NTNU
Norwegian University of
Science and Technology

Privacy Leakage in Fitness Equipment Communication

Benedicte Væting Svenskerud

Master of Science in Communication Technology
Submission date: March 2018
Supervisor: Stig Frode Mjølsnes, IIK
Co-supervisor: Øivind Kure, Universitetet i Oslo, UiO

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Title:	Privacy Leakage in Fitness Equipment Communication
Student:	Benedicte Væting Svenskerud

Problem description:

Fitness trackers and wearables are getting increasingly popular as an aid to monitor general activity and physical exercise. The common goal for all these systems is to collect user metrics and sensor data in order to present some physical performance analysis, such as calorie consumption, distance tracking or sleep quality. The data measured through typical fitness trackers is step count, heart rate and GPS location. The users of these devices span in both age and ambition, from professional athletes to elderly people.

In addition to the wearables, device manufacturers usually provides smart phone applications for the user to track the activity and view analysis reports. Most manufacturers also provides connectivity to large online communities for sharing personal activity metrics with other users. When using fitness tracker applications with online connectivity, the user agreements may not be transparent with respect to the extend of personal data exchanged to global servers.

This master thesis will investigate the data flow from personal fitness trackers through manufacturer applications and online communities. The findings will be evaluated with respect to of the respective manufacturer application user agreements, and discussed in context of privacy leakage. The thesis will also try to identify potential relay of user data from the manufacturers to third parties.

Supervisor:	Stig Frode Mjølsnes, IIK
Co-supervisor:	Øivind Kure, UiO

Abstract

The technology is constantly evolving with use of personal data as a central component of new applications and services. At the same time, physical activity has become an important part of the modern society. This has led to an increased use of wearable fitness devices, as a common accessory for both professional athletes and regular people. These devices help people track their health and activity progression, as well as it serves as a motivational factor. The wearable fitness devices are usually connected to a smartphone through an application provided by the manufacturer. Through these apps, a user can review historical activity data and plan future sessions. The data is also often made available through the manufacturer's website, but this requires login. When using these devices and services, one may ask whether users accept the terms of use without knowing the details of how the personal information is handled.

This thesis investigates privacy leakage by identifying where data is shared from the applications to other destinations on the Internet. It also examines the active tracking mechanisms used on the manufacturer's websites. The study evaluates three major manufacturers of wearable fitness devices. The test results are discussed with respect to the privacy policies of the companies. I have defined the following research questions for the thesis:

1. Is the information provided by the manufacturers sufficient for the users to fully understand the extent of the data sharing?
2. Are there any undisclosed parties that receive information about the users?
3. What incentives do the manufacturers have for collecting user data?
4. How is the distribution of responsibility for handling the personal data in question?

The result shows that multiple third parties receives data from both the applications and the websites. Further, their privacy policies do not give sufficient information about who is receiving the data or for what purpose. In general, the policies are vague and hard to understand for a regular user. This shows that there is a need for better regulation in the future, to ensure that all parties responsible for processing of personal data are forced to improve their operations.

Sammendrag

Det gjøres stadig store teknologiske fremskritt i dagens samfunn, hvor personlig data i økende grad er forankret i nye applikasjoner og tjenester. Trening og fysisk aktivitet har samtidig blitt satt mer i fokus. Dette har medført at aktivitetsbånd og smartklokker har blitt et vanlig tilbehør, både for den mest aktive, men også for den vanlige mosjonisten. Effekten av hjelpemidlene gjør treningen mer målbar og motiverende. For å få best utbytte av produktet, må man benytte seg av en tilhørende applikasjon for å koble enheten til en smarttelefon. Dette gjør det mulig å se historisk treningsdata, samt planlegge fremtidig aktivitet. Dataen blir også ofte tilgjengelig på en nettside som krever innlogging. Man kan stille seg spørrende til om man, ved bruk av disse hjelpemidlene, samtykker til å gi fra seg personlig informasjon om egen helse under ensidige og uklare vilkår.

Denne oppgangen undersøker deling av brukerinformasjon ved å identifisere mottakere av nettverkstrafikk fra applikasjonene og hvilke aktører som har aktive sporingsmekanismer på produsentenes hjemmesider. Studiet tar for seg tre ulike produsenter av aktivitetsmålere, hvor testresultatene diskuteres i lys av deres personvernerklæringer. For å undersøke om informasjon deles til tredjepart, og hvor mye informasjon brukerene har tilgang til om dette, har jeg utformet følgende problemstillinger:

1. Er informasjonen som er gjort tilgjengelig av produsentene tilstrekkelig for at brukerne forstår omfanget av informasjonsdeling?
2. Eksisterer det mottakere av brukerinformasjon som det ikke har blitt opplyst om?
3. Hvilke insentiver har produsentene for å samle data om brukerne?
4. Hvilket ansvar har de ulike aktørene som håndterer brukerdataen?

Resulatene fra dette studiet viser først og fremst at det er flere tredjepartaktører som mottar data fra applikasjonene og web-sidene. Personvernerklæringene gir ikke en tydelig indikasjon på hvem disse aktørene er, hvilken type data de mottar eller til hvilket formål. Erklæringene fremstår gjennomgående vanskelige å forstå for en normal bruker. Dette viser at det er et stort behov for nye personvernregler som vil stille større krav til aktører som håndterer personlig data.

Preface

This master thesis concludes my Master of Science Degree at the Norwegian University of Science and Technology (NTNU). My specialization is in the field of Digital Economics at the Department of Information Security and Communication Technology (IIK) at the Faculty of Information Technology and Electrical Engineering (IE).

I would like to thank my supervisor, Øivind Kure, for his contribution and guidance throughout this thesis.

Benedicte Væting Svenskerud
Oslo, March 2018

Contents

List of Figures

List of Tables

Chapter 1
Introduction

Over the last years, exercise and general physical activity have gained greater focus. Throughout these years, it has also been a great development regarding technical fitness equipment. Now, there are many providers of small wearable gadgets which can be used to measure activity. Smart watches and activity bands has now become a common accessory, both for the most fitness-minded and for those who use these tools as a motivation to maintain recommended physical activity. The equipment has some variations to the measured data, some activity bands only register general activity in steps and pulse. Some have built-in Global Positioning System (GPS), whilst other depend on the connected phone's GPS. A common property of all the devices is that they require users to create an account. To gain most benefit of the devices, it is usually accommodated with an application, or web interface provided by the manufacturer. The connected applications and the websites are responsible for handling and presenting the activity sensor data to the user.

