by capturing and analyzing data transmissions that occurred as we ran a structured series of activities for each application, as described in our methodology, as well as by opportunistically identifying other data types that were sent over the course of our research.

We could not observe the data transmitted by the BASIS Peak iPhone application because the application used HTTPS certificate pinning[32]. We were, however, able to monitor the BASIS Android application. We also could not analyze the data transmitted by the Apple Watch using our methodology, though we did not observe any HTTP requests emitting from the app during our standard tests.

[31] 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/`.

[32] 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 thought to be legitimate by the device operating system.

Data type	Basis	Bellabeat	Fitbit	Garmin	Jawbone	Withings	Xiaomi
Name / DOB / Gender / Heigh / Weight / Email							
Friends' email address(es)		X		X			X
Geolocation	*	X	*	X			X
Phone serial number		X	X	X	X	X	X
IMEI Number	X	X	X	X	X	X	
Wearable MAC address					X		
Steps per time interval and/or heart rate over time	*		*				
Manual activities and/or measurements	X	X					X
Food intake	X	X				X	X
Reproductive health info	X		X	X	X	X	X

Table 3: Sensitive Data Transmissions. For items marked with a "*", we did not directly observe this data being transmitted, as the application encrypted and/or encoded its payloads. However, the user interfaces updated to display the data type following HTTP transmissions.

2.3.1 BASIC PERSONAL INFORMATION

We define basic personal information as that which is distinctly linked with a specific identifiable person; this includes biographical details, name, and communications identifiers. Such information that is transmitted by fitness tracking applications include: name, email address, password, gender, date of birth, height, weight, username, and contacts' email addresses. This information is typically transmitted during the following tasks: Initial registration, log in, share / add friends.

All applications save the Apple Watch ask for the user's name. All but the Mio GO application send this information over the Internet. In fact, the Mio GO applications that we tested do not appear to send any data over the Internet whatsoever – even though there is a required registration form and a user agreement that the user must accept.

2.3.2 FITNESS INFORMATION

We observed two major categories of fitness data transmitted to service providers by their mobile applications. Data collected automatically by the device itself ("fitness band data"), and data manually entered by the user into the application ("manual fitness information").

GENERATED FITNESS DATA

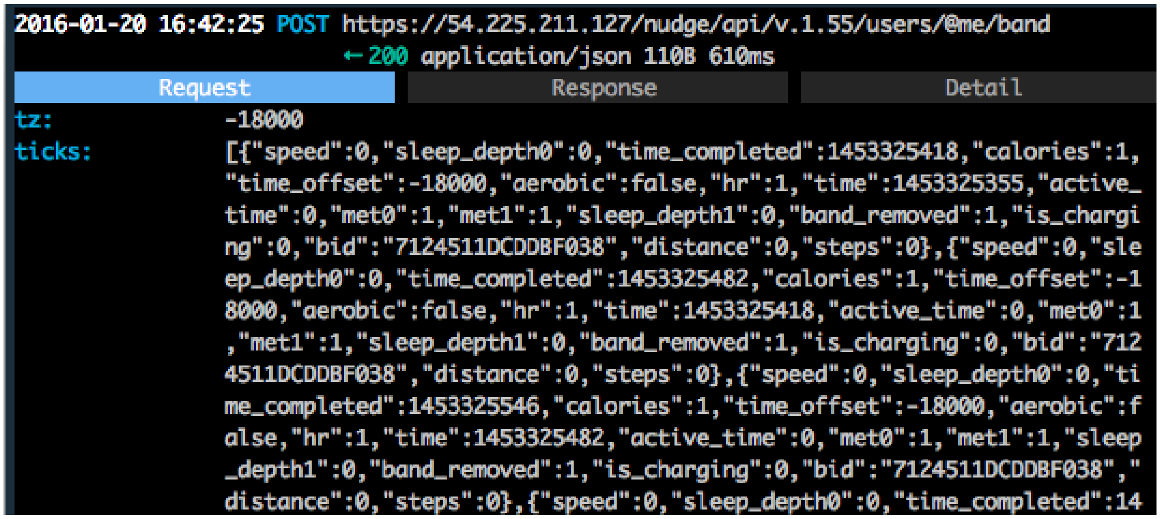
We observed fitness band data transmissions that included steps taken, stairs climbed, stairs down, calories burned, speed, sleep depth, whether or not activity can be classified as aerobic, heart rate, and blood pressure. This data is usually represented as numbers and organized in time series format, to indicate the amount of each data type that was performed in a given time interval (minutes, hours, days).

We could not observe the precise data being sent over the network for Garmin, BASIS, Fitbit, and Apple Watch because they used proprietary encoding and/or encryption to format band data. We did not have the resources to attempt to reverse engineer these formats.

MANUAL FITNESS DATA

Fitness tracking applications provide their users with a wide range of data types for manual input. These can range from reporting current mood, logging weight, or food intake (which is often linked to nutritional information, as is the case with Jawbone and Fitbit). Many applications support setting fitness goals (number of steps, amount of sleep, number of calories burned).

Many applications let users manually log fitness activities, either writing in a description or choosing from a list of options, entering duration, distance. LEAF users can input data such as



```
2016-01-20 16:42:25 POST https://54.225.211.127/nudge/api/v.1.55/users/@me/band
                          ←200 application/json 110B 610ms
tz:            -18000
ticks:         [{"speed":0,"sleep_depth0":0,"time_completed":1453325418,"calories":1,
               "time_offset":-18000,"aerobic":false,"hr":1,"time":1453325355,"active_
               time":0,"met0":1,"met1":1,"sleep_depth1":0,"band_removed":1,"is_chargi
               ng":0,"bid":"7124511DCDDBF038","distance":0,"steps":0},{"speed":0,"sle
               ep_depth0":0,"time_completed":1453325482,"calories":1,"time_offset":-1
               8000,"aerobic":false,"hr":1,"time":1453325418,"active_time":0,"met0":1
               ,"met1":1,"sleep_depth1":0,"band_removed":1,"is_charging":0,"bid":"712
               4511DCDDBF038","distance":0,"steps":0},{"speed":0,"sleep_depth0":0,"ti
               me_completed":1453325546,"calories":1,"time_offset":-18000,"aerobic":f
               alse,"hr":1,"time":1453325482,"active_time":0,"met0":1,"met1":1,"sleep
               _depth1":0,"band_removed":1,"is_charging":0,"bid":"7124511DCDDBF038","
               distance":0,"steps":0},{"speed":0,"sleep_depth0":0,"time_completed":14
```

Figure 1: Screenshot from mitmproxy showing fitness band data sent to Jawbone's servers. Indicates steps/movement per time interval.

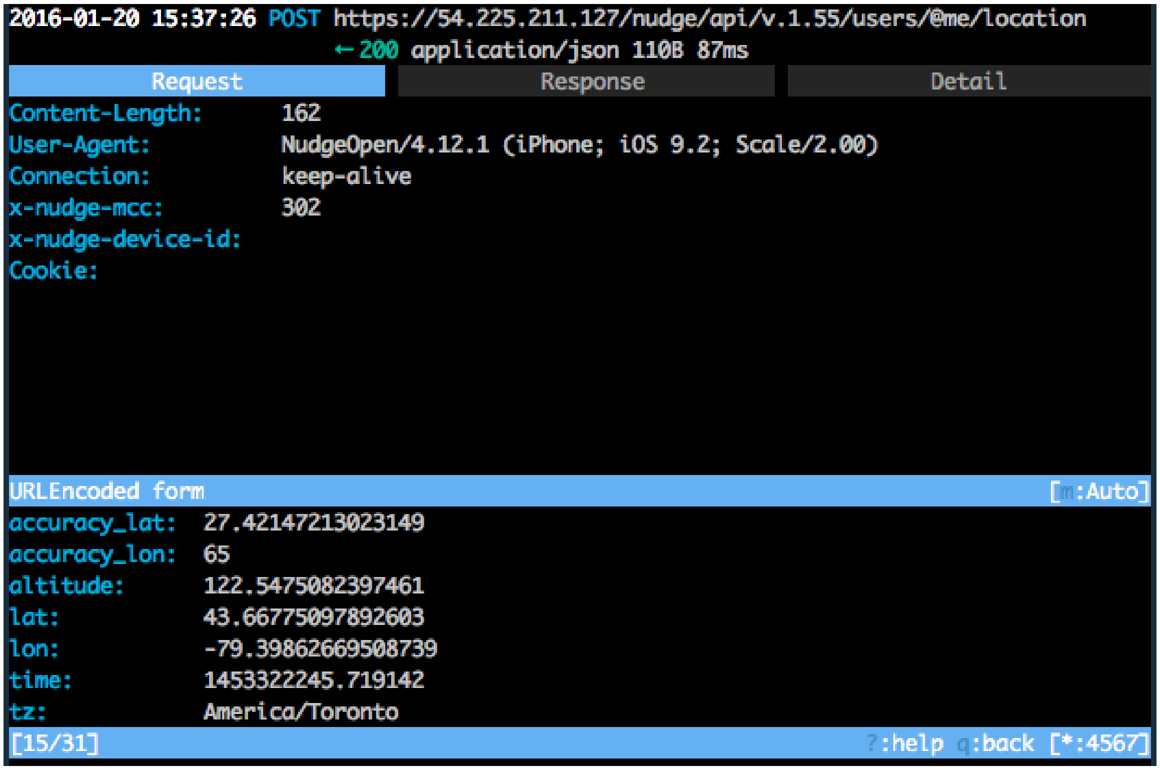
pregnancy status, menstrual cycle duration, and records of conducting breathing exercises. Xiaomi and Mio GO users cannot create manual fitness data. In some cases the server will respond with the estimated number of calories burned during the logged activity after this data is sent to the server.

2.3.3 GEOLOCATION

Several fitness tracking applications transmit location information over the Internet. Some, like Fitbit and Basis, transmit it while the end user is actively using or has recently used custom workout mapping features. However, we found that Jawbone and Withings applications both passively sent the users' current location during routine use of the application. The actions of these applications were surprising given that the collection of this information was not linked with a given fitness activity; we remain unclear why this degree of passive location tracking is implemented by these applications.

Jawbone periodically transmits longitude and latitude to its servers while users have the mobile application open; these transmissions are correlated with predefined user events, such as opening the application or syncing with a device. This geolocation information has a precision of up to 14 decimal points; this effectively discloses the mobile devices' location to within a few millimetres.

Withings Health Mate similarly transmits location information when the user refreshes his or her timeline. In both cases of Withings and Jawbone, the application does not directly notify the user that location transmissions are occurring, nor does the user interface even suggest that location information is related to the task being performed.



```
2016-01-20 15:37:26 POST https://54.225.211.127/nudge/api/v.1.55/users/@me/location
                         ← 200 application/json 110B 87ms
        Request                    Response                    Detail
Content-Length:       162
User-Agent:           NudgeOpen/4.12.1 (iPhone; iOS 9.2; Scale/2.00)
Connection:           keep-alive
x-nudge-mcc:          302
x-nudge-device-id:
Cookie:








URLEncoded form                                                    [m:Auto]
accuracy_lat:  27.42147213023149
accuracy_lon:  65
altitude:      122.5475082397461
lat:           43.66775097892603
lon:           -79.39862669508739
time:          1453322245.719142
tz:            America/Toronto
[15/31]                                       ?:help q:back [*:4567]
```

Figure 2: Jawbone UP iPhone application sending precise location when the user opens up the application. Authentication details have been redacted from the screenshot.

> Jawbone routinely transmits precise geolocation information —down to millimetres —when the user does simple tasks like opening the app, or syncing their wearable to their phone.

2.3.4 SOCIAL INFORMATION

All applications other than Mio, Apple, Basis, and Xiaomi included social features that rely on users adding their contacts. Of those, all applications other than Garmin Connect and Withings Health Mate request access to a user's contacts in order to suggest friends to add. These applications send a full list of contact email addresses over the Internet to the fitness tracking companies' respective servers, and return a list of contacts using the same fitness tracking service. Garmin, by contrast, simply lets users search for others using an in-app form. Withings lets users share some basic fitness statistics with friends whose email addresses must be manually inputted. When users connect with others who are also using the fitness tracking companies' social tools they usually can then share a subset of fitness information for comparative or competitive purposes.

2.3.5 DEVICE IDENTIFIERS

Mobile phones and wearable fitness devices have serial numbers, network radio addresses (MAC addresses), and a variety of other unique identifiers that let them communicate with other devices or otherwise be identified.

The most common unique identifier that was sent over the Internet by fitness tracker mobile applications was the Bluetooth Media Access Control (MAC) address of the fitness tracking band that was paired with the mobile phone. Fitbit, Withings, Bellabeat, and Xiaomi transmitted this information to their cloud services. Jawbone transmitted a unique number to servers when syncing data from the band with the app. We speculate that this since this identifier is referred to as a "bid" it could serve as an internally-used "band identifier" for Jawbone's fitness wearable.

One application, BASIS Peak, transmitted the serial number of the mobile phone itself to BASIS' servers. The Android version of Xiaomi's Mi Health application transmitted our test phone's International Mobile Equipment Identifier number, which is a serial number that is permanently attached to the mobile device, as opposed to the Subscriber Identity Module (SIM) that was inserted into the phone.

2.3.6 SUMMARY

Of the fitness tracking applications for which we could inspect their data transmissions, only the Mio Fuse did not transmit user fitness data to company servers. All fitness tracking applications, save for the Mio Fuse and perhaps the Apple Watch, transmit every logged fitness event over the Internet. These transmissions both enable data backup and facilitate data sharing between friends, though these transmissions also enable data analytics or sharing of personal and health data by the fitness tracking company itself.

In some cases, however, it was unclear why certain data transmissions were occurring. The transfer of the mobile phone serial number to Basis, the IMEI number to Xiaomi, and the unexpected routine transmissions of fine-grained location data to Jawbone and Withings, were all examples of transmissions of sensitive information that did not appear necessary, or at the very least, for which the user is poorly notified.