The main goal of this thesis is to bring a better understanding to the users about the implications of using wearable fitness trackers which communicates with co-existing applications and websites. This is done by examine various aspects of data sharing, including investigations of the data path of the information sent from the smartphone applications to other locations on the Internet. The different destinations will be evaluated an seen in context with user agreements and public information about data sharing from the respective fitness wearable manufacturers.

The fact that these companies collect and share user data is no secret, but the transparency of which data is shared and to whom is often obfuscated behind vague generic descriptions. Most users are aware of the sharing to some extent, but with the benefit of the doubt, it does not seem to impact the popularity of fitness devices significantly. The trends indicates strong growth in number of sold units. In 2016 it was registered 720,000 sold smart watches and activity bands and in 2017 this number increased to 900,000, reported by the foundation "Elektronikkbransjen" [15].

A possible lack of knowledge and interest to fully comprehend user agreements when using such devices, leaves a large responsibility with the manufacturers to handle the collected data within certain limits of respect and ethics. Where the personal data is shared, and for what purpose, are important and should be information available for the users. If it shows that data is shared to a larger extent than the user have understood to agree, the consequence might lead to distrust and people abandoning the products.

In addition to the bundled apps to the physical fitness devices, several popular third party applications are available on the market, such as Strava. These apps can be used together with a smartphone or with a wearable fitness device. In November 2017, Strava released a map which included visualizations of all tracked activities by the users of the app. Such maps are regularly released and is the basis for a service where users can find new tracks and motivation for their workouts. This map included more that 3 trillion individual GPS data points and stood out as even more detailed than previous [16]. After its release, the map was further examined and it turned out that the details of the map also gives away what might be extremely sensitive information about a subset of users; namely military personnel on active service [16]. The map also made United States (US) military bases identifiable and mappable.

The release of the Strava heat map shows a problematic scenario where soldiers uses wearable fitness equipment in the same manner as "normal" people. As a result of tracking their daily exercise, common areas where the soldiers reside may be known and further utilized by someone with bad intentions. In this case, it looks like the soldiers track their workouts and has certain features enabled without thinking about the implications that follows. Although the map is based on public data, and does not include any personal information, it is possible to visit the service and look up users based on the routes they have run publicly [17]. Strava stated in the aftermath of the map release that they were committed to helping people better understand the app settings, and in this way give users control over what they share. The incident with Strava, shows a good example on how big data analytics may impose a risk.

1.1 Objectives

The goal of this master thesis is to investigate if there is occurrence of privacy leakage for several fitness devices produced by different manufactures. This includes examination of the network traffic from the associated application for a set of different devices. It also includes the same investigation for the websites provided by the developer of the fitness equipment. The possible findings will be discussed in context of the company's privacy policies. More specifically, the main research questions for this thesis are:

1. Is the information provided by the manufacturers sufficient for the users to fully understand the extent of the data sharing?

2. Are there any undisclosed parties that receive information about the users?

3. What incentives do the manufacturers have for collecting user data?

4. How is the distribution of responsibility for handling the personal data in question?

1.2 Scope

The scope of this thesis will be to evaluate the privacy policies issued by the manufacturers of wearable fitness devices. The evaluation includes identifying disclosures regarding data sharing, usage of tracking mechanisms and the purpose of such measures.

This thesis will focus on three well-known manufacturers of wearable fitness equipment, namely, Garmin, Fitbit and Polar. This because they all are large manufacturers which provide devices, applications and a website in a bundle.

The devices and their associated applications will be tested with respect to network traffic and access privileges. Further, the associated websites will be investigated to identify active tracking mechanisms. The findings will be discussed with respect to the information presented in the privacy policies.

1.3 Contribution

The contribution of this thesis is to identify the availability of information about data sharing provided by manufacturers of wearable fitness devices. The test performed will serve as an indication on whether the provided information is valid and sufficient for a user to fully understand the extent and purpose of data sharing. This includes both sensitive personal information as well as aggregated de-identified data. Further, this thesis contributes to the discussion on the motives for collecting big data and the following potential benefits and implications for users. In total, the thesis aims to provide value to both manufacturers and users with respect to rights and responsibilities for those who use the equipment.

1.4 Outline

The thesis is structured into 7 chapters, and the outline is as follows:

- Chapter 1, Introduction: contains the motivation and objectives for the thesis. This also includes the scope and limitations, as well as the contribution.
- Chapter 2, Background: necessary background material for the thesis. This includes a section about privacy in general and on the Internet, an introduction to Internet tracking techologies, and other related work.
- Chapter 3, Privacy Policies: a survey of the privacy policies provided by the manufacturers of the different fitness wearables.
- Chapter 4, Wearable Fitness Devices: This chapter presents the physical wearable fitness devices and their associated applications and websites.
- Chapter 5, Methodology: gives a description of the research methods utilized, challenges that may arise and limitations within the method.
- Chapter 6, Result: This chapter presents the findings retrieved in the experiment. The results are discussed and commented throughout the chapter.
- Chapter 7, Discussion: summarizes and discusses the results found in the thesis.

Chapter 2
Background

This chapter provides an introduction to the background material for the topics discussed throughout this thesis. This will give the reader a better understanding of the concepts and topics discussed in later chapter. The chapter includes an introduction to privacy with associated rules and regulations. There is also a section that gives an overview of existing technologies for online web tracking. The last section in the chapter presents an overview of previous work within the field of privacy leakage.

2.1 Privacy

Privacy if defined in four different ways by the English Dictionary [18]:

1. *the state of being apart from other people or concealed from their view; solitude; seclusion*

2. *the state of being free from unwanted or undue intrusion or disturbance in one's private life or affairs; freedom to be let alone*

3. *freedom from damaging publicity, public scrutiny, secret surveillance, or unauthorized disclosure of one's personal data or information, as by a government, corporation, or individual*

4. the state of being concealed; secrecy:

Although the definition of privacy is clear, privacy itself is a complicated matter and largely depends on the situation in hand.

2.1.1 Privacy on the Internet

On the Internet, the meaning of privacy is as important but may show its face differently. Online privacy involves the ability to control what information a user

reveals and also to control who could access that information. So the privacy on the Internet concerns how a user´s personal data is being protected and is about keeping wanted information from leaving the network. The concept of privacy on the Internet constitutes the protection of an individual's integrity and is recognized as a fundamental human right.

The companies that provide solutions for fitness tracking in one or another way, both in use of the associated app or the web interface, demands the user to register and thereby provide personal information. The information required varies between the manufacturers, but every user who wishes to make use of the offered services must register and create a user account. In addition, the ability to access and review tracked fitness data through a web interface exists. This gives providers of all services, including third parties and affiliates, several opportunities to collect information about their users, namely by using online tracking methods.

Types of Information

Several data classifications exist, and throughout this thesis I will use different terms related to this. Therefore, I feel that it is important to review the different existing categories of information.

Anonymous and Pseudonymous Information The anonymous information, Non-Personally Identifiable Information (Non-PII) includes the following data:

- Analytics
- Browser Information
- Cookie Data
- Date/Time
- Demographic Data
- Hardware/Software Type
- Interaction Data
- Page Views
- Serving Domains

Whilst the pseudonymous information concerns the Internet Protocol (IP) address of the client.

Personally Identifiable Information Personally Identifiable Information (PII) concerns any information relating to an identifies or identifiable natural person ("data subject"); and identifiable person is one who can be identified, directly or indirectly,

in particular by reference to an identifier such as a name, and identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person [19]. Normally PII relates to the following data:

- Name
- Address
- Phone Number
- Email Address
- Login Credentials

2.1.2 Legislative Privacy Rules

In Norway it is the Norwegian Data Protection Authority (DPA) that protects the individual's privacy [20]. The independent body, that is a subordinate to the Ministry of Local Government and Modernization, upholds a number of acts and regulations concerning data protection. Their main legislation that directs their work is however the Personal Data Act (PDA) [21]. Their work is carried out using general information, dialogue, complaints handling and inspection [20]. This to follow up on their means which is to supervise that authorities, companies, organizations and individuals follow data protection legislation [20].

Transfer of Personal Data to Other Countries

When it comes to transferring personal data to other countries, citizens of Norway is protected by the PDA ("Personopplysningsloven") [21] and the Personal Data Regulations (PDR) [22]. The latter is actually the Norwegian implementation of the Data Protection Directive 95/46/EC [23], which was designed to harmonize data privacy laws across Europe. In May, this regulation will be replaced by General Data Protection Regulation (GDPR).

The GDPR [19], defines "cross-border processing" as meaning either:

- processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State

or;

- processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which

substantially affects or is likely to substantially affect data subjects in more than one Member State

2.1.3 The EU General Data Protection Regulation

The European Union (EU) GDPR ("Datasikkerhetsreguleringen") may be looked upon as a new regulation for the digital age. The regulations will be deployed and set active from May 2018. The regulation consists of eleven chapters and lays out rules relating to the protection of natural persons with regard to the processing of personal data. The regulation protects fundamental rights and freedom particularly regarding a person's right to the protection of personal data.

Even though Norway is not part of the EU, Norwegian citizens will be protected by this regulation due to Norway's membership in the European Economic Area (EEA) Agreement ("EØS-avtalen"). The aim of GDPR is to protect all citizens from privacy and data breaches. This is a reaction to the big technological changes that has happened since 1995, when the former directive was established, the society has been undergoing rapid technical development and is now very (and still increasingly) data-driven.

One of the biggest changes may be that the regulation entails extended jurisdiction of the GDPR - it includes all companies processing personal data of subjects residing in the EU [24]. Therefore, it does not only affect companies residing in EU themselves but is independent of the company's location. GDPR will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in EU or not. By the GDPR, a *controller* is defined as [19]:

> *..the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.*

A *processor* is formerly defined as [19]:

> *.. a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*

A *controller* is the party that determines the purposes and means of processing personal data, whilst a *processor* is responsible for the actual processing of the personal data on behalf of the controller [25]. The GDPR places specific legal obligations to these parties. The processor is for instance required to maintain records of personal data and processing activities and if this party is responsible for a breach, it will have legal liability. Involvement of a processor will not relieve the

controller's responsibilities. When a controller is in use of a processor, it is required to have a written contract. The main goal of such a contract is that both parties are in complete understanding of their responsibilities and liabilities. GDPR places further obligations on the controller, one is to make sure that contracts between the controller and processor comply with the rules established by the regulation.

The introduction of GDPR also implies the ability to penalize companies that do not follow the regulations. Organizations in breach can be fined up to 4% of annual global turnover or $20 Million (whichever is greater) [24]. This represent the maximum fine for the most serious infringements defined by the regulation. These rules applies to both controllers and processors, which means that *clouds* will not be an exempt from GDPR enforcement [24].

Also, the conditions for consent is strengthened with the introduction of GDPR. Companies will no longer be able to use long illegible terms and conditions filled with lots of legal text that is hard to understand. In addition to the consent must be as easy to withdraw as to give in the first place, the request for consent *must be given in an intelligible and easily accessible form, using clear and plain language, with the purpose for data processing attached to that consent* [24].

Chapter 3 in the GDPR [19], describes *The Rights of the data subject*. The chapter consists of several fundamental rights regarding privacy on the Internet. Some key rights will be presented here.

Right of Access by the Data Subject The GDPR defines that a data subject has the right to obtain (from the data controller) confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. As a response, the controller must provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency as well as an empowerment of data subjects.

Right to be Forgotten This right is also knows as *Data Erasure*. It entitles the data subject's power when it comes to stored data, because a subject can force the controller to erase his/her personal data, cease further dissemination of the data and potentially have third parties halt processing of the data. The conditions for erasure may be; that the data looses its relevance and therefore, the processing of the data is no longer needed. The right to be forgotten may also be invoked by a data subject if a decision to withdraw consent is made. Further, this right requires controllers to compare subjects' rights to the *public interest in the availability of the data* when considering such requests [26].