2.4 SECURITY AND PRIVACY ISSUES OVERVIEW

We now describe three categories of security and privacy issues that we explored during our research. First, we look at Bluetooth privacy, specifically at the metadata transmissions that leak out of fitness trackers. Next, we focus on transmission security, specifically at whether or not personal data is encrypted when transmitted over the Internet in order to protect confidentiality. Finally, we examine data integrity, which focuses on whether or not fitness data can be thought of as authentic records of activity that have not been tampered with.

Our results for each studied application are summarized in Table 4. When we identified security and privacy issues, we followed a responsible disclosure process and attempted to notify the security teams of affected companies in a secure manner prior to the publication of our results. The timelines associated with our communications with various companies is summarized in Table 5.

2.4.1 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 most contacted companies in November 2015, and stated we had security issues to discuss with their security teams. We also informed the companies that we intended to publish our findings at the end of January 2016.

Table 5 identifies when we contacted companies and the times of subsequent engagements with them.

2.5 BLUETOOTH PRIVACY

2.5.1 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

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 4: Technical security and privacy issues in fitness trackers

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 5: Security vulnerability disclosure timeline by company

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

sophisticated tracking software that uses multiple scanners placed in different geographic locations could use such methods to more precisely plot a device wearer's movement over space and time. Figure 3 shows how RamBLE plots Bluetooth-enabled devices on a map based on MAC address broadcasts.

2.5.2 ANALYSIS

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

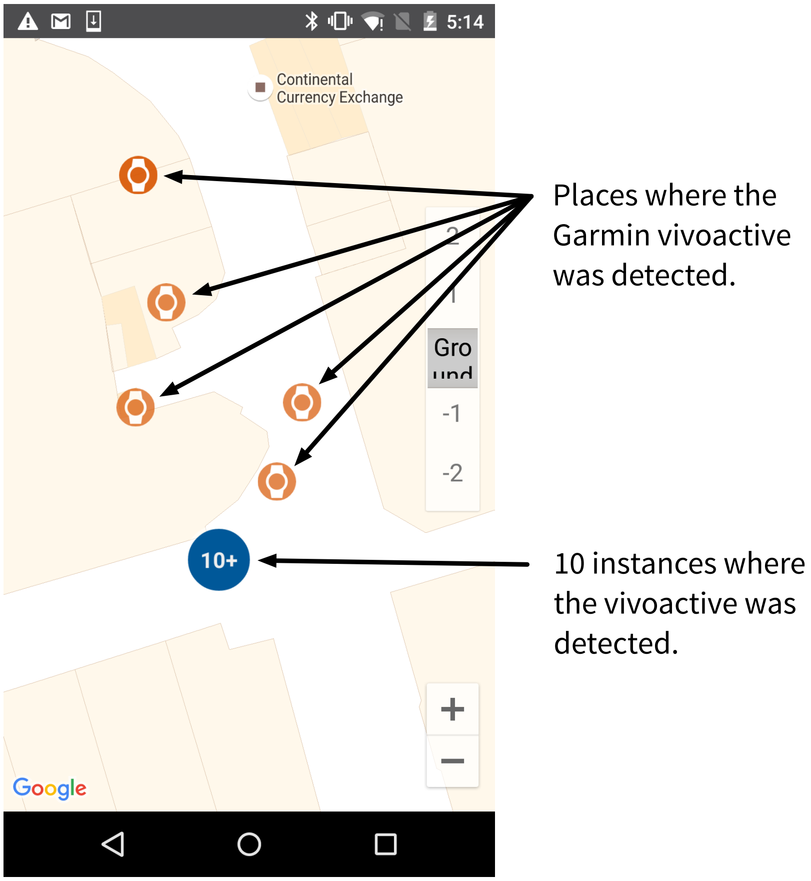


Figure 3: Screenshot from the RamBLE application showing a map of a shopping centre. Icons indicate locations where RamBLE scans detected the presence of a particular Garmin Vivoactive fitness wearable over a period of 40 minutes.

over Bluetooth to the user's phone, and the Intel team did not indicate that it intended to fix the emission of a persistent MAC address through advertising packets when the device was not connected to a mobile device.

2.5.3 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.

2.6 TRANSMISSION SECURITY

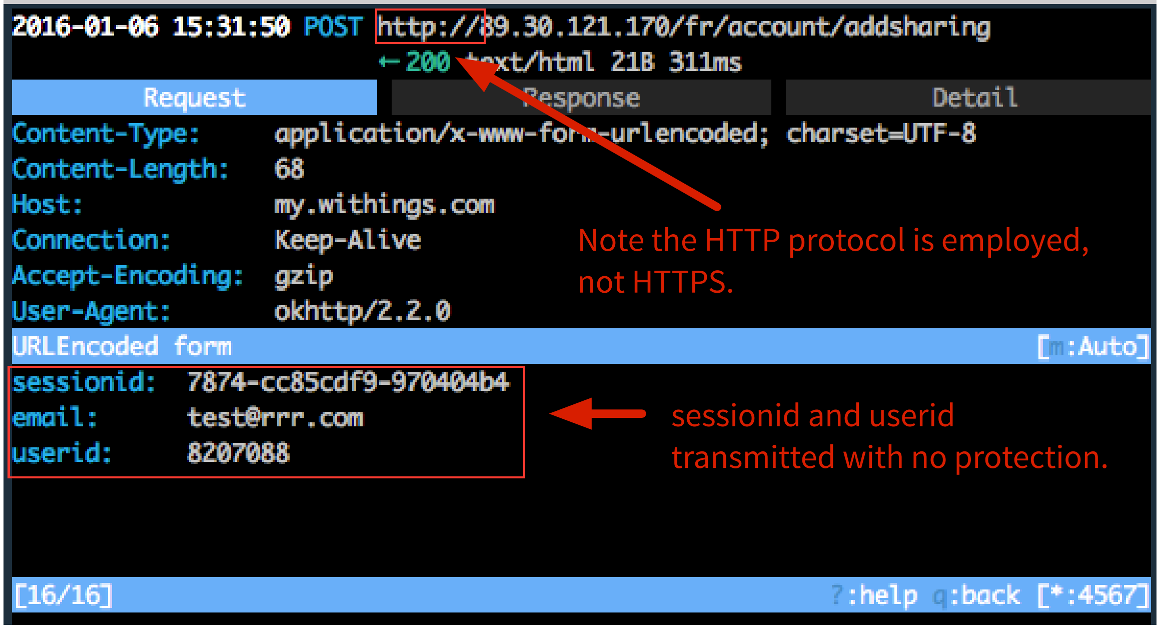
Our research revealed that most fitness devices’ mobile applications used HTTPS to routinely encrypt their communications with remote servers. These transmission take place when for signing up, logging in, logging fitness data, and for other application events. By adopting HTTPS, fitness tracking companies are helping to shield consumers from third parties’ who would monitor or tamper with fitness data exchanged between users’ mobile applications and company servers. This security practice was not employed in two notable cases.

2.6.1 GARMIN CONNECT

The Garmin Connect Android and iOS applications did not use HTTPS for routine data transmission, such as fitness event logging, downloading daily fitness summaries, and the modification of privacy settings. Consequently all fitness data transmitted using the company’s mobile applications could 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 included 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.

2.6.2 WITHINGS HEALTH MATE

The Withings Health Mate Android application generally employed HTTPS and the Health Mate iPhone application appeared to use it consistently. However, HTTPS was not used for the Android version's "Share my dashboard" feature. This feature let 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 included 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 could 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.[33] Figure 5 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.

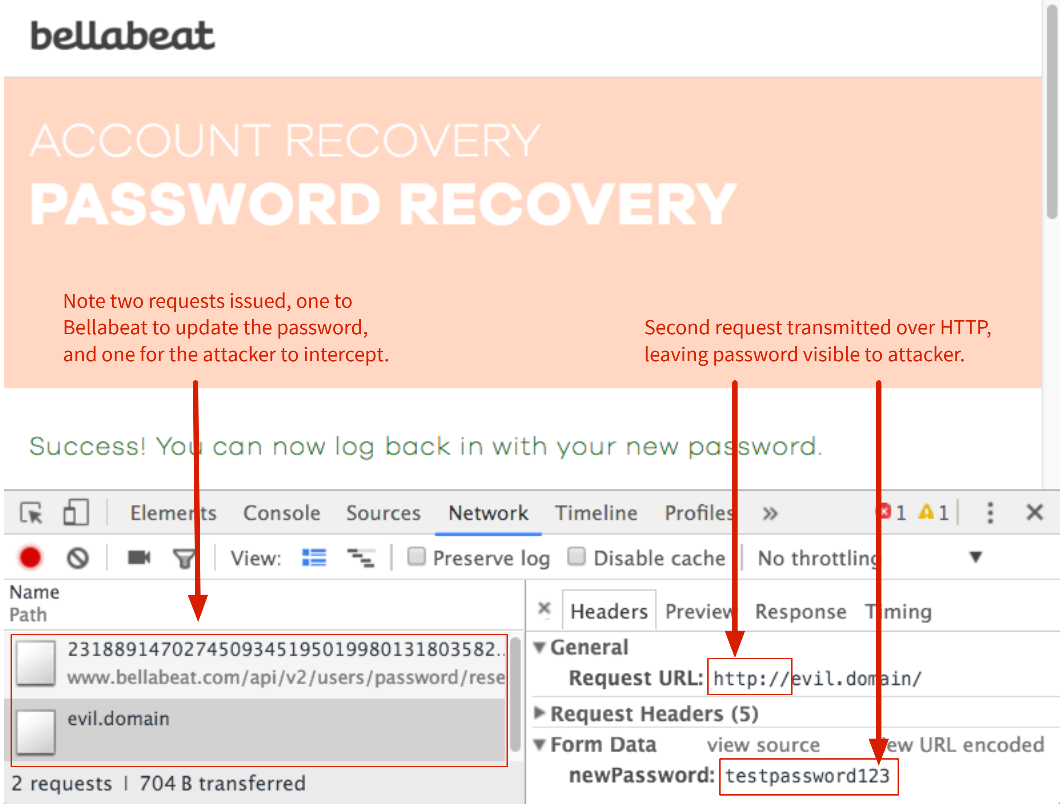
Figure 4: Screenshot from mitmproxy showing an intercepted plaintext HTTP request originating from the Withings Health Mate Android application that contains the sessionid and userid (as well as a contact's email address).

2.6.3 BELLABEAT LEAF

We observed the Bellabeat LEAF application to regularly employ HTTPS for its data transfers, thus helping to protect the confidentiality of user fitness data. However, we discovered that

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

Bellabeat sends an email to the user that instructs them to visit a reset link, if a user initiates a password reset request. That linked web page was served over HTTP. Even though the form used on the web page submitted its data over HTTPS, the fact that the page itself was served without encryption means that a man-in-the-middle attacker could modify the page's JavaScript code to ensure that the password reset form sends the new password over HTTPS to Bellabeat as expected, but also sends it over HTTP and/or to an arbitrary URL, thus enabling the attacker to collect the new password and obtain access to the targeted user's account.



bellabeat

ACCOUNT RECOVERY

PASSWORD RECOVERY

Note two requests issued, one to Bellabeat to update the password, and one for the attacker to intercept.

Second request transmitted over HTTP, leaving password visible to attacker.

Success! You can now log back in with your new password.

2318891470274509345195019980131803582..
www.bellabeat.com/api/v2/users/password/rese

evil.domain

2 requests | 704 B transferred

▼General
Request URL: http://evil.domain/

▶Request Headers (5)

▼Form Data view source view URL encoded
newPassword: testpassword123

Figure 5: Screenshot from the Bellabeat password reset web page, served over HTTP, with proof-of-concept JavaScript code to send the user's new password to a third party.

Bellabeat fixed this issue shortly after we notified them. At the time of writing, the company's password reset emails directed users to a page served over HTTPS.

2.6.4 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 vulnerabilities in the Withings Health Mate Android application and Bellabeat LEAF exposed their users to similar threat, though the potential for exposure was smaller. The difference between the two vulnerabilities is that while Garmin data could be passively collected by someone controlling the network, an attacker would have to wait for the particular user actions discussed above to exploit the Withings Health Mate Android application and Bellabeat LEAF. Only once the attacker received the aforementioned request could they exploit the vulnerability.

Neither Garmin nor Withings responded to our attempts to contact their security teams about these issues. However, since the initial release of our technical findings in February 2016, both Garmin and Withings fixed the issues we identified in this section.

> Prior to the publication of our findings, all of Garmin Connect's transmissions of sensitive data about the fitness habits of its users were vulnerable to third party surveillance or modification.

2.7 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. We found three fitness applications that were susceptible to spoofed manual data being accepted by fitness tracker servers and presented in the mobile application interface as fitness events that a user had input.
- **Generated fitness data** is sent following the user syncing their fitness wearable with the application. Generated fitness data is in 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 wearable itself. Three applications were vulnerable to generated fitness data being accepted by fitness tracker servers and presented in the mobile application interface as legitimate fitness events.

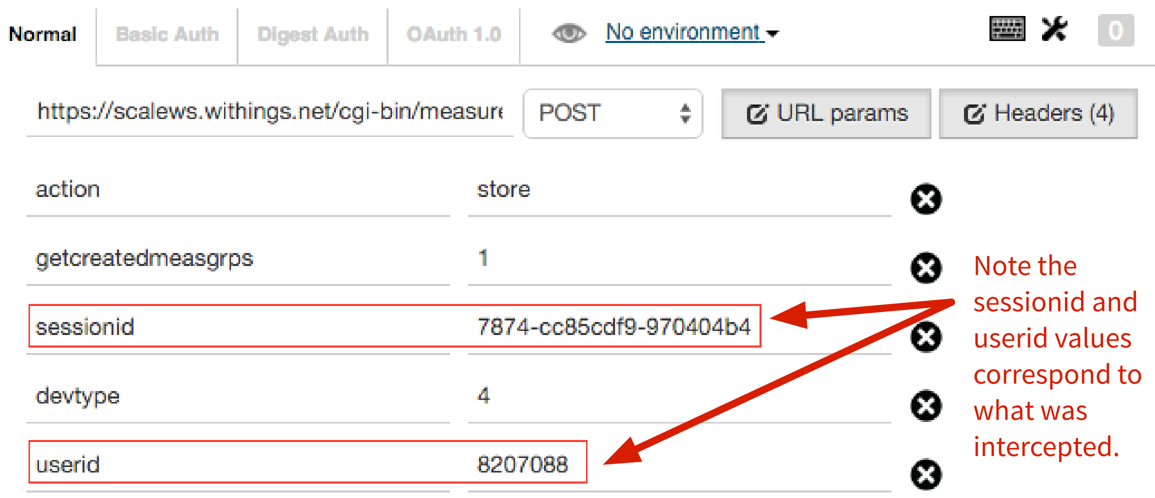
We distinguish between manual fitness data and generated fitness data because the data generated by the wearable are the product of continual and passive measurements, as opposed to the end user self-reporting manual fitness entries.

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

Garmin Connect did not use HTTPS for most application functions. In addition to not using transport security the application used OAuth 1.0 for user 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.[34]

In practice, Garmin's decision to use OAuth 1.0 without HTTPS for its mobile applications enabled 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 was also 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 included a function that made an unencrypted HTTP request. In the process of making these requests the user session credentials were exposed to third parties who could 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 was recognized, processed, and incorporated into fitness statistics by Withings servers and the Health Mate application, as demonstrated in Figures 6, 7, 8, and 9.



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

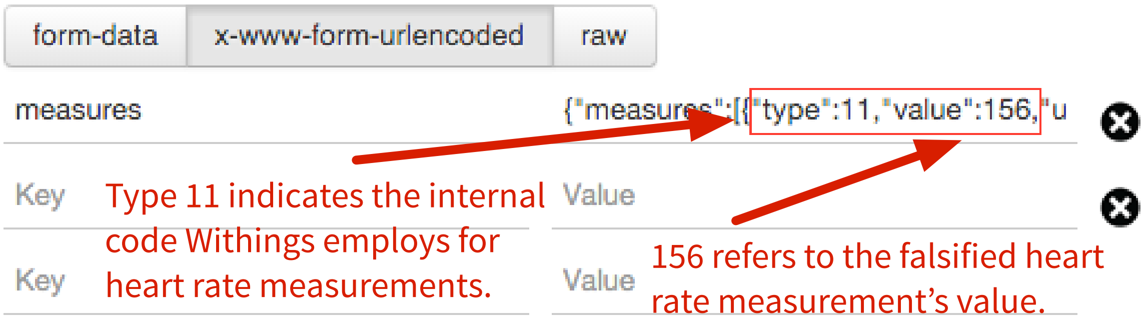
POST

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

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

Figure 6: Attacker using intercepted Withings Health Mate user's sessionid and userid values in a pre-constructed request to create new fitness data.

[34] 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`.

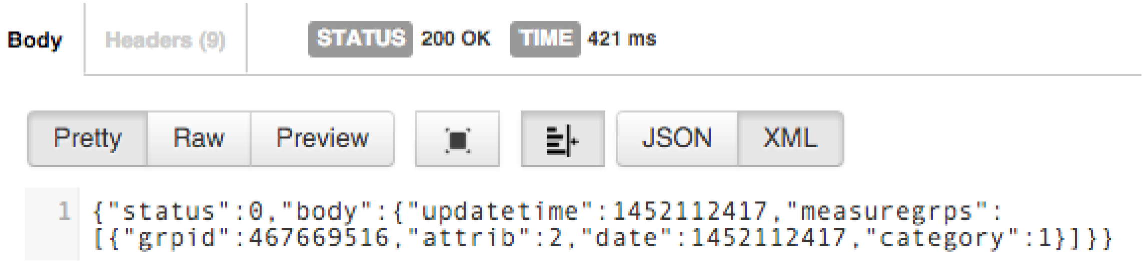


measures {"measures":[{"type":11,"value":156,"u

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

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

Figure 7: 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

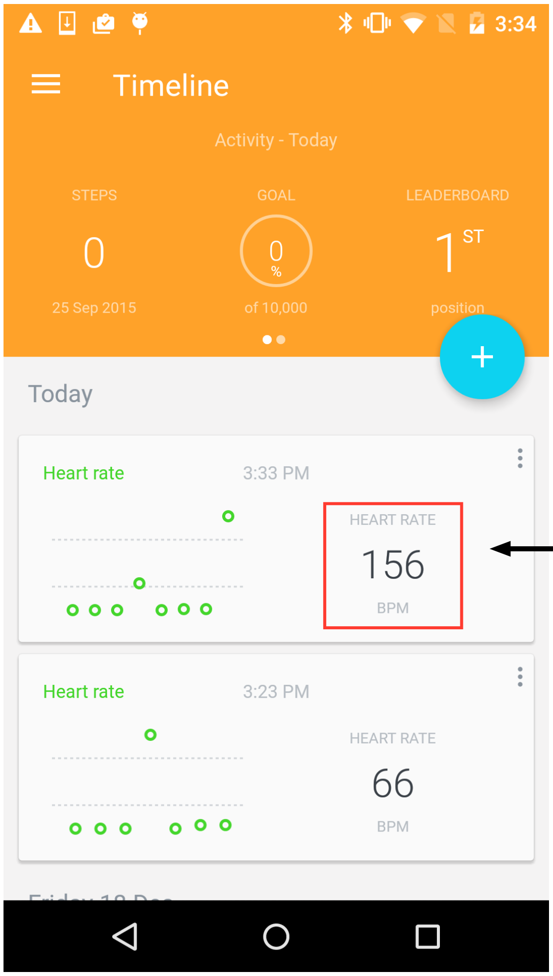
```
{"status":0,"body":{"updatetime":1452112417,"measuregrps":
[{"grpid":467669516,"attrib":2,"date":1452112417,"category":1}]}}
```

Figure 8: 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.

2.7.2 FITNESS BAND TAMPERING BY THE USER

The Bellabeat LEAF, 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 data originated from the a fitness wearable. 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 Bellabeat, 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 10. 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 11. A more sophisticated approach would randomly allocate steps to establish a more realistic-looking distribution.



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

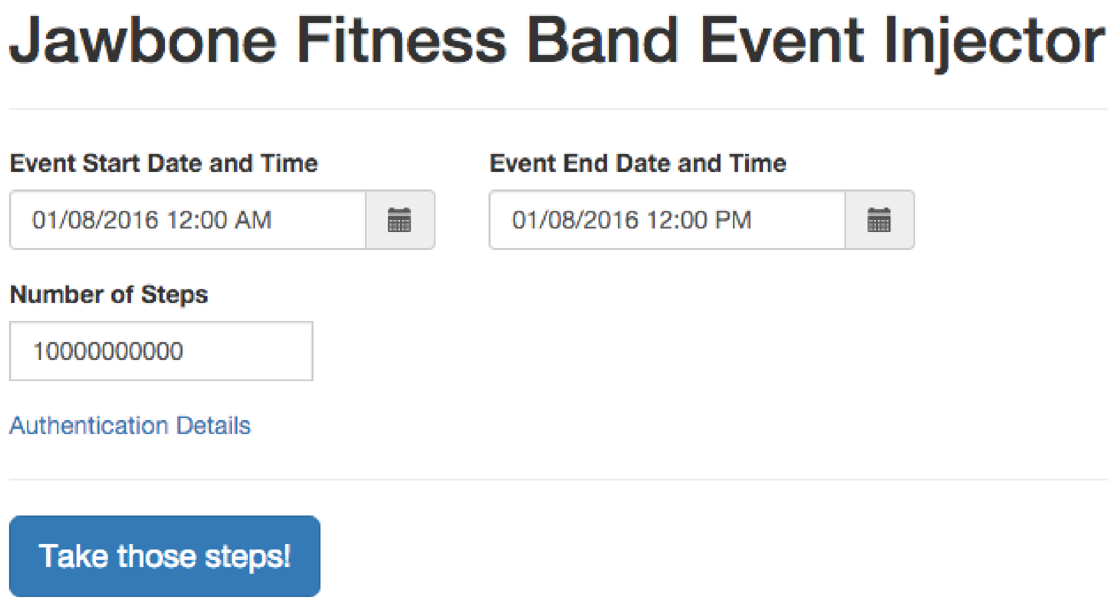
Figure 9: The false heart rate data appearing in the user's Withings Health Mate application.

> 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. Bellabeat responded, stating it would "try to fix all the problems".

2.7.3 MEASURES TO HINDER GENERATED FITNESS DATA TAMPERING

We found that Fitbit took 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.



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

Encryption was performed by software on the Charge HR, and as a result we could not determine how data transmissions were encrypted. However, we analyzed 22 Bluetooth transmissions generated by the device and found some consistencies. Each transmission included 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 were uniformly distributed at random. Moreover, the number of bytes were 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 was followed by a two-byte value and a zero byte. The two-byte value may have referred 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 running on our test network and signed by a certificate authority we had added to our test mobile phones (as described in Section 2.2.1). To analyze Basis Peak's traffic we had to remove the application's certificate pinning functionality.

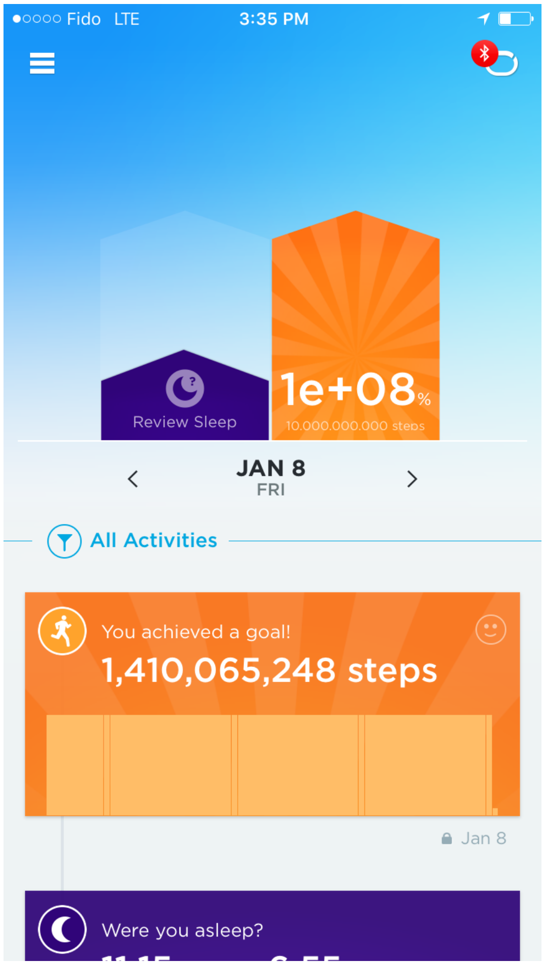


Figure 11: Jawbone UP application accepting falsified generated fitness data from our application. Note the uniformly distributed time-series graph.

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 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 2.2.1).

2.7.4 ANALYSIS

Our ability to successfully issue falsified requests to Bellabeat, Jawbone, and Withings calls into question the integrity of generated fitness data for these three 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 Bellabeat, 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.

2.7.5 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 Bellabeat, 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.

2.8 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 were 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 exposed its customers to the risk that their sensitive fitness data was being collected or tampered by unauthorized third parties, as did 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

Companies that produce fitness wearables develop and publish privacy policies as well as terms of service agreements. These documents are ostensibly designed to inform consumers about their protections and rights pursuant to using the companies' devices and services. The policies often include critical information concerning what is, and is not, considered personal information by the company in question, how and the extent to which a consumer can request access to their personal data, outline the kinds of information the may be collected in the course of using the wearable and associated services, and the relative degrees of security deployed to protect wearable-related information.

In this section, we analyse the relevant privacy policies and terms of service/use that are publicly available to users of our studied fitness wearables. We conclude that companies:

- have adopted significantly different interpretations of what constitutes personal information;
- have generally sought to ensure that legal complaints are taken up outside of Canada, and;
- have established policies concerning access to, correction of, or deletion of wearable-related that data vary considerable across the industry.

Moreover, we find that the use of company-wide privacy policies and terms of use, which often apply to a variety different devices and services, make it challenging for end users to determine which specific aspects of the policies apply to different components of a company's offerings.

This section begins by describing the methodology we adopted to analyze company policies, followed by the major findings that emerged in our analyses. The full set of questions and raw data which emerged from them is available at the Open Effect website[35]. Our conclusion highlights how the existing policies threaten to reinforce, as opposed to alleviate, many of the concerns that consumers possess concerning the use of wearables and the ability of companies to disclose and share fitness data that users provide to wearable companies.

3.1 PRIVACY POLICIES AND TERMS OF SERVICE

We adopted a methodology that researchers previously used to analyze the data capture, processing, use, and disclosure practices of social networking companies.[36] The methodology relies on archiving privacy policies and terms of service documents and then subjecting them

[35] See: `https://openeffect.ca/fitness-trackers`

[36] See the 'Canadian Access to Social Media Information (CATSMI) Project': `http://catsmi.ca`.

to a uniform set of questions and analyses. The results of these analyses, in conjunction with technical analyses conducted in Section 2 and findings from consumer efforts to try and access their personal data, discussed in Section Four, are used to understand the extent to which consumers can understand the collection, processing, use, and disclosure of their data. Section Five presents the full discussion of synthesized results of these different analytical methods.

3.2 POLICY METHODOLOGY

We collected privacy policies and terms of service documents from the studied companies examined in August 2015, save for one company (Bellabeat) that was added in February 2016. Our rationale for adding Bellabeat after initially selecting for cases was to include a company that included a focus on women's health issues, whereas all other wearable devices omitted women's health features such as menstrual cycle tracking. Table 7 identifies the specific dates on which privacy policies and companies' associated terms of service were collected.

3.2.1 DEVELOPMENT OF QUESTIONS

A total of 33 questions were developed. These were organized into six themes. Our focus was to understand the availability of privacy policy and terms of service information (e.g. general policy questions), information about how to complain or learn about company practices (e.g. procedures for users), and then an extensive set of sections on capture, disclosure, and security of information that companies collect about their users. The final series of questions focus on the extent to which individuals can access or correct data that is held by fitness wearable companies.