Data Portability GDPR also introduces *Data Portability* which deals with the right of a data subject to receive personal data concerning them. The data a subject can claim is the data they have previously provided in a *commonly use and machine readable format* and have the right to transmit that data to another controller.

Privacy by design This design as a concept has existed for many years. Although, the introduction of GDPR is the first time it becomes a part of a legal requirement. Privacy by design means that security measures should be included from the onset of designing a system, rather than being an addition. It also includes that controllers must hold and process only the data absolutely necessary for the completion of its duties, more accurate *data minimization*. The access to personal data should also be limited to those needing it to act out the processing.

Further, the regulation also introduces the duty of appointing Data Protection Officers (DPO) for public authorities or if certain processing activities is performed. The DPO will be responsible for assisting authorities and companies in monitoring and will also function as a regulatory adviser. The DPO will also be the contact point for data subjects and the supervisory authority [27]. The officer must be independent, an expert in data protection, adequately resourced, and report to the highest management level [27].

The requirement for appointing a DPO also include companies where processing is the "core" activity of the business. This also applies the activities including regular and systematic monitoring of individuals on a large scale. Regular and systematic monitoring of data subject means all forms of tracking and profiling, both online and offline, e.g. behavioral advertising [27]. The process of determining if the monitoring happens in large scale, relies on several factors as the number of data subjects concerned, the volume of personal data, the range of different data items, geographical extent of the activity and the duration or permanence of the processing activity [27].

2.2 Tracking Technologies

The reality is that the Internet has made data collection much easier, now traces are left all over the place. And according to the Norwegian DPA, the development is further driven by Internet of Things (IoT) and the growing use of wearable devices such as smart watches and smartphones. As the devices become a part of users daily lives, new ways of tracking methods arise and the data that may be collected has also shifted. Now, geographical location and even health statistics may be collected. However, more conventional tracking mechanisms are utilized online.

The following section will present some of the technologies used to collect information about users on the Internet. The tools presented, is a collection of the most widely used mechanisms for tracking users on the web and will also give some insight into information gathered from mobile users, where applications often are used to deliver the main service.

2.2.1 Cookies

Initially, cookies were intended to enhance the user's interaction with the Web by enabling the user to return to a site and being able to resume interaction where it was left off on the previous visit [28]. The European Commission describes a cookie in the following way;

> *..a small piece of data that a website asks your browser to store on your computer or mobile device. The cookie allows the website to "remember" your actions or preferences over time.*

A cookie is mainly used by websites in order to [29]:

- Identify users
- Remember users' custom preferences
- Help users complete tasks without having to re-enter information when browsing from one page to another or when visiting the site later

From a more technical point of view, the *HTTP State Management Mechanism* [30] is a document that defines the HTTP Cookie and Set-Cookie header fields. It is these header fields that can be used by HTTP servers and thereby be able to store state (called cookies) at HTTP user agents [30]. Further, this makes it possible for the servers to maintain a stateful session over the mostly stateless protocol, the HTTP protocol.

The enabling of cookies is regulated, but to what degree varies from country to country. For example, the European Commissions guidelines states that the use of cookies [29]:

> *..requires prior informed consent for storage or for access to information stored on a user's terminal equipment. In other words, you must ask users if they agree to most cookies and similar technologies (e.g. web beacons, Flash cookies, etc.) before the site starts to use them.*

Further, the Norwegian rules on the use of cookies only correspond to some extent with the European Guidelines. Following Norwegian rules, it is not possible

for a user to accept some, but not all cookies on a website. The Act on Electronic Communications ("Ekomloven") [31], states the following:

> *The storage of information in the user's communication equipment, or access to such, is not permitted without the user being informed of the information being processed, the purpose of the processing, who processes the information and has agreed to this.*

User privacy may be invaded with the use of cookies. Without the user's knowledge or awareness, personal information can be easily obtained through web tracking and information gathering [28]. As a response to the fear of having their privacy interrupted, many users delete their cookies regularly or leave this job to available software programs. One important thing to notice is although; the use of cookies is not equal to misusing user data. In addition, some previous studies have based their results upon the total number of cookies. This may be a misleading metric, since cookies and certainly not the quantity may not have anything to do with tracking [32].

Cookie Types

Several types of cookies exists [29], and the specification is given by its lifespan and the domain it belongs to. By lifespan a cookie can either be a:

> **Session Cookie** - gets erased when the user closes the browser
> **Persistent Cookie** - remains on the user's device for predefined period of time

A classification by domain gives either:

> **First-party cookies** - set by the web server of the visited page and share the same domain
> **Third-party cookies** - stored by a different domain to the visited page's domain. This can happen when a web page references a file, such as JavaScript, located outside its domain

2.2.2 Flash Cookies

People started to deleting cookies in their browser and as a response to this, the Flash cookie was developed. With this a new identifier called Persistent Identification Element (PIE), was defined [28]. This is a unique identifier with similar coding to a regular Hypertext Transfer Protocol (HTTP) cookie. The PIE enables the use of the Local Shared Object (LSO) feature of Adobe's Flash Player plug-in. This software is installed on the majority of computers all over the world. Like the regular

HTTP cookie, the Flash cookie was also developed in order to improve the user experience when browsing on the web. The intention with Flash cookies is that they should be used for basic functions and to remember user preferences. With the Flash cookie, these preferences were made memorable, also when a user alternates between different web pages. Some web pages also uses the Flash cookie in order to "re-spawn" or re-instantiate HTTP cookies that are deleted by a user [33].

Flash cookies, are by function, more persistent than regular HTTP cookies as they;

- Can contain up to 100KB of information by default (HTTP cookies have a limit at 4 KB)
- Does not have expiration dates by default (HTTP cookies expire at the end of a session unless programmed otherwise)
- Flash cookies are stored in a different location than HTTP cookies
- Different browsers on a computer can access the same persistent Flash cookies
- Not controlled by the browser

These features make the Flash cookie better suited and more resilient for tracking than HTTP cookies [33].

2.2.3 Web Beacons

Web beacons are small, often invisible, HyperText Markup Language (HTML) objects that may be embedded in web pages and emails to track user activity. A common form of use is by an imperceptible image, often a single-pixel Graphics Interchange Format (GIF) [28]. When the web page or email is loaded, the browser requests to download the image source from a server. This enables the server owner to log the detailed information about the requesting user such as IP address, date, time, browser, and so on.