In aggregate, these questions are calibrated to understand the extent to which individuals are informed about how fitness devices and their associated companies collect, process, disclose, and protect information. They are also meant to reveal just what is, and is not, considered personal information and whether differences in definitions are associated with different technical or policy protections concerning different kinds of information. 3.2.2 Application of Questions In answering each question, we examined whether the privacy policies or terms of service that were collected provided a clear answer to what was asked. In some cases answers are repetitive across different questions. We sought to be charitable, insofar as where a policy's language was not precise, but could be interpreted to provide an answer to one of our questions, we assert the company does positively answer the question. However, we were also critical in the actual usefulness of information to end users; a company may have a responsive policy, but how that policy is written may be difficult for an end-user to interpret and thus only partially or 'maybe' answer the question. As we will discuss, it is often the case that end-users may be uncertain as to what practices the policies do, and do not, permit.

Company	Document Type	Date Collected
Apple	Privacy Policy	8/21/2015
Apple	Apple Watch Terms of Service	8/21/2015
Basis	Privacy Policy	8/4/2015
Bellabeat	Privacy Policy	2/16/2016
Bellabeat	Terms of Service	2/16/2016
Fitbit	Privacy Policy	8/4/2015
Fitbit	Terms of Service	8/4/2015
Garmin	Privacy Statement (Canada)	8/4/2015
Garmin	Privacy Statement (United States)	8/4/2015
Garmin	Terms of Use (Canada)	8/4/2015
Garmin	Terms of Use (United States)	8/4/2015
Jawbone	UP Privacy Policy	8/20/2015
Jawbone	UP Terms of Service	8/20/2015
Mio	Privacy Policy	8/4/2015
Mio	Terms of Service	8/4/2015
Withings	API Terms of Use	8/4/2015
Withings	Applications Terms of Use	8/4/2015
Withings	Countries We Deliver To	8/4/2015
Withings	General Sales Conditions	8/4/2015
Withings	Legal Information	8/4/2015
Withings	Policy on Cookies	8/4/2015
Withings	Policy Statement on Data Protection	8/4/2015
Withings	Privacy Policy	8/4/2015
Withings	Services Terms and Conditions	8/4/2015
Withings	Website Terms of Use	8/4/2015
Xiaomi	Mi Band User Agreement and Privacy Policy	8/4/2015

Table 7: When company policies were accessed

We note we did not approach any of the studied companies to clarify their policies and terms of service.[37] This was done on the basis that we could not guarantee responses from all companies (thus potentially giving a more positive analysis to some policies over others, where companies were non-responsive to questions) and because we wanted to approach this from the perspective of a semi-interested consumer who would read, but might not raise questions about, the given policies. As such, our analyses are drawn from how we interpreted what we read: we have not sought additional corporate guidance nor have we consulted with contract lawyers. The result is that our analyses are meant to provide insights of well-informed consumers as opposed to constituting comprehensive legal analyses of each and every policy we analyzed.

3.2.2 COMPARISON OF QUESTIONS

We based our questions on those featured in previous research funded under the Office of the Privacy Commissioner of Canada's contributions program. That project was conducted by Dr. Colin Bennett and Dr. Christopher Parsons.[38] We made comparisons after first collecting primary data from the various companies' privacy policies and terms of service documents. We returned to the analyses two months after initially conducting them to ensure that we still reached the same conclusions; where there was doubt, a second researcher was asked to consult and evaluate any apparent uncertainties or changes in the reading of policies in the first and second rounds of policy reading.

3.3 COMPARATIVE ANALYSES OF COMPANY POLICIES

We conducted both meta-analyses of privacy policies and terms of service, as well as detailed content-level analyses of the policies. The following sections present our most significant findings in our comparisons; for a full analysis of each company with regards to each question, see the Open Effect website[39].

3.3.1 GENERAL POLICY QUESTIONS

We began by investigating whether wearable device users could access companies' privacy policies from the Android and iOS application stores hosting the fitness wearables' companion applications. Apple Watch was excluded, on the basis that no application is available in the iOS

[37] However, in some cases we did ask for companies to clarify certain questions – such as whether data was shared with third-parties like insurers – as part of the PIPEDA requests that we sent to them, and which are described in Section 4. Such questions did not involve us challenging particular language in any given company's policies, but instead was meant to understand how they would describe such practices to customers.

[38] See the 'Canadian Access to Social Media Information (CATSMI) Project' at CATSMI `http://catsmi.ca`.

[39] `https://openeffect.ca/fitness-trackers`

application store. All other companies, save for Xiaomi, included links to their privacy policy in both application stores; Xiaomi lacked a link to their privacy policy in the Android store. We then examined the companies' websites, to determine if we could access the same privacy policies. All the policies, save for those of Jawbone and Xiaomi, were relatively easy to find at the bottom of wearable product pages. In the case of Jawbone, however, visitors had to click a 'privacy policy' link at the bottom of the company's webpage and subsequently click (and read) both the 'Software & Services' and 'UP privacy policy' pages. In the case of Xiaomi, the privacy policy at the bottom of the company's product page is different from that accessible via the iOS store, which may confuse users about the actual policies Xiaomi has established to protect users' personal information.

Many of these privacy policies, however, fail to explicitly break down and differentiate between data collected in the course of providing information via the company's website, to collecting fitness data with wearables, to processing that data using mobile device applications. Of the companies we reviewed, Apple, Jawbone, and Xiaomi arguably had the most explicit discussions of how wearable-related data is regulated by corporate privacy policies. In Apple's case, users must read the 'Approach to Privacy' section of Apple's website[40], with details on Apple Health and fitness data not explicitly included in their actual privacy policy. Jawbone has unique pages for their wearables, as does Xiaomi, which make it very clear to readers how the companies treat fitness-related information. Xiaomi's policy, however, was only accessible from the iOS store when we conducted our evaluations.

Perhaps most worryingly, it is commonplace for companies to reference their privacy policy in terms of service/use documents and vice versa. Despite the interwoven nature of these documents they are not always linked to one another and thus individuals must separately find the associated documents. It is often important to read the privacy policies and terms of service/use documents in conjunction; privacy policy documents cited international guidelines, such as the United States - European Union Safe Harbour Framework, United States - Swiss Safe Harbour Framework, and Better Business Bureau European Union Safe Harbour, whereas the actual terms or arbitrating disagreements and their jurisdictions wherein arbitration is to take place is noted in terms of service/use documents. Six of the surveyed companies (Apple, Bellabeat, Fitbit, Garmin, Jawbone, Withings) note that arbitration must occur in the United States, though two of these (Apple, Garmin) offer London-based arbitration for EU citizens. Xiaomi asserts that its terms of service agreement is governed by the Republic of Singapore. The sole Canadian company, Mio, does not mention the jurisdiction in which complaints or arbitration must be taken up.

[40] See `http://www.apple.com/ca/privacy/approach-to-privacy/`

3.3.2 PROCEDURES FOR USERS

After users read corporate policy documents, or if they simply have questions concerning a given wearable company's data handling or processing practices, they need to have a way of contacting the company. To understand the procedures available to users we focused on the availability of information companies provide to their customers to file complaints and access their data. While all companies we examined had some way of contacting the company about privacy-related issues, only four of nine had contact information for dedicated privacy or data protection staff. The other companies included contact information but it was often non-specific, such as 'support@mybasis.com', 'hi@bellabeat.com', 'webmaster@garmin.com', 'info@jawbone.com', and 'info@mioglobal.com'.

When examining companies privacy policies, terms of service/use documents, and product license information it became apparent that the full contours of a complaint process were rarely outlined. In fact, only Jawbone had a detailed discussion of arbitration processes associated with product- and service-based complaints; fourteen subsections in the company's Terms of Use discuss this issue, in detail, though there is no mention of it in Jawbone's privacy policy. While Apple lacks this degree of detail, it does commit that if customers are unsatisfied with how the company tries to address a grievance, the company will "endeavor to provide you with information about relevant complaint avenues which may be applicable to your circumstances." A subset of companies, including Basis, Fitbit, Garmin, and Withings make mention that customers can either take up complaints through the Better Business Bureau European Union Safe Harbour of JAMS International.[41] Mio, and Bellabeat lack formal complaints processes, and Xiaomi just asserts that complaints should be resolved amicably.

Complaints may depend on access to information retained by companies. As such, whether there is a statute limiting access to data, or if data is inaccessible following the deletion of an account, is important for collecting evidence needed to file a complaint. Several companies, including Apple, Basis, Bellabeat, and Mio, do not disclose for how long they retain personally identifiable information associated with their wearable products in their privacy policies or terms of service/use documents.

The remaining companies tend to offer ambiguous statements on data retention periods. Fitbit, as an example, retains personally identifiable information (PII) as long as a user maintains an account, and only deletes accounts after individuals contact the company's support agents requesting a deletion.

Garmin stores data as long as "necessary to fulfill the purposes outlined in this Privacy Statement unless a longer retention period is required or permitted by law." The company may decline to process requests "that jeopardize the privacy of others, are extremely impractical, or

[41] JAMS International is an organization headquartered in London works to settle disputes between parties. Their core function is to help result disputes for parties located in different jurisdictions.

would cause us to take any action that is not permissible under applicable laws." 'Residual' information, or that used for 'recordkeeping purposes', may also be stored indefinitely by the company.

Jawbone recommends that individuals contact the company's support email address to have their data deleted, while noting that some data will have been "aggregated into anonymized system usage statistics" and thus remain on Jawbone servers after a deletion request is made. While Jawbone permits users to download their data as a CSV file there is no indication how long after requesting deletion that data can be downloaded.

Withings notes it retains data indefinitely or until a user deletes their account; while individuals are informed they can export data, it is unclear how encompassing this right is, or how it would be specifically exercised.

Finally, Xiaomi does not indicate how long data is retained on their servers after a user terminates their Mi Account. It does, however, outline that once the company obtains "sufficient information to accommodate your request for access or correction of your personal data, we shall process in accordance with the laws of your country. While we try our utmost in acceding to your requests, unreasonably repetitive or unrealistic requests or those that put others' privacy at risk may be declined." A "reasonable fee" may be imposed on some data access/correction cases.

3.3.3 CAPTURE OF PERSONALLY IDENTIFIABLE INFORMATION

Wearable companies collect information generated automatically, or manually, by individuals using the wearables and their companion mobile applications. However, the definitions that are applied to what is, and is not, personally identifiable information can have significant impacts on the degree of protection afforded to collected data. This section focuses on the differentiations between companies' definitions of personal, non-personal, and sensitive information as well as whether the privacy policies or terms of service establish specific rules pertaining to collecting informations about minors.

Only one company, Xiaomi, explicitly stated that fitness tracker information constituted personally identifiable information (PII) and gave an extensive list of other data that is PII, such as email address, phone number, mobile device identifiers (e.g. IMEI), location information, and physical characteristics (e.g. age, weight, height, gender). More generally, companies maintained that information that relates to an identified or identifiable person constitutes PII. For Fitbit, "data that could reasonably be linked back to you" is PII, for Garmin it is "information that identifies a particular individual", and for Basis information that the user provides to the company is PII. Mio noted that PII is that which "you decide to provide us with" and that may include fitness data. Jawbone lacked an explicit definition of PII. Withings stated that personal data included "any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." This general statement, however, is not directly correlated with fitness data and thus leaves unclear whether that data sufficiently relates to an identified or identifiable person.

Several companies excluded fitness information from some of their definitions of PII. For Bellabeat the term encapsulates "information that relates to an identified or identifiable natural person" and sensitive PII means "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sexual health." The company identifies fitness data as PII but excludes it from the sensitive personal data category. In Garmin's case they exclude 'activity data' from PII, which includes steps, location, distance, pace, activity, time, and calories burned. It is unclear if Mio's definition of personal data necessarily captures fitness data. Apple did not include fitness data as a kind of personal data that the company collects, either, though this may stem from Apple's inability to access fitness data: it is stored such that only users, and not the company, can access and disclose the health-related information. Consequently there remains a question of whether this storage of encrypted data – which Apple cannot access – constitutes the collection of personal information or the storage of encrypted data instead.

The majority of companies we reviewed distinguished between collecting data from minors versus adults; some automatically delete minors' information upon discovering it whereas in other cases parental/guardian consent can authorize a minor's use of the wearable device. Companies that avoided knowingly collecting, using, or disclosing information about children include Apple, Basis, Bellabeat, Fitbit, Garmin, and Withings. Adults could consent to minors using products from Apple, Basis, and Withings. Xiaomi considered it up to parents to determine whether children can use the company's wearables and did not actively seek minors' information, and parents/guardians were invited to request the company delete their children's' data if it had been collected with parental/guardian consent. Only Jawbone and Mio lacked any policies concerning the collection of minors' information.

3.3.4 DISCLOSURES OF INFORMATION

Fitness trackers are worn, principally, so that individuals can track their own levels of physical activity, often with the aim of increasing their daily exercise levels. In addition to this fitness-related information, they provide personal biographical data, location data is collected, mood data sometimes inserted, and more. In effect, large volumes of potentially sensitive information is collected and stored by the companies selling wearable devices and offering associated fitness applications. In light of this, we examined fitness tracker companies' privacy policies to determine the extents to which companies assert their right to disclose fitness information to third parties, and the conditions under which such disclosures are authorized.

It was rare for companies to explicitly state to whom they will share or disclose information. Basis informed its users that information that has been aggregated and de-identified may be shared or sold to third parties or in order to complete business practices (e.g. processing payments). Jawbone also shared aggregated statistics. Likewise, Bellabeat could share information with third-parties to complete business practices, as could automatically collected information. Mio, Withings, and Xiaomi could also share information in the course of business operations. Of note, Garmin asserts that in addition to maybe using third parties to process collected data, the language is expansive enough[42] to render it unclear when data cannot be permanently shared (as opposed to temporary processing under contract). The company also stated that it may share information with affiliates, with the listing denoted in their 10-K form that was filed with the United States Security Exchange Commission. When we followed the link provided by the company it was not evident where that form was located. Only Fitbit was explicit about the advertising and analytics companies that it uses, though did not identify with whom fitness data might be shared.

All companies, save for Apple, Withings, and Xiaomi reserved the right to sell user data in the case of a bankruptcy, leaving open the possibility for data to be released to other parties. Basis, Fitbit, and could also sell de-identified data. All companies noted that they could choose to, or be compelled to, disclose information to state authorities; while Apple provided guidance on their website vis-a-vis their transparency report about the requirements they established for disclosing data, no other company clearly outlined a company's procedures for receiving, and evaluating, demands or orders served by public bodies. No company noted that it could share information with insurance companies or make it available to wellness programs.

3.3.5 SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

Given the sensitivity of the information collected by wearable companies, we examined the commitments different companies made, if any, to the security of the data they transmit and retain. Apple and Xiaomi were the only companies that had clear and strong assertions about the kinds of security provided to user data. The former company asserted, "data in the Health app and your Health data on Apple watch are encrypted with keys protected by your passcode. Your Health data only leaves or is received by your iPhone or Apple Watch when you choose to sync, back up your data, or grant access to a third-party app. Any Health data backed up to iCloud is encrypted both in transit and on our servers." Xiaomi had a particularly detailed discussion

[42] Based on our analysis of Garmin's publicly available documents, we found that the company may share information with its: affiliates, third-parties to operate its business, others generally with either the user's consent or as required under law, third-parties or affiliates or subsidiaries in the event of reorganizations or mergers or sales or joint ventures or assignment transfer or other disposition of "Garmin's business, assets, or stock" such as in connection with bankruptcy or other proceeding.

of its security practices, including assertions that servers were kept in secure rooms, that data was exchanged using SSL, that two-step/factor authentication could be used to secure data, that there were regular reviews of security policies, that confidentiality agreements barred Xiaomi employees and contractors from discussing user data, and that employees had access to subsets, as opposed to all of, users' data.

Other companies made broader statements concerning the security of data they were entrusted with. Basis employed "reasonable security measures". Bellabeat also employs such methods though the company "cannot guarantee that our security measures will prevent third-parties such as so-called hackers from illegally obtaining access to personal data. We do not warrant or represent that personal data about you will be protected against, loss, misuse, or alteration by third parties." Fitbit used "a combination of technical and administrative security controls to maintain the security of your data" and, like Garmin consumers, were recommended to contact support if they have questions concerning the security of their data; Fitbit assures consumers that it "takes reasonable security measures to help protect against loss, misuse, and unauthorized disclosure or alteration of the Personal Information under its control." Jawbone also limited its assertion of security, writing that while it applied "organizational and technical measures to ensure access to your information is limited to persons with a need to know neither we – nor any company – can fully eliminate security risks." Mio stated it does not retain credit card information and that third party service providers it employed must "maintain the privacy and security of your data." Withings had a slightly more specific, physical security, statement, writing that "data are mainly stored on servers located in France [...] equipped with the latest security equipment and advanced security techniques and procedures. Access is strictly restricted and various security controls, consisting of security staff, security doors and biometric readers, must be passed. Remote access to the servers is highly restricted and controlled."

No company made any mention of alerting users in the case of a data breach.

3.3.6 ACCESS AND CORRECTION

The data that is collected by wearable fitness companies' devices and applications can provide a rich dataset concerning personal health and activity. While most companies display the information to users, often with accompanying recommendations or suggestions for further fitness improvements, users in academic and non-academic studies alike[43] have indicated concern that fitness trackers companies might function like data roach motels: the users' data may check in, but it can never be removed from the companies in question. As such, we examined

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

terms of service/use and privacy policies to understand the extent to which personal information can be accessed, corrected, and exported by users.

Four companies explicitly noted that users have a right to access and export their data: Bellabeat, Jawbone, Withings, and Xiaomi. In the case of Apple, users could access and export their data, though given the encrypted nature of Health data the company could not provide such data to end users. Basis excluded any mention of exporting data and Garmin reserved the right to not implement data correction requests where they would "jeopardize the privacy of others, are extremely impractical, or would cause [Garmin] to take any action that is not permissible under applicable laws." Mio failed to include any discussion of accessing or exporting data.

Of the companies, only Jawbone and Fitbit stated that their data set will be exported in an open format (CSV file or XLS). Withings stated that "[y]our personal data is and shall remain easily accessible. This means that you can always export your personal data in an open format for you to easily keep and access", though there is no information about either the exportation process or the format(s) the data is structures in. Bellabeat, while not disclosing the format of the exported data, noted that exercising one's right of access can incur a "small processing fee" if less than twelve months have followed from the user's last access request. Xiaomi, also, reserved the right to charge a "reasonable fee" for user access to their own data.

All companies, save for Mio, acknowledged that users have at least some limited rights to correct data. The specificity of what can be changed varies; Basis users, as an example, were informed they can change name, address, and contact information (and nothing else is mentioned) whereas Bellabeat suggested users self-update their profile or contact support. Fitbit and Jawbone both asserted individuals' right to update their information. Withings had an explicit right to amend your data as one of the company's principles, with amendments possible in the application or by contacting the company's support team. In the case of Xiaomi individuals had to verify their identity; after doing so Xiaomi would "accommodate" the request, though there were no specific details concerning what such accommodation would entail.

3.4 CONCLUSION

Companies' privacy policies and terms of service/use agreements varied considerably from one another. Our empirical analysis of these documents revealed that companies had divergent definitions of what constitutes personal information, generally ensured that complaints against companies are taken up outside of Canada, that policies concerning access, export, and correction of data differed significantly, and that security guarantees differed in their level of detail.

What was perhaps most pressing was how the policies reinforce and exacerbate concerns that individuals have concerning fitness tracking devices and services. That data can be sold or exchanged with third parties reinforces concerns that consumers had about the privacy of their data: data is ‘private’ only to the extent that such privacy was fiscally responsible for the company. In the case of bankruptcy, partnerships, or acquisitions many companies would include their users’ personal data amongst the other assets possessed, and tradeable/saleable, by the company in question.

Moreover, while data was in many cases are apparently available for sale to third parties, it was often far less apparent how, and to what extent, individuals could comprehensively export their own personal information from fitness tracker companies. In some cases exporting data might have incurred some charges, whereas in others is seemingly limited to basic biographical information. Where individuals had a complaint concerning how a company treats such requests, the companies’ own policies tended to assert that disputes must be taken up in non-Canadian jurisdictions. Regardless of the accuracy of such policy statements they could serve to confuse or mislead consumers who may interpret corporate policies as necessarily overriding national privacy and right of access laws.

One issue area that stands out, from the policy documents, is that no companies made any mention of sharing information directly with insurance companies. However, the parties with whom data could be ‘aggregated and disclosed in a de-identified manner’ were often left unstated, with the effect of rendering it unclear if such third parties might include insurance companies or other health-focused organizations.

Privacy policies and terms of service documents have been critiqued by scholars in the past for being opaque, unclear, misleading, and even contradictory[44]. Our survey of privacy policies and terms of service/use support this generalized conclusion. In the next section we focus on the ability of Canadians to successfully exert their legal rights to access personal information retained by fitness tracker companies. That exercise, in tandem with research conducted in Sections 4 and 5, will subsequently let us analyze whether the data items disclosed in technical analyses and policy evaluation are the same, or whether there is significant variance between what companies actually collect, what they say they collect, and what they disclose to users they collect.

[44] See, for example: McDonald, A. M. and Cranor, L. F. (2008). The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society.http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

4 PIPEDA FINDINGS

Fitness wearable manufacturers, like all other companies doing business in Canada, are subject to the Personal Information Protection and Electronic Documents Act (PIPEDA). Principle 4.9 of PIPEDA outlines the access and correction rights of Canadians with regard to their personal data being collected and/or utilized by commercial organizations. Canadians have the right to "be informed of the existence, use, and disclosure of their personal information and be given access to that information."[45] Individuals may be required to provide proof of identity such that organizations can retrieve the requested information. Organizations have a maximum of thirty days to respond to a request, and may notify individuals they require an extension of an additional thirty days to fully respond. Access should be provided at minimal or no cost.

This section describes how fitness wearable companies, most of which were based outside of Canada, responded to requests for access to personal information under Canadian law. Overall, we find variation in whether companies responded, the level of security and identity verification, the level of detail in responding to questions about how personal data is managed, and how customers could access their raw data. No responsive companies requested our participants pay fees to access their personal data.

4.1 METHODOLOGY

For each studied fitness tracker we recruited a research participant to use the device and companion smartphone for two months. They were instructed to use them as a normal user would. Participants were recruited from the University of Toronto community. They were compensated by being able to keep their fitness tracker after the conclusion of the study. After two months' time we provided participants the text of an email for them to send to the manufacturer of their fitness wearable. Table 8 indicates when initial contact was made and documents the speed at which companies provided responses.

Participants were asked to send companies emails that constituted formal requests for access to their information under PIPEDA. The request asked questions about the respective companies' data sharing with third parties such as insurance companies, legal jurisdiction, policies regarding government requests for data, data security measures, and Bluetooth security measures. The letter also requested access to all personal information held by the company, and listed the following specific information:

- fitness data,
- IP addresses,

[45] Office of the Privacy Commissioner of Canada. Interpretation Bulletin: Access to Personal Information. Online at: https://www.priv.gc.ca/leg_c/interpretations_05_access_e.asp

- account details,
- geolocation,
- information about the user collected through the app,
- other kinds of information,
- and information about disclosures to third parties.

The letter cites PIPEDA and informs companies of their requirement to respond to participants within thirty days at no or minimal cost. The entirety of the letter is reproduced on the Open Effect website[46]. Given that this was an project funded by the Office of the Privacy Commissioner of Canada (OPC), we declined to include a formal complaints process to the OPC should companies prove non-responsive to participants' requests, though we did not prevent participants from complaining in a personal capacity if they wanted to. As far as we know, no participant initiated a formal complaint to the OPC.

Participants emailed their requests to fitness tracker companies to the email address of the privacy contact listed on the company's privacy policy. If they did not receive a response after thirty days we provided participants with the text of a reminder email for them to send to the company in question.

4.2 RESPONSE RATES

Overall, six out of nine companies replied in some form to our participants' emails. Responsive companies were Apple, Basis, Bellabeat, Fitbit, Jawbone, and Xiaomi. Three companies, Garmin, Mio, and Withings, did not respond and thus prevented our participants' from executing their legal right of access. After repeated attempts to contact, and emails rejected by Xiaomi's mailserver[47], Xiaomi Customer Service replied to our participant and indicated they would consider the request. However, our participant was never contacted again after receiving this indication. The quote below captures the single response from Xiaomi received by the participant. Table 8 outlines the timeline of participant PIPEDA request engagements with fitness tracker companies.

[46] See: `https://openeffect.ca/fitness-trackers`

[47] Our participant's first attempt to contact Xiaomi was to the email address listed on their privacy policy (legalqa@xiaomi.com). This email resulted in a rejected message with the status "failed permanently: 550 Denied by policy". After contacting several other email addresses, customer service finally responded.

Company	Request Sent	Reminder Sent	Initial Response	Additional info sent	Question responses	Additional info sent	Data received
Apple	11/2/2015	N/A	11/3/2015	11/3/2015	11/13/2015	N/A	11/13/2015
Basis	10/23/2015	N/A	11/23/2015	N/A	11/23/2015	2/29/2016	–
Bellabeat	12/15/2015	N/A	2/10/2016	N/A	2/10/2016	3/1/2015	–
Fitbit	10/22/2015	N/A	11/14/2015	2/29/2016	3/15/2016	N/A	3/15/2016
Garmin	11/16/2015	12/17/2015	–	–		–	–
Jawbone	11/3/2015	N/A	12/8/2015	N/A	12/8/2015	N/A	–
Mio	11/10/2015	12/12/2015	–	–	–	–	–
Withings	11/16/2015	3/8/2016	–	–	–	–	–
Xiaomi	11/10/2015	1/12/2016	1/12/2016	–	–	–	–

Table 8: Timeline of participant PIPEDA request and subsequent interactions with companies. Note that in the case of Fitbit, our participant took over two months to provide identity verification to Fitbit, thus delaying the company's response.

> We are so honored that our products have gained your favor, We want to sincerely appreciated for your kind love and interests towards to Xiaomi We shall passing on this information to the respective channel for further consideration. They will be reaching out to you once we want to expand our business further, or any related information, discussion is in need. Thank you very much!
>
> We appreciate your understanding and cooperation. if you have any further question, please feel free to contact us. May you experience a lifetime of love, happiness and joy!

Five out of nine fitness companies provided a formal response to participants' PIPEDA access requests. We now turn our discussion to the those responses, grouped into themes.

4.3 SECURITY MEASURES

None of the responsive companies provided access to personal data alongside the initial written response to participants' request letters. Three asked for additional information to verify the requester's identity and three required an additional email to verify the participant identity or set up a secure data exchange.

Apple, in its reply, asked for several different pieces of identifying information to verify the identity of our participant. These were:

- Full name;

- Apple ID if known;
- email address;
- street address;
- telephone number;
- a registered product serial number; and
- AppleCare support case number (if available).

Apple responded to several of the questions posed in the request letter after receiving this identifying information and also provided a data dump to the participant in a password-protected ZIP file. The password for this file was provided in a subsequent email to the participant.

Basis responded to the questions in the request letter but did not immediately provide data to the participant. Instead, Basis instructed our participant to create a PGP key and send the public key to Basis so that they could encrypt a data dump against the participants' key.[48] This approach offered a high-security way of transmitting data but, in the case of our participant, posed problems on the basis that creating such a key is a non-trivial process for many end-users. In our situation the participant could not create a key on their own owing to a lack of expertise. We did, however, create one for them and had the participant send it to Basis, who, at the time of writing, have not followed up.

Bellabeat asked the participant to provide their account username or email address prior to providing access to data. Fitbit asked the participant to verify their email address and provide the approximate date on which they first paired their device. Fitbit also informed our participant that they were "unable to deliver your information in a non-secure format." They provided two options for secure exchange. The first was to share the data in Google Drive with our participant, and the second was to send an encrypted zip file. Our participant chose Google Drive.

Jawbone directed our participant to its data export tool where the user had to authenticate using their Jawbone account prior to accessing their fitness data.

4.4 DATA RECEIVED

The PIPEDA letters that participants sent to fitness companies included a request for access to all personal data pertaining to the participant held by the companies. Specific data types were requested, as described in the letter sample on Open Effect's website[49].