The owner of the beacon can use this information to track user activity. How many times, and for how long, the web page was accessed. Geographical location of the IP addresses of the visitors. In more advanced schemes, the server request might also include information about existing cookies in the requesting browser. In combination, the beacon and cookie information might enable highly advanced tracking.

For emails, the web beacon may reveal information every time a email is opened and read. This allows the sender to gather detailed information about when and where individual recipient reads email. In larger scales it may be used to identify valid email addresses, verifying that the content made it past spam filters and read by a user.

The concerns related the use of web beacons is, to a large extent, be similar to the use of cookies. Nevertheless, it is worth mentioning that a web beacon actually is invisible and harder to notice than a cookie, specially since the use of cookies is strictly regulated, see Section 2.2.1. Additionally, it is not possible to reject a web beacon in the same way as one could disallow data to be collected with the use of a cookie.

2.2.4 Other Tracking Mechanisms

Software Development Kits (SDKs)

Software Development Kits (SDKs) are blocks of code that may be installed in mobile applications. SDKs helps to gain insight into how a user interact with a mobile application and collect certain information about the device and network you use to access the application [6].

Digital Fingerprinting

Digital fingerprinting revolves the electronic imprint devices used to access the Internet leaves behind. A digital fingerprint is composed of several elements, and can provide detailed information about a user. This information may include IP address, browser and software type, device information as well as language settings [34].

2.3 Related Work

There has been performed a lot of studies on the topic of privacy leakage over the past years. These studies vary from technical research on the topic of cryptography and protocol security, to areas such as user information sharing and the impact of social networks on individuals.

Annually, the Norwegian DPA releases a report on the state and trends within privacy. The report reviews major changes and events throughout the previous year with respect to privacy, information sharing, legal changes and big security incidents. It also addresses the emotional aspect for individuals in context of sensitive information and how new technologies may challenge our personal life. One of the main focuses within the report of 2018, is the need for trust among users when accepting certain terms of use for services that handle personal and sensitive information. The report points on how changes and countermeasures usually are implemented as a result of some major breach or security leakage incident. They also discuss the challenges associated with outsourcing services to foreign countries with different regulations and ethics. The full report can be found here [35].

On the topic of security and privacy policies for fitness devices, there is a research report, *Every Step You Fake*, issued by the research organization *Open Effect* in 2016. The research covers many different topics related to wearable fitness tracking systems such as understanding the policy and legal agreements, what data that is being collected by the devices and their associated mobile applications, what data that is sent to remote servers and how this data is secured, to whom it may be shared and how the data may be used by different companies. The study covers eight different wearable devices from both American, European and Chinese vendors. The research report shows that personal information is shared over the Internet with a widely varying level of data security. They also discovered some cases of severe security vulnerabilities such as geolocation transmissions that do not appear to benefit the end-user. The report also questions the availability for users to access and correction their personal data, in addition to unclear privacy policies with respect to sale of user information to third parties. The full report can be found here [36].

Chapter 3
Privacy Policies

A privacy policy is a document that explains how an organization handles any customer, client or employee information gathered in its operations [37].

This chapter has the following structure; Section 3.1 reviews the various privacy policies for the manufacturers of wearable fitness equipment. In Section 3.2 a summary of the findings in the policies can be found.

3.1 Review of Privacy Policies

3.1.1 Garmin

The Garmin Connect application is available both for iOS (Apple) as well as for Android enabled devices. This section is a review of relevant parts of Garmin's privacy policy, [5].

Ways Garmin Collects and Uses Personal Information

The following sections will give a description on how Garmin collects and uses the personal information they hold about their users.

Creation of User Account Upon creation of a Garmin account either on the Garmin website or in the mobile application some personal information is required. This includes name and email address. A full name is not required, but optional during the registration. To log into the account, the email address is used as the user name. A password also needs to be set in order to make the account password-protected.

When Logging in to Garmin Account With Social Media Credentials A user may log in to the registered Garmin account using social media credentials. As an example, this may be a user's Facebook login credentials. At the first login to the Garmin account, the user will be asked to approve certain information to Garmin.

This information is name, email address, profile photo, posts, comments and other information associated with the social media account that the user wants to log in with. Due to the way the social sign-on configuration works, Garmin gets access to all this information. Although, Garmin states that they only retain and use the e-mail address for association to the Garmin account. In this way it is possible to use this e-mail address as a login credential to the Garmin account in the future. It is also possible for a user to log in with social media credentials only the first time.

When Buying Products on a Garmin Website Information will be collected when a user makes a purchase on a Garmin page. This includes the user's name, mailing and billing address, as well as telephone number. This collection is made purely to process the order and fulfill the purchase. Garmin does not view or store payment card information. This is taken care of by a third party called Adyen. Garmin recommends the user to carefully review Adyen's privacy policy [38].

When Communicating with Garmin When communicating with Garmin's customer service via email, phone or in person, collection of personal information may happen. Information relevant for collection in this case is; name, mailing address, phone number, email address and contact preferences as well as information about the Garmin device(s) the customer owns, e.g. serial numbers and date of purchase. Creation of event logs that includes capturing information related to the support or service issue may also happen. In order to assist in providing required support, Garmin may access the user account. In certain situations, recording and reviewing conversations between customer and support representatives may be relevant. Personal information may be utilized in communication between customers and support.

When Granting Permissions to Connect Mobile App Several permissions are requested by Garmin when a user downloads the Garmin Connect Mobile app. If granted, these permissions gives Garmin the ability to access certain data from the smartphone. Garmin states that the permissions are optional, but if a user chooses to decline, some features may not be available or fully functional. The complete list of permissions requested by Garmin's application is presented in Table 3.1. Further explanations and comments are given in Section 6.1.3.

When Using Location Features on a Garmin Device or App If a user chooses to enable several location-based services e.g. weather, traffic information, fuel prices, movie times and local event information, on the Garmin application or device, the physical location of the device will be collected. This is a prerequisite that makes it possible for Garmin (or one of their providers) to deliver these location-based services.

Permissions		
SMS Phone Calendar	Contacts	Location
Camera Photos Media	Files	Device ID
Call Information		

Table 3.1: Permissions Requested by Garmin [5].