[48] PGP, or "Pretty Good Privacy", is an encryption technique used to secure communications. Please consult here for more details: https://ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp

[49] See: https://openeffect.ca/fitness-trackers

Apple was the only company that responded with what they stated was the participant's "personal information in full". As described above, Basis indicated it would provide access once our participant provided a PGP public key for them to encrypt the data file against. Bellabeat similarly promised access after identity confirmation, though at time of writing, the company has not responded after our participant provided the requested information. Jawbone directed our participant to its data download tool, even though the request letter specifically asked for personal data not available through a data download tool. Jawbone did not mention the request for additional data in its response.

In its response letter, Basis provided information about two of the specific data types that were requested. Regarding the logging of IP addresses, Basis stated that it "does not track which IP addresses are used by you, your devices, or accounts." Regarding geolocation information, Basis stated that "Basis does not collect location information with the exception of the optional "playground" feature you may have enabled." IP addresses were provided for specific dates and times, leading us to speculate they represent records of each establishment of a login session with Basis' servers.

Fitbit provided our participant a Google Drive spreadsheet with several Sheets, entitled "User Info", "Step Data", "Body Description", "Sleep", "Weight", "Active Minutes", "Heart Rate", "IP Address", and "Activity". Fitbit provided a record of our participants' heart rate in five minute intervals. Step Data was not provided in such a granular format, but aggregated step counts into daily intervals. Sleep data included start time, end time, minutes to fall asleep, times woken up, among other fields.

Apple provided several spreadsheets. One of them is a data definition document, which provides descriptions for the various data fields found throughout the other files.

Our participant did not receive any health data from Apple. In its response letter, Apple stated that with regard to Health and Fitness data, requesters should consult the "Our Approach to Privacy" document, that includes the following statement: "Your data in the Health app and your activity data on Apple Watch are encrypted with keys protected by your passcode" and that "any Health data backed up to iCloud is encrypted both in transit and on our server".[50] While our participant did back up Health data to iCloud, Apple did not provide our participant with access to the encrypted data that his or her passcode could then decrypt. Apple did provide a timestamped list of IP addresses used to access our participant's iCloud account.

The only data relevant to the Apple Watch our participant received from Apple were three MAC addresses from a spreadsheet of various other hardware identifiers associated with our participant (laptop, iPhone, etc.). The MAC addresses were labelled eousb_mac_addr, bt_mac_addr, and wifi_mac_addr, seemingly representing addresses for USB, Bluetooth, and WiFi. The three addresses were incrementing hexadecimal values. Notably the Bluetooth MAC address was

[50] Apple. Approach to Privacy. Retrieved from: http://www.apple.com/privacy/approach-to-privacy/.

different than any values we observed in our technical tests.

4.5 RESPONSES TO QUESTIONS

Each participant's PIPEDA right to information request letter contained five questions about the fitness tracking companies' data handling practices. Each of the following subsections begins by recounting the question, and then summarizes companies' responses.

4.5.1 DATA SHARING

Can you clarify whether my data, either in an individualized data set or as part of an aggregate data set, has been provided to insurance agencies? And if it has been provided (either voluntarily, as part of a commercial transaction, or on other grounds) please identify to which insurance agencies it has been provided.

Apple stated it "does not share personal information with insurance companies, in aggregated form or otherwise." Basis similarly, though less specifically, and only referring to the past, stated that it "has not provided your data to insurance companies." Bellabeat responded that data generated by the LEAF "have not been provided to any 3rd parties nor will it be" and went on to note that users would be informed and asked for explicit consent if such transfers were to occur. Fitbit stated that it does not "provide your identifiable data to third parties outside of the purposes identified in our Privacy Policy". Bellabeat's response, however, does not explicitly address data generated in the companion application, which includes menstrual cycle frequency, breathing exercise routines, and pregnancy status. Jawbone, in contrast to the other companies, provided a wide range of scenarios in which personal data may be shared, including "for the purposes of a business deal", "in connection with investigating fraud", and to provide social features to its users. Apple, Basis, and Bellabeat companion applications do not have social features.

4.5.2 JURISDICTION

I wanted to clarify what jurisdiction any concerns, complaints, or conflicts are resolved in. I live in Canada; am I bound to engage with your company in a non-Canadian arbitration or legal environment? I am not planning on engaging in such a conflict but wanted to better understand my rights.

Apple did not mention the jurisdiction in which complaints were to be resolved. Basis did not provide a clear response to this question, stating the location would be dependent on "the specific nature of the issue and the parties involved." Bellabeat provided a URL to its Terms of Service, and provided an excerpt from that policy that stated the terms were governed by the laws of California and that users consented to that jurisdiction serving as a venue for any claims. Fitbit asked our participant to "please see our Terms of Service under Dispute Resolution. Fitbit and our users agree to a binding arbitration under California law", and additionally advised the participant to speak with an attorney if they had further questions. Jawbone provided three pages of information about its binding arbitration process. This included a sections such as: definitions, information about informal complaint resolution process (contact customer service), agreement to arbitrate with right to opt out, description of arbitration, opt out provision (notify in writing within 30 days of TOS agreement or by fax), arbitration fee limiting, arbitration rules (American Arbitration Association (AAA)), Selection of arbitrator process (AAA selection), arbitration initiation process, time restriction (within 1 year after occurrence of grievance), recovery and attorney's fees, arbitration confidentiality rules, and survival of arbitration provision beyond the use of Jawbone products or services.

4.5.3 DISCLOSURES TO GOVERNMENT AGENCIES

What are your policies, practices, or processes for handling requests from authorities from international jurisdictions, such as from Canadian policing organizations? How would you respond if my information was requested as evidence in a Canadian court case or criminal proceeding?

In its response, Apple simply requested the participant to refer to their web page on government information requests.[51] Fitbit stated that it would only respond to requests for data "issued by a U.S. governmental entity or court and when properly served." The company went on to say that parties outside the United States should use appropriate international processes such as Mutual Legal Assistance Treaties or letters rogatory. Basis stated that its policy "is to comply with applicable laws and regulations in the jurisdictions in which it does business." Bellabeat replied that they had forwarded the question to their legal team and would get back with a response, which has not been received as of the time of writing after their reply. Finally, Jawbone, while it did not directly respond to this question, did assert that the company would share data "to comply with relevant laws [...] or respond to lawful requests, court orders, and legal process."

[51] Apple. Government Information Requests. Retrieved from: `http://www.apple.com/privacy/government-information-requests`.

4.5.4 DATA SECURITY

Is the personal data transmitted between my mobile phone and your web servers secured against potential eavesdroppers? What about between my fitness band and my phone?

In its response, Apple stated that personal data transferred between the iPhone and Apple servers uses encryption. It referred our participant to an article about iCloud data security.[52] Basis responded that it uses standard security practices for channels between the device and the phone and the phone and any servers. Bellabeat proclaimed ”[p]ersonal data transmitted on the relation LEAF - smartphone app - web server is secured against all potential attacks.” Fitbit stated it encrypts traffic between its app and website under normals conditions. Finally, Jawbone stated it uses “organizational and technical measures” to prevent unauthorized access, including the use of HTTPS for data transmissions. Jawbone cautions that they – nor any company – cannot totally eliminate security risks.

4.5.5 BLUETOOTH SECURITY

Can you describe in more detail what practices you’ve implemented to ensure Bluetooth data transmissions are privacy-protective?

Apple did not directly address the Bluetooth security of Apple Watch in its response. This might be because we did not mention the Apple Watch by name in our PIPEDA request letter, and simply referred to the company’s “fitness tracking device”. Apple, in its response, stated “we have no knowledge of your fitness band and would like to point out that Apple does not make such a product. [...] Perhaps your reference is to the Apple Watch [...]”. Basis stated that data is only transmitted to a mobile phone that the Peak has been paired with, and that pairing requires user interaction and physical control of both the Peak and the mobile phone. Fitbit’s reply confirmed our technical findings, that “transmission[s] between the tracker and the site is encrypted end-to-end, meaning that the mobile device proxying this traffic is unable to read the data.” Bellabeat responded that they “change the private addresses of the LEAF devices on a weekly basis,” which we take to mean that the LEAF’s Bluetooth MAC address is changed weekly, in contrast to our technical findings showing the LEAF’s MAC address to be fixed. Jawbone states that “all band data is sent over an encrypted channel.”

[52] Apple. iCloud security and privacy overview. Retrieved from: `https://support.apple.com/en-gb/HT202303`.

4.6 CONCLUSION

In summary, Garmin, Withings, Mio, and Xiaomi did not respond at all to individuals' requests for access to their personal information within the legally-prescribed timeframe. Given these companies' products were purchased within Canada, the companies certainly have a commercial presence in the country. Therefore, as they have not responded to legal requests for access, the companies appear to be in violation of Section 4.9 of PIPEDA.

Apple, Basis, Bellabeat, Jawbone, and Fitbit's responses to access requests varied considerably in the security and identity verification approaches taken, the level of detail of the responses to questions, and how actual raw personal information was made available to requesters, if at all. Bellabeat notably made two troubling statements: One, that its device is secured against all possible attacks, which contradicts common guidance that nothing is ever entirely secure; and two, that it changes the private address of its fitness wearable every week, which we were unable to confirm based on our laboratory tests.

In the next section, we turn to a synthesis of the data received through the PIPEDA access requests with the data types described in our earlier policy and technical sections.

5 DATA EXPECTATIONS VERSUS REALITY

Section 2, 3, and 4 described the methodologies and results of our three analytic approaches to assessing fitness tracker privacy and security. Our technical findings detailed the types of data we observed to be transmitted to fitness tracker servers and highlighted several security vulnerabilities. Our policy analyses revealed varying definitions of personal information, procedures for users, and claims about data privacy and confidentiality. Finally, our analyses of company responses to our research participants' PIPEDA access requests described the variation in how (and if) companies responded to Canadians exercising their privacy rights.

This section presents notable findings from our comparison of the results of our three methods. First, we compare what security measures we observed to be in place for fitness trackers with company claims about security made in policy documents or in responses to PIPEDA access requests. Next, we identify several categories of personal information that we observed to be transmitted to fitness tracker companies, but were unavailable for participants to access through a PIPEDA request or through a company data export tool.

5.1 SECURITY ON PAPER AND IN PRACTICE

Several fitness tracking companies exhibited a disparity between the data security approaches described in policy documents, included in responses to PIPEDA access requests, and observed in network analysis. In particular, claims about reasonable security mechanisms in policy documents were contrasted with a failure to implement standard industry practices in some cases. Table 9 presents a comparison between company claims and technical observations about data security.

In Garmin's privacy policy, the company wrote that it employed "reasonable" measures to protect user personal information. While we found Garmin's privacy policy to not consider fitness activity data as personal information, we found that both activity data as well as profile information such as name, height, weight, age, and gender, were all transmitted with no transit-level security. The consequence was that such data was accessible for collection by third parties with network privilege. Securing such transmissions is, in our opinion, a reasonable measure to protect personal information.

Withings did not specifically mention the security of data in transit in its privacy policy. We could not obtain additional information about the company's security claims and policies given that the company (like Garmin) failed to respond to our participant's PIPEDA request. Withings did however, mention that their servers apply "the optimum level of security". The security of personal data is only as strong as its weakest link and given that we found sub-optimal security levels in Withings mobile application (described in Sectionrefsec:security) we do not concur that the chain of custody of personal data in the Withings data ecosystem could be accurately described as “optimum”.

We found another notable case of a disparity between corporate claims and technical observations in Bellabeat. In its PIPEDA response, the company claims that personal data “is secured against all potential attacks”. This statement contrasted with our technical observations; we discovered that Bellabeat failed to serve its password reset link over HTTPS, leaving end users vulnerable to man-in-the-middle attacks that could steal user credentials. A similar contrast was evidenced in Bellabeat’s privacy policy, which much more conservatively asserts that it “cannot guarantee” that its security measures will stop “so-called hackers” from accessing personal data. Such a disparity between official policy and company responses to individual’s access inquiries could confuse consumers about the extent to which a company protects the personal data under its control.

5.2 THE COLLECTION-ACCESS GAP

In all applications for which we observed data collection, we found personal information that was sent over the Internet and was not subsequently available for access by our participants – either through a PIPEDA request letter or a data export tool.

Save for a single fitness wearable company, Xiaomi, the companies we investigated either responded to our participants’ PIPEDA access request or provided a data export tool as part of their service. However, only Apple, Fitbit and Basis both provided data in their PIPEDA request responses and also included a free data export tool. Jawbone did not provide any raw data in its response but advised the requester to use their data export tool. Withings and Garmin offered a data export tool, but did not reply to our participants’ PIPEDA requests.

However, in many cases, we observed that the data available through export tools was less detailed or comprehensive than the data we observed being sent over the Internet. Table 10 highlights some examples of classes of personal data we observed to be transmitted to fitness wearable servers that were subsequently inaccessible either through PIPEDA requests of data export tools.

Notably, while Jawbone provided both a data export tool and responded to our participant’s PIPEDA request, the company did not provide any access to the detailed geolocation information we observed it to be collection (as described in Section 2.3). Withings did not respond to an access request but did not include geolocation information in its data export tool. Jawbone furthermore did not provide any response or mention our participants’ explicit question in their PIPEDA request regarding geolocation information. That such detailed and routinely-collected personal data is seemingly ignored by Jawbone in both its data export tool and legal response to a citizen access request is an example of inadequate handling of personal information with respect to access rights. Given that Withings did not respond at all to our access request indi-

Company	Security Statement(s)	Notes
Apple	Approach to Privacy (via PIPEDA Response): “[D]ata in the Health app and your Health data on Apple watch are encrypted with keys protected by your passcode.”	Data export only available on phone itself. No health data was provided in response to PIPEDA request.
Basis	Privacy Policy: “We have implemented reasonable security measures in order to protect the information we collect”	Used transit encryption. Certificate encryption employed.
Bellabeat	Privacy Policy: “[C]annot guarantee that our security measures will prevent third-parties such as so-called hackers from illegally obtaining access to personal data.”PIPEDA Response: “Personal data [...] is secured against all potential attacks”	Emailed password reset link vulnerable to MITM. The application did not use certificate pinning.
Fitbit	Privacy Policy: “[A] combination of technical and administrative security controls”	Used transit encryption, fitness data encrypted on wearable itself. Did not use certificate pinning.
Garmin	Privacy Policy: “Garmin takes reasonable security measures to help protect [...] the Personal Information under its control”	Did not use encryption to secure personal data in transit. Did not use certificate pinning.
Jawbone	Privacy Policy: Takes “organizational and technical measures”	Used transit encryption. Did not use certificate pinning.
Mio	–	No data transmitted by app.
Withings	Privacy Policy: “applying the optimum level of security”	Generally used transit encryption. Security hole in “Share my dashboard”. Did not use certificate pinning.
Xiaomi	Privacy Policy: “data is exchanged using SSL”	Used transit encryption. Did not use certificate pinning.

Table 9: Security statements compared to technical observations

cates a general disregard towards responding to Canadians exercising their legal rights.

In general, responding to a PIPEDA access request with a link to a data export tool is not the same as complete access. We have observed multiple instances where unique identifiers such as the MAC address, IP address, and IMEI numbers are transmitted in association with fitness information and other personal information. These unique identifiers ought to be considered personal information by fitness tracking companies given that they are collected at the same time as – and thus associated with – fitness information and basic personal information[53]. We therefore argue that fitness trackers' data export tools generally provide incomplete access to personal information and that companies should respond more fully to PIPEDA requests by carefully developing a complete inventory of the personal information under their control, and either update their data export tools to include this information, or provide as a supplementary resource to the data export tool to citizens requesting access to their personal information.

5.3 CONCLUSION

We observed two major types of gaps between what fitness tracking companies say they do and what actually happens when it comes to their customers' personal data. Generic security claims hid the reality that two applications exhibited serious problems in maintaining the confidentiality of personal information in transit over the internet. Several different categories of sensitive information, often in the form of unique identifiers that could link fitness and biographical data to a single mobile phone hardware or single specific fitness wearable, were ostensibly collected by several fitness tracking companies. However, such identifiers were not necessarily made accessible to consumers upon issuing PIPEDA request or through data export tools. As a result of these inaccurate, or in some cases contradictory findings, consumers may be misled or confused about the actual extent of security measures in place or breadth of personal data collected by fitness tracking companies.

[53] Similar to the Office of the Privacy Commissioner's findings here: https://www.priv.gc.ca/cf-dc/2005/315_20050809_03_e.asp

Company	Inaccessible personal information	Defined as personal information in policy?	Notes from PIPEDA response
Basis	IP address	Explicitly defined as Non-Personally Identifiable Information	Claims to not collect IP address
Bellabeat	Menstrual cycle data, pregnancy status	Policy describes date of period, pregnancy status as “personal health information”	No data provided
Fitbit	Wearable MAC address	Unclear based on company privacy policy.	Not mentioned
Garmin	Wearable MAC address, IP address	IP address is explicitly defined as Non-Personally Identifiable Information. Unclear how company defines MAC addresses.	No access provided
Jawbone	Geolocation, contacts’ email, Wearable MAC address, IP address	Company does not have a definition for Personally Identifiable Information.	Response included link to data export tool
Withings	Geolocation, contacts’ email, Wearable MAC address, IP address	Ambiguous, but likely defined as Personally Identifiable Information	No access provided
Xiaomi	IMEI number, Wearable MAC address, IP address, basic personal information, step count / time.	Defined as Personally Identifiable Information, with the exception of the wearable’s MAC address, which is not clearly defined.	No access provided

Table 10: Personal data observed to be collected for which participants could not obtain access.

6 RECOMMENDATIONS AND BEST PRACTICES

This report has examined the extent to which consumer fitness wearables technically transfer and secure data, the policy processes that companies publish concerning the devices and associated services, and companies' respective compliance with PIPEDA requests. In this section, we provide a set of recommendations for how companies could best secure data, explain company practices to end users, as well as maximally comply with PIPEDA requests.

Our recommendations may not be applicable to all companies' products but, generally, will apply to the majority of companies and their associated programs. Such recommendations are often drawn from either a single company's practices, or a synthesis of companies' practices, and thus may stand in excess of existing industry general practices. This section is divided between technical, policy, and PIPEDA-based suggestions for companies, and concludes with a brief discussion concerning how Canadian government bodies might better clarify the obligations or expectations that fitness wearable companies should meet to provide products that possess adequate privacy safeguards.

6.1 TECHNICAL RECOMMENDATIONS

In the course of our technical analyses of fitness wearables and their companion applications we encountered security issues associated with data transmissions between mobile applications and fitness tracker companies' servers, data tampering vulnerabilities, and privacy concerns associated with Bluetooth.

6.1.1 ADOPT HTTPS AND CERTIFICATE PINNING

Fitness wearables and their companion applications collect, and transmit, large volumes of personal information. And in some cases that data is either sent without encrypting data in transit or in a manner where cryptographic certificates are used to let third parties access data in transit. The result is that personal information may be being collected and transmitted by fitness wearable companies in insecure ways.

We recommend that companies employ transit-level encryption for all of their Internet communications to ensure that no personal data is left unprotected in transit. We further recommend that companies implement certificate pinning in their companion applications to inhibit third parties from inappropriately circumventing the protections offered by HTTPS. Neither HTTPS nor certificate pinning will fully secure fitness content from third parties but doing so will significantly reduce the likelihood that individuals' information may be accessed by third parties.

6.1.2 INCLUDE ON-DEVICE ENCRYPTION

Fitness wearable companies that encrypt data payloads prior to transmission from the fitness bands, to be decrypted only after reaching the company's servers, significantly reduces the ability of users to tamper with or modify recorded fitness data. The result is that the integrity of the user's data is more reliable and less likely to have been fraudulently tampered with.

In order to protect the integrity of fitness data we recommend that companies explore methods of securing data to prevent such tampering.

6.1.3 ADOPT AND IMPLEMENT BLUETOOTH LOW ENERGY PRIVACY FEATURES

Only a single company's product, the Apple Watch, implemented Bluetooth LE (BLE) privacy and thus prevented third parties from tracking the fitness device's location using scanning equipment placed throughout the built infrastructure. In some cases, companies expressed interest in implementing BLE privacy but noted that the varying support for the protocol in Android devices has prevented them from adopting the privacy-protective protocol. In the absence of adopting BLE users could be inappropriately tracked by third parties where the wearable is temporarily delinked from it associated companion application on a mobile device.

We recommend that, where possible, all fitness wearables be developed / updated with firmware that implements LE privacy and thus changes its MAC address at a regular interval (eg: every ten minutes). Fitness wearable firmware will need to include a fixed, private Identity Resolving Key (IRK), that is exchanged with the mobile phone with which it is paired. The wearable's firmware will then regularly generates a new MAC address based on its IRK, and the MAC address can only be resolved to the wearable by another device that has stored the IRK and has functionality enabling its resolution. This functionality is available to devices that properly implement Bluetooth Low Energy (Bluetooth 4.0 or later), which according to developer documentation includes iPhones running iOS 6[54] or later and Android devices running Android 4.3 or later.[55]

6.1.4 PROVIDE A SECURE METHOD TO COMMUNICATE SECURITY ISSUES

Our attempts to establish secure lines of communication with technical security staff at fitness wearable companies were often met with frustration. Most companies did not include a dedicated security contact on their websites. We instead resorted to contacting the email addresses listed on company privacy policies, asking to be connected with a security staff member who

[54] iOS Developer Library. About Core Bluetooth.
`https://developer.apple.com/library/ios/documentation/NetworkingInternetWeb/Conceptual/CoreBluetooth_concepts/AboutCoreBluetooth/Introduction.html`.

[55] Android Developers. Bluetooth Low Energy.
`http://developer.android.com/guide/topics/connectivity/bluetooth-le.html`

could communicate over PGP encrypted email. We did not wish to risk the capture of sensitive information about security vulnerabilities by communicating over an insecure channel. We were eventually able to establish encrypted communications with the companies that responded to our inquiries.

To make it easy for researchers to report security problems with fitness wearable applications, companies should publicize the contact information of a member of their security team, and link to that contact's PGP public key alongside the email address. Another option would be to publish a secure website in which researchers can report bugs in a standardized manner. Fitbit is the only company we found to employ this approach. Fitbit also offers a bug bounty program[56], which could similarly be employed by other fitness wearable companies.

6.2 CORPORATE POLICY RECOMMENDATIONS

When we evaluated corporate privacy policies and terms of service/use documents it became apparent that companies often did not present information in clear or direct ways. Moreover, certain kinds of information that might be most interesting to individuals was lacking. Recommendations in this section focus on making some policy decisions more transparent as well as improving the actual presentation of information so users can better make use of the corporate documentation.

6.2.1 APPLICATION STORES SHOULD INCLUDES LINKS TO RELEVANT PRIVACY POLICIES

While most companies include a link to a privacy policy in the mobile applications stores from which users download companion apps for their fitness wearables, this is not universally the case. Moreover, sometimes the links in the application stores present information that is different from privacy policy information available on company websites. The result is that users who are interested in companies' privacy policies may be unable to find the most accurate ones for the fitness wearables they have purchased.

We recommend that all companies include links to privacy policies associated with their wearable devices and companion applications.

6.2.2 DEVELOP SPECIFIC POLICIES FOR EACH SYSTEM

Companies often aggregate all of their privacy policies and terms of service into a single page or document, which is available either through a link of mobile application download pages or

[56] A bug bounty is a financial incentive that rewards the responsible disclosure of security issues to companies. Fitbit uses the bug bounty platform "Bugcrowd", found here: `https://bugcrowd.com/fitbit`.

on company websites. Doing so, however, can limit individuals' understanding of what information is collected, processes, retained, or disclosed as part of using the wearable device and companion application in question.

We recommend that companies develop, and highlight, device and companion application-specific privacy policies and terms of service/use documents. Doing so will let individuals understand company data practices at a granular level, instead of having to subsequently divine whether certain collection policies are associated with website visitation, or using wearable devices, or is associated with a separate company product or initiative.

6.2.3 DETAIL COMPLAINT PROCESSES

Many companies discuss the jurisdictions in which complaints must be made, or the arbitration systems that must be used, when customers have an issue with a company's given products. Given that many of these companies are attempting to force individuals to take action outside of their own jurisdictions, companies ought to provide high levels of detail to explain how formal complaints can actually be brought. Moreover, companies ought to explain the extent to which arbitration requirements impact Canadians' own rights to file complaints concerning corporate practices.

Therefore, we recommend that companies be explicit with regards to how formal complaints must be brought against the company and outline the extent to which arbitration clauses affect Canadians' abilities to exercise their rights under Canadian law.

6.2.4 DETAIL DATA RETENTION AND ACCESS RIGHTS

Some fitness tracker companies do not state for how long data is retained after being collected or for how long they retain data after a user has either stopped using the services offered by the company or deleted their account. This prevents users from knowing how much of their data to which they might be able to request access, as well as stopping them from knowing for how long they can try and get access/copies of their data after leaving the service.

We recommend that companies provide explicit data inventories of all the personal and non-personal information that is collected and which pertains to specific users, and how long each of these data items are retained. Moreover, companies should disclose how long it takes for a company to entirely purge a user's data from their infrastructure after the user deletes/closes their account(s) with the company in question.

6.2.5 DEFINE FITNESS INFORMATION AS PERSONAL DATA

Few companies explicitly assert that the fitness data collected by wearable devices constitutes personal information; the result is that individuals may believe that the company safeguards or values such data in a diminished way as compared to financial or directly bibliographic information.

We recommend that fitness wearable companies explicitly define fitness data as personal information on the basis that it reveals biological and fitness characteristics pertaining to an individual with whom the company can associate the data. Moreover, such data can be incredible revealing should it be associated with geolocational, mood, diary, food, or other data that in aggregate could reveal either mental characteristics or increase the ability of the company or other third party to geolocate the user based on their fitness entries. The result is that fitness data should be as strongly protected as financial information or other kinds of data that the company regards as highly sensitive information pertaining to an identified or identifiable person.

6.2.6 CLARIFY WHAT DATA IS SHARED WITH WHAT THIRD PARTIES

Most fitness wearable companies rely on third party data processing for at least some of their functionality, but it is rarely clear from companies' privacy policies or terms of use/service documents which companies are responsible for which processing activities. The result is that users cannot ascertain whether third parties are processing email, website analytics, or more sensitive activities such as analyzing health and fitness data, or processing complaints.

We recommend that fitness companies update their privacy policies and terms of service to be explicit about what kinds of data processing third parties are being contracted to perform, and to identify the specific organizations that are responsible for such processing. The result would be to enhance transparency into existing corporate practices and clarify for users how different kinds of data are being handled on their behalf by wearable companies and their contracted agents.

6.2.7 EXPLAIN DISCLOSURES WITH GOVERNMENT AGENCIES

Fitness wearable companies' online documentation routinely asserts that respective companies may disclose users' information to government agencies, but few provide details on the specific situations under which such disclosures might be required or the policies that the companies have established to ensure only appropriate disclosures take place.

We recommend that wearable companies publish law enforcement guideline handbooks that discuss the kinds of legal orders that might be served on a given company, how the company responds to such orders, and the specific data items that might be disclosed under each kind of order. Such handbooks are already published by many leading information technology companies and thus templates for how to develop these handbooks could be adopted from pre-existing sources.

6.2.8 DATA SECURITY AND STORAGE

Companies provide generalized statements concerning data security, such as “reasonable security measures” are adopted. Few users, however, will understand what constitute reasonable or unreasonable security measure. As such, companies should be more specific about how they secure their users’ data.

We recommend that companies explicitly state how they secure their data collection practices, data that is in transit between devices and company servers, data being processed by third-parties, and how data is secured at rest or in company facilities. Moreover, companies should be explicit in identifying to whom data processing or storage is outsourced, as well as the jurisdiction(s) in which a user’s data is kept.

6.2.9 PROVIDE COMPREHENSIVE DATA INVENTORIES

Privacy policies routinely discuss how ‘identifiable data’ may be collected but the specificity of the precise data items collected vary significantly across companies. The result is that while individuals may have a rough understanding of the range of data that is collected about them, they are unlikely to understand the full range of identifiers or personal information data points that are collected by the fitness tracking company.

We recommend that companies include, as part of their privacy policies, full data inventories of the identifiers and other user-related information that is collected by the company, and accompany each identifier with an example of what the identifier would look like, and the period of time for which the identifier(s) is retained by the company or third-party that processes the data on the company’s behalf.