Other Uses of Personal Information Garmin retains the right to use personal information for internal statistics, marketing or operational purposes. This includes the generation of sales reports and using the statistics to survey user related factors.

Entities with Which Garmin May Share Personal Information

With Other Garmin Companies Garmin retains the right to transfer personal data to other Garmin companies. A link to the full list of Garmin companies is given in this statement [39]. The listed companies are firms that constitute the global company that Garmin is. By transferring personal information between these companies, information may also be moved to other countries. Moreover, this means that the privacy policy that protects a user's personal data also change as data is moved. Garmin also states that all Garmin companies are required to follow the privacy practices set forth in the statement surveyed here.

With Data and Content Providers When using a Garmin auto navigation device or application and a user provide consent, Garmin will collect and upload from the device. The data subject for collection is; location, speed, direction and time and date of recording. If a user accepts it, Garmin may also share de-identified data with or sell the data to third parties in order to improve the quality of the services delivered by content providers.

With Social Network Providers If a user has accepted to receive marketing correspondence about products and applications from Garmin, the company states that they from time to time provide e-mail addresses to social network providers. This is done so they can help Garmin display advertisements on social network pages of other users who share common qualities e.g. demographics and interests.

With Service Providers Third party service providers contribute in administration of some activities and on behalf of Garmin. Tasks delivered by third party

service providers may be; completion of purchases and the following delivery, process credit card transactions, sending e-mails, delivery of ads, analyzing site and app usage, tracking of the effectiveness of Garmin's marketing campaigns, and allow users to connect to social networks. Garmin retains the right to share personal information with these actors to the extent necessary for the sole purpose of enabling them to perform services on Garmin's behalf.

Here, Garmin also specifically informs that they use cloud services form Adobe in assisting in sending e-mails.

Ad Event Logs If a user chooses to use Garmin advertisements that contain advertisements, Garmin may collect information that logs several actions related to the advertisements. Garmin may collect following or similar information; which advertisements were viewed and how often were they clicked etc. In this way the service providers are able to provide content and advertising that may be of interest to the user.

Other Disclosures Garmin may redistribute personal information about a user to other parties if the user has consented to it in such form of consent as may be required under applicable law. Subject to applicable laws in the user jurisdiction, disclosure of personal information to others as Garmin believe it to be necessary or appropriate may also happen [5]:

(a) under applicable law or regulation, including laws or regulations outside user's country of residence
(b) to comply with legal process
(c) to respond to requests from public authorities and law enforcement officials, including officials outside country of residence
(d) to assist or support theft investigators involving Garmin products or property
(e) to enforce any of Garmin's terms and conditions or policies
(f) to protect operation or those of any affiliates and subsidiaries
(g) to protect the right, privacy, safety or property of Garmin, its affiliates and subsidiaries, users and others
(h) to permit Garmin to pursue available remedies or limit damages that Garmin may sustain

In case of reorganization, merger, sale, joint venture, assignment, transfer or other disposition, Garmin may also transfer personal information to an affiliate, a subsidiary or to a third-party.

Ways a User May Share Personal Information or Direct Garmin to Share Personal Information

By the use of certain services, a user may share personal information or direct Garmin to do so. As a general standpoint, Garmin will not transfer or sell personal activity data to any third party a user has been noticed and granted consent. The services that includes sharing PII are as follows.

LiveTrack LiveTrack is a feature available on some Garmin devices. The service involves a link that may be sent to people of the user's choice. This allow the recipients to see real-time location of the device in use. Garmin urges the user to exhibit caution regarding to whom a user shares such a link. If a user chooses to post an invitation to view the location of the Garmin device on a third-party social network, it is possible that persons in addition to the user's intentional invitations, may have access to the same information.

Message Boards and Forums Garmin's websites and applications include message boards, forums, chat functionality, blogs and similar features where a user can post information, messages and other material. Any information disclosed through such services may become public information as well as it may be available to visitors of the sites and the general public. Discretion when using such features is urged by Garmin, both when it comes to posting personal information or any other information.

Promotions Entering into sweepstakes, contests or similar promotions, Garmin may use the information to administer those promotions. To the extent that the terms and conditions of any such promotion regarding the treatment of Personal Information about you conflict with this Privacy Statement, the terms and conditions of the promotion will control [5].

Cookies and Similar Technology

In order to analyze the usage pattern of a Garmin website, Garmin in assistance by third-party analytic service providers, collect certain information when a user visits these websites. The information collected includes IP address, geographic location of the device, browser type, browser language, date and time of request, time(s) of visit(s), demographics, page views and page elements clicked. The ability to collect this information is given using cookies, pixel tags, web beacons, clear GIFS or other similar tools on their sites or in email messages. These tools help Garmin collect and analyze such information which further may help in the delivery of better, more relevant content on the sites, measuring effectiveness of advertisements as well as identifying and fixing problems. Garmin may also engage a third-party to provide

online advertisements on their behalf. They may also make use of technological tools like a pixel tag or similar to collect information. The aggregated information may also be utilized to send targeted advertisements.

Garmin also uses locally stored objects, Flash cookies, in certain situations where Adobe Flash Player is used to provide special content such as videos or clips. This tracking technology remembers settings, preferences and usage and is similar to browser cookies, but is not manageable through the browser.

When a user syncs their Garmin device, data recorded on the device being synced, is transferred from the device to Garmin's servers. For every synchronization, Garmin logs data about the transmission. Examples of the type of data being logged is; IP address. sync time and date, crash and diagnostic logs, geographic location of the device, information about the network used to sync and the battery level of the device. This information is used for identification and resolving synchronization issues.

Garmin also tracks and collects data from users about their usage of Garmin Express and Garmin mobile applications. Analytic information in this case is; date and time of the device accessing Garmin's servers, software version, geographic location of the device, language, what information and files that have been downloaded to the device, user behavior e.g. features used, frequency of use, device state information, device model, hardware and operating system information, and information related to the device functions. Garmin uses this collected information to improve the quality and functionality of their services. It also helps them to develop and market products and features that may serve the user in the best possible way. In addition, identification of problems and fixing usability problems is listed as one of the use cases for the information collected in the syncing process.

The privacy policy gives examples of some third-party providers of analytics and similar services Garmin currently use. The complete list from the policy is given in Table 3.2. Further explanation of the individual providers can be found in Appendix B.

Garmin informs that any information received by a third-party is governed by these companies own privacy policies. As an example, the table shows that Tealium is present as a provider of *Tag Management*. Tealium receives information from the users of Garmin's websites such as IP address, browser and Operating System (OS) information. For further insight to how Tealium uses this information, the reader is referred to another document, namely Tealium's privacy statement.

Provider
Analytics
- Google Analytics
- Google Search Console
- HockeyApp
Crashlytics (Fabric)
- Splunk
Tag Management
- Tealium IQ
Social Networks
- Google
- Facebook

Table 3.2: Third-Party Providers Garmin [5].

Links, Third Party Apps and Third Parties' Privacy Practices

Garmin takes no responsibility for the websites, apps and products that are not operated by the company itself. They are not responsible for the privacy practices or the content of any linked sites and applications [5]. If a user enabled any third party sites or applications, the personal information collected here, will be controlled by the privacy policy of that third-party and is therefore beyond Garmin's control.

Security

Garmin states that they take reasonable security measures to help protect against loss, misuse, unauthorized access and unauthorized disclosure or alteration of the personal information that is under their control. They also links to another informational site, *Keeping Data Safe at Garmin* [40]. Here, users can read more about the efforts Garmin takes in order to make the use of their services more secure.

Garmin also encourages any user to report what they might think is a security issue or vulnerability. For safety reasons, Garmin can not publish their measures to ensure users' safety.

Access, Correction and Deletion

Users may request insight in their personal information by emailing a request to Garmin. Further, requests can be sent for either updating or deleting the information. The deletion includes both PII and the Garmin account. Thus, Garmin informs that the response on the request will be handled in accordance with applicable law.

Comments on Garmin's Privacy Policy

At first look, the Garmin privacy policy stands out as uncluttered and easy to navigate, but with high textual density. The language used makes the document rather easy to read. Upon closer examination, the use of referrals to other informational sites with the use of plain Uniform Resource Locators (URLs) occur at several occasions in the text. As a result of this, it is very difficult to get a complete overview of which terms one really has to accept to make use of Garmin's services. When the referrals especially are used in connection with the elaboration of technology and tracking, it is particularly vulnerable. This field of technology is hard enough for a user to understand initially.

Further, the company requires very little user data in order to create a user profile. Only name, email address and a password is mandatory. Also, the policy clearly states which permissions are requested when using the Garmin Connect Mobile application. There is a section that explains the use of tracking technologies, and also in this section, a precise and simple language is used. The policy also gives examples of third-party providers of analytics and similar services. Here, it would be even better if the company provided a complete overview over all third parties involved. Although, it is better with some insight rather than none.

3.1.2 Fitbit

Fitbit recently updated their privacy policy and terms of service. The latest update took effect from 30th of October 2017. Fitbit states that transparency is an important key to any healthy relationship and they want to make their privacy policy as understandable as possible for any user. According to Fitbit, the updates reflect the evolution of their products and services [41] and therefore, the privacy policy and "terms of service" needs to follow this development. The update also includes a reorganization and clarifications, with examples and additional details where this is required.

The following section is a review of Fitbit's privacy policy and refers to the Fitbit Privacy Policy, [42].

Information Collected by Fitbit

Fitbit collects information about their user's in multiple ways. A user may choose to enter a lot of information, or choose a more neutral line. This section will present the different types of information gathered, and also show how the information is retrieved.

Information Provided By The User

Account Information Some information is required to create an account and thereby use Fitbit's services. This information includes;

- Name
- Email address
- Password
- Date of birth
- Gender
- Height
- Weight
- Mobile telephone number[1]

Additional information may also be added by the user, but this is a voluntary choice. The supplementary information a user may add is a profile photo, community username, food log, alarm, and messages on discussion boards or to friends using the same services.

Additional Information Fitbit wishes to constantly improve their services and the user experience. In order to do this a user may choose to provide Fitbit with additional information. This may include connecting with friends that have not yet joined by providing their email addresses, accessing social network accounts, or using the contact list on the user's mobile device[2]. Further, after participation in a survey, contest or promotion, Fitbit collects information submitted.

If a user decides to connect their Fitbit account to another service (i.e. Facebook or Google), Fitbit may receive information from this service provider. Information may in this case be a user's name, profile picture, age range, language, email address and friend list [42]. It is also possible for a user to grant the Fitbit application access to fitness information from another application.

Payment and Card Information Some of Fitbit's devices support payments and transactions with third parties. Upon activation of this feature, certain information must be added regarding identification and verification. More specifically, this information includes; name, a credit or debit card number, card expiration date and Card Verification Value (CVV) code. The handling of this crucial information is done in such a way that the transaction takes place without exposing the card number. Transaction history is not recorded by Fitbit.

Information Received From Use

[1] In some cases

[2] The contact list will not be stored, gets deleted after it is used for adding contacts as friends.

Fitbit Device Information The device collects data in order to estimate different metrics including; step count, distance, number of burned calories, weight, heart rate, sleep stages, active minutes and location. When the device synchronizes with the Fitbit application or other software, data temporarily stored on the device is transferred from the device to Fitbit's servers.

Location Information Features included in Fitbit's services include the use GPS signals, device sensors, Wi-Fi access points and cell tower IDs. If a user grants Fitbit to access these data, it will be collected by Fitbit. The company may also derive approximate location based on the user's IP address.

Usage Information Usage data includes information about interactions with the Fitbit services such as content views, installation of applications or software, creation or login to user accounts, pairing of a Fitbit device to a user account or interactions with an application on the device. This data is received by Fitbit. Data about the devices and computers used to access any Fitbit services is also collected. This information includes IP address, browser type, language, OS, Fitbit or mobile device information[3], referring web page, page visited, location[4] as well as information about cookies.

How is The Information Used?

To Provide, Improve and Develop Services The information collected by Fitbit is being utilized to deliver services, research of existing services and development of new ones. The information may also be used to help a user to get in touch with another user. A match may be done if a user has an e-mail address contained in another contact list. In this case they may show that the acquaintance exist. If precise location information is enabled, Fitbit also uses this to record where a workout took place or to map an activity.

To Personalize Services Information collected by Fitbit contributes to delivery of personalized services. One effect of this is that a user is displayed more custom content. The information also enables improvement of the inferences made when it comes to activity and workouts. In this case, as an example, information like height, weight, gender and age allows Fitbit to personalize daily exercise and activity statistics like the number of calories burned and distance traveled.

To Communicate The information that is gathered by Fitbit is also used to send notifications as well as informing about new features or products.

[3]including device application identifiers
[4]Depends on the permissions the user has granted Fitbit

Promoting Safety and Security Promotions of safety and security related the services Fitbit provides is also a result of the data collection. Information may for example be used for authentication, to facilitate secure payment or to protect against fraud and abuse.

How is The Information Shared?

Upon Agreement or Directions Some user activity may be shared if a user gives directions directly. Certain information will be shared as a result of preferences set by the user. By participating in challenges, a user is informed that this will result in sharing of specific information. This information is no longer shared based upon personal preferences and will be visible to all other participants in the challenge. This applies to the user's profile photo, posted messages, total steps in a challenge, personal statistics and achievements.

It is also possible for a user to authorize sharing of information with others, e.g. a third-party application when this is granted access to the account. This information is no longer governed by Fitbit but by the third-party privacy policy and user terms.

For External Processing Information is transferred to Fitbit's corporate affiliates, service providers and other partners that process data for the company. The data is being processed according to their instructions and guidelines. The partners provide Fitbit with global services that include customer support, information technology, payments, sales etc..

Legal Reasons To comply with a law, regulation, legal process or governmental request, Fitbit may preserve or disclose information about a user.

Information that has gone through de-identification and no longer can be used to identify an individual (Non-PII) may be shared freely with the public or third-parties.

If a merger, acquisition or sale of assets happens, Fitbit will take measures to protect the confidentiality of PII. A notice before transferring any PII to a new entity will be given to the best of their ability.

Access To Information

Fitbit provides every user with account settings and tools for accessing PII associated with the user account. Another feature is the possibility to download certain account information. This also includes activity data and other statistics collected by the wearable fitness device. In one single data export it is possible for a user to download 31 days of activity. In addition, Fitbit states that this feature is added because the

firm feels that the individual user data belongs to the user - therefore, they should always have access to it.

Analytics and Advertising Services Provided by Others

Fitbit has partnered up and is receiving analytics and advertising services from other teams. These services include interaction data, advertisements on Fitbit's behalf and advertisement performance measurements. The third-party partner firms may use cookies and similar technologies to collect information about user interactions with the services offered as well as other websites and applications. Fitbit refers to a separate *Cookie Use Statement* [6]. The technologies for information collection by Fitbit and third parties are presented in Table 3.3.

Technology
Cookies
Pixels (Web Beacons)
Local Storage
SDKs

Table 3.3: Tracking technologies, Fitbit [6].

The different technologies presented in Table 3.3 are used for different purposes. These are also presented in the *Cookie Use Statement* [6]. Fitbit further informs that their websites do not respond to "Do Not Track" signals. The reason for this is that they do not track their users over time and across third-party websites to provide targeted advertising.

Policy Regarding Children

Children under the age of 13 are not permitted to create accounts unless their parents has consented on their behalf.

Information Security

Fitbit emphasizes the importance of keeping user data safe and they use Transport Layer Security (TLS) to encrypt many of their offered services. They also indicate that no transmission of data is completely secure no matter method used for transport.

International Operations and Data Transfers

Due to global operations, transfers of information collected inside the EEA (amongst others) to the US may happen. Fitbit complies with the EU-US and Swiss-US

Privacy Shield principles regarding collection, use, sharing and retention of personal information from the EEA and Switzerland. This is also further described in *EU-US Shield* [43]. The shield has been developed in order to provide companies on the both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data between the countries. Companies can join on a voluntary basis, but as soon as the commitment to participate has taken place, the obligation is enforceable under US law [43].

Comments on Fitbit's Privacy Policy

By first impression, the policy looks well organized. The language used in the policy is also easy to read and understand. Fitbit uses references to other sources for more information. In one case the referred document also includes a reference to another source. Use of support documents like this, and in this manner, makes the document harder to navigate and a user might loose the complete overview over the given information.

By logging into their accounts, users have the ability to review and update their personal information. It is also positive that the privacy policy clearly states that information associated with a user account gets deleted when the account itself is deleted[5]. On the other hand, deletion of accounts must be requested by contacting the customer service which seems a bit extensive.

3.1.3 Polar

This section is based on the review of the Polar privacy policy [7].

The current privacy policy from Polar took effect on August 1st, 2017. The policy is introduced with several defining statements regarding Polar's organization of services. Also, the introduction states that if any inconsistency between any of their *Special Terms* and the privacy policy reviewed, the applicable special terms will prevail over the terms presented in the policy. Further, Polar informs the reader that by using or accessing Polar sites, any services or by participating to events offered by the company, the user acknowledges and consents to the collection, use and disclosure of personal data and other information. If the users do not agree, they are requested to not to use any of the services offered by the company.

Collection of information

Information of a user is typically collected in the following scenarios [7];

[5]Some delay may occur as the process of deletion takes time. Fitbit also retains the right to preserve information for legal reasons or to prevent harm [42]

- execution of purchases
- usage or registration into services
- entering promotions, sweepstakes, contests or other campaign
- use of services offered in Polar sites
- other communication with Polar, e.g. customer care

Then a rather extensive list with examples of information that may be collected follows. This includes details of the queries or requests made, products and services provided (including delivery details) and information relating to the Polar products and/or their use, financial details e.g. payments made, billing address, credit checks and other such financial information, details of agreements between the user and Polar, records of contacts and communications, information the user have provided and other transactions information and demographic location e.g. age, gender, weight, height and language preferences [7]. Further, Polar websites may include message boards or forums, any information provided by the user in such contexts may be collected by Polar. This information may also become public and may be available to other users of the same services and to the general public.

Polar informs their users of how they define PII and also states that some Non-PII may become personal and identifiable when a user submits additional personal data. The personal data Polar possesses may be used as follows