6.2.10 DATA BREACH NOTIFICATION

Several companies assure users they will strive to secure user data while, at the same time, admitting that they cannot guarantee that data will never be accessed by an unauthorized third party. These companies do not state they will alert users of such an unauthorized access. The result is that users are storing personal data with companies that may have already suffered a data breach, or that may suffer one in the future, and not necessarily be informed that their personal data has been inappropriately accessed.

We recommend that companies adopt data breach notification policies and declare their existence in companies’ privacy policy. Without such proactive requirements in the privacy policies companies may only notify small subsets of users who must be notified under relevant data breach legislation in the United States, and thus leave most users ignorant of whether their data has been accessed by an unauthorized party.

6.2.11 ENSHRINE RIGHT OF ACCESS TO DATA

While some companies explicitly note that individuals enjoy a right to access and export their data, this isn't universally true. The result is that user data are locked into some services per their policy language.

We recommend that companies formally include a statement that users have a right to access and export their data at no or a minimal cost. Such data should be exported in a structured format so that it can be repurposed as the user sees fit, and fees should not be bound to premium services or service offerings from the company. Ideally companies should let individuals simply download or export their data for free. This data should not solely be limited to fitness data, but include all the personal information retained by companies, such as IP addresses, MAC addresses, other device identifiers, friends' contacts, and geolocation records.

6.3 PIPEDA COMPLIANCE RECOMMENDATIONS AND BEST PRACTICES

In addition to enshrining the right to access data, as recommended above, companies can do more to better respond to individual requests for access. The following recommendations should help all companies provide their customers with a more efficient, thorough, responsive, and secure access to information experience.

6.3.1 RESPOND TO REQUESTS FOR ACCESS

Companies doing business in Canada should comply with Canadian law, and respond to access requests within the mandated time frame. While Apple, Basis, Jawbone, Bellabeat, and Fitbit responded, Mio, Withings, Garmin, and Xiaomi did not. All non-responsive companies have a significant business presence in Canada (with Mio being a Canadian company) and therefore they are subject to the access provisions of PIPEDA.

We thus recommend that the counsel for fitness wearable companies educate themselves as to their organizations' obligations under Canadian law and follow the guidance issued by Office of the Privacy Commissioner[57] and contained in this report to better comply with the law.

6.3.2 PROVIDE CLEAR ANSWERS

Companies should explicitly address each question posed to them by individuals inquiring about their data. While Bellabeat, Basis, and Fitbit should be commended for answering each question in our participants' letters, Apple and Jawbone only addressed some of the issues raised in the requests, and did not mention that they had omitted responses to some other questions.

[57] See, for example: Office of the Privacy Commissioner of Canada (2015). Privacy Toolkit: A Guide for Businesses and Organizations. https://www.priv.gc.ca/information/pub/guide_org_e.asp#s209

We recommend that companies should provide complete responses concerning data handling activities when a customer poses them to a given company. Moreover, where no answer can be provided to a particular question the reason for the non-response should be provided.

6.3.3 INCLUDE A DEDICATED PRIVACY CONTACT

Companies should have a dedicated email listed on their privacy policy to handle privacy and access inquiries. In many cases, we observed companies including generic contact email addresses or forms listed on their policies. These email addresses led to customer service departments and often required several layers of forwarded emails before the right contact at the organization received the request. PIPEDA specifies that companies should have a dedicated privacy contact.[58]

We recommend that fitness tracking companies include contact information in their policy documents to become more responsive to customer privacy and access questions. Moreover, this privacy contact should offer secure (e.g. HTTPS contact form, or PGP encryption) means for customers to send and receive requests from the dedicated company privacy experts or counsel.

6.3.4 PROVIDE SECURE AND USABLE ACCESS

Companies should ensure that the method by which they provide access to personal information is both secure and user-friendly. While requiring users to create a PGP keypair and send a public key to a company is a highly secure method in theory, however PGP is notoriously difficult to useSee, for example: Whitten, A., Tygar, J. D. (1999, August). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In Usenix Security (Vol. 1999). `https://www.usenix.org/legacy/events/sec99/full_papers/whitten/whitten.ps`, and presents an unnecessary barrier to access. Links to data export tools, served with transit-level encryption and requiring user authentication, are a good method, however, these tools must provide complete access to all personal information, not just fitness data.

We recommend that companies offer both communications encryption to communicate with users as well as technically accessible-means to communicate with the organization. Doing anything less means that individuals may be forced to receive copies of their information in insecure ways that could expose them to risks should a third party intercept the communications in question.

[58] *ibid*

6.4 THE FEDERAL GOVERNMENT'S ROLE

As discussed in Section 1, the United States government has asserted that data collected from wearable devices is not classified as 'health' data and, thus, companies do not have to meet HIPPA compliance when collecting, processing, or disclosing data to other parties. In contrast, the European Data Protection Supervisor (EDPS) has stated that 'lifestyle' information associated with fitness trackers constitutes personal information when the collected data enables inferences about a person's health. This is the case, "especially when the purpose of the application is to monitor health or well-being of the individual (whether in a medical context or otherwise)." [59] This, in effect, means that the EDPS precludes fitness companies from asserting the information collected in the course of providing a product is non-personal data and, consequently, a higher-than-otherwise-normal level of data security must be afforded to fitness data in the European Union.

Arguably the information collected by fitness companies will largely be defined as personal information under Canadian commercial privacy legislation. Per section 2(1) of the Personal Information and Electronic Documents Act (PIPEDA) personal information includes "information about an identifiable individual." PIPEDA itself applies to every organization that gathers personal information in course of commercial activities, or where the information is "about an employee of, or an applicant for employment with, the organizations and that organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business." Such information must be about a specific individual, and thus not just 'about' something pertaining to an individual; effectively there must be demonstrable links between the information and the person in question. Moreover, information might belong to a set of people simultaneously; an example might include genetic information that pertains a person and their family more generally.

The Office of the Privacy Commissioner of Canada has yet to provide specific guidance for fitness tracking companies. The Office has written in a report 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." [60] The authors of the report explain that advice provided in OPC reports concerning mobile application developers, gaming consoles, and online behavioural advertising "are relevant in the context of wearable computing as well." [61] However, OPC has stated it will be providing guidance regarding digital health

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

[60] 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`.

[61] *ibid*

technologies in the near future[62], and we hope that our recommendations will be considered in such guidance.

In our assessment of separate OPC guidance concerning 'what is personal information' under federal privacy legislation, we find a series of analogous types of data collection where the data collected is by definition personal.[63] To begin, in the health context personal information "that has been de-identified does not qualify as anonymous information if there is a serious possibility of linking the de-identified data back to an identifiable individual." On this basis, information that fitness wearable companies claim is 'de-anonymized' may still actually be considered personal data unless they actively affect the data such that no person can be re-identified as a result of gaining access to the 'anonymous' data set.[64] Moreover, while many companies fail to explicitly assert that fitness data constitutes personal information, these analogous examples of past activities examined by the OPC suggest that some of these companies' activities entail collecting, retaining, and processing personal data.

Where surveillance captures an individual's physical image or movement it is implicated in collecting personal information, even if the capturing is not recorded.[65] Fitness wearables are clearly collecting the information associated with individuals' movement and, thus, are involved in the collection of personal information. Moreover, information collected pertaining to geolocation – be it by GPS[66] or localized RFID tag[67] – constitutes personal information as well. And given that some applications are involved in the granular collection of a user's geolocation the applications and associated wearables are involved in the capture of personal information. Furthermore, the collection of Internet Protocol (IP) addresses is considered personal information if it can be associated with an identifiable individual;[68] given the fitness wearable compa-

[62] Office of the Privacy Commissioner of Canada (2015). The OPC Strategic Privacy Priorities 2015-2020. Available at https://www.priv.gc.ca/information/pub/pp_2015_e.asp

[63] Office of the Privacy Commissioner of Canada. (2015). "Legal information related to PIPEDA," Office of the Privacy Commissioner of Canada, December 11, 2015, retrieved March 21, 2016, https://www.priv.gc.ca/leg_c/interpretations_02_e.asp.

[64] Office of the Privacy Commissioner of Canada. (2009). " PIPEDA Case Summary 2009-018: Psychologist's anonymized peer review notes are the personal information of the patient," Office of the Privacy Commissioner of Canada, February 23, 2009, retrieved March 21, 2016, https://www.priv.gc.ca/cf-dc/2009/2009_018_0223_e.asp.

[65] Office of the Privacy Commissioner of Canada. (2006). "PIPEDA Case Summary 2006-360: Bank erroneously e-mails employees' personal information to client," Office of the Privacy Commissioner of Canada, November 14, 2006, retrieved March 21, 2016, https://www.priv.gc.ca/cf-dc/2006/360_20061114_e.asp.

[66] Office of the Privacy Commissioner of Canada. (2006). "PIPEDA Case Summary 2006-351: Use of personal information collected by Global Positioning System considered," Office of the Privacy Commissioner of Canada, November 9, 2006, retrieved March 21, 2016, https://www.priv.gc.ca/cf-dc/2006/351_20061109_e.asp.

[67] Office of the Privacy Commissioner of Canada. (2008). "Radio Frequency Identification (RFID) in the Workplace: A Consultation Paper on Recommendations for Good Practices," Office of the Privacy Commissioner of Canada, March 2008, retrieved March 21, 2016, https://www.priv.gc.ca/information/research-recherche/consultations/2008/rfid_e.asp.

[68] Office of the Privacy Commissioner of Canada. (2005). "PIPEDA Case Summary 2005-315: Web-centred

nies collect IP addresses at the same time as they are collecting other personal information, including billing, biographic, and uniquely-associated fitness data, then these companies' collection of IP address information should be considered 'personal information', even if a given company can only associate personal information with the IP address briefly.

When OPC develops formal, industry specific, guidance for developing fitness wearables such that companies understand the full contours of their obligations under Canadian law, then this may lead to clearer privacy policies that are responsive to domestic federal legislation. Moreover, specific guidance might help companies understand their need to respond to Canadians' requests to access their data under PIPEDA. Consequently, we recommend that OPC's forthcoming guidance on emerging digital health technoglogies include the following:

- Clarify what kinds of common data identifiers, and classes of data which are collected by fitness companies, are considered personal information under Canadian law;
- Outline why companies should include data inventories of their applications so that individuals can determine what precise kinds of data might be being collected; and
- Offer comments concerning the extent to which IP addresses and geolocation information constitution personal information.

The goal of this would be to encourage business and industry to develop relatively explicit policies that communicate the kinds of information the companies collect, and specifying which is private information per Canadian law, the means by which individuals can subsequently access such information, and the practices that are explicitly put in place to retain and process the data.

6.5 CONCLUSION

Many of the companies that we examined were principally based in the United States. As such, they may not be fully aware of their privacy obligations under Canadian law. However, even when setting specific Canadian law issues aside, companies should adopt technical solutions

company's safeguards and handling of access request and privacy complaint questioned," Office of the Privacy Commissioner of Canada, August 9, 2005, retrieved March 21, 2016, https://www.priv.gc.ca/cf-dc/2005/315_20050809_03_e.asp; Office of the Privacy Commissioner of Canada. (2009). "PIPEDA Case Summary 2009-010: Report of Findings Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection," Office of the Privacy Commissioner of Canada, August 13, 2009, retrieved March 21, 2016, https://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.asp; Office of the Privacy Commissioner of Canada. (2005). "PIPEDA Case Summary 2005-319: ISP's anti-spam measures questioned," Office of the Privacy Commissioner of Canada, November 8, 2005, retrieved March 21, 2016, https://www.priv.gc.ca/cf-dc/2005/319_20051103_e.asp.

that universally increase the protection afforded to end users. Moreover, updating policy documents to clarify how users' information is collected, processed, analyzed, retained, and disclosed will let all of a given company's users better appreciate the controls that the company asserts over the information in its possession.

A core concern that individuals have stated in past studies[69] is that information, once provided to fitness wearable companies, is difficult to comprehensively extract from the companies. Moreover, the terms under which data might be shared are often regarded as unclear by users; we found that while it was often explicit how and why companies could share information, that the core problem was that it could be shared in the first place, and often without the end user's awareness. Companies should be more explicit about the relative lack of rights individuals have to their data once providing it to a fitness wearable company.

While companies might, in some instances, be excused for not entirely understanding their obligations under PIPEDA, this should not permanently excuse their limited responses. Companies should commit to responding to all of their customers' questions regardless of where they are from. At the very least this should mean that companies fully respond to specific questions that are put to them (e.g. does a company share information with insurance companies or other third parties) and, ideally, respond comprehensively as required to under the requesters' domestic law.

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

7 CONCLUSION

Fitness tracking devices collect a wide range of personal information, usually transmit it to servers controlled by fitness tracking companies, and provide widely varying levels of both data security and responsiveness to Canadians' right to information requests. In some notable cases, we discovered severe security vulnerabilities, incredibly sensitive geolocation transmissions that serve no apparent benefit to the end user, and that were not available to users for access and correction, and unclear policies leaving the door open for the sale of users' fitness data to third parties without express consent of the users.

Our report has described the current landscape of the fitness tracking industry, compiled consumers' worries about location tracking and third party access to fitness data, and identified current policy questions surrounding the trackers. We examined fitness trackers technically, finding that transit-level security was not adequately employed for two trackers, that fitness data can be falsified in many cases, and that most fitness wearables emit a trackable unique identifier. We found that fitness data is often not treated as personal data by companies. We looked at how companies responded to Canadians exercising their right to information and found that companies did not provide access to some of the personal data we observed to be collected. Finally, we provided several recommendations to fitness wearable companies, in the hope that they can adopt as many of them as possible to enhance the privacy and security of their consumers.

We hope that the findings described in this report can assist regulators in Canada and around the world as they grapple with emerging privacy issues associated with the Internet of Things. Fitness data is sensitive data about one's body, and just one example of how data-collecting technologies are growing more and more ubiquitous in our most intimate spaces. It is important that we address privacy and security issues now, at the cusp of this trend's emergence, so that future generations of products, policies, and regulations can benefit from informed discussions about these devices' data practices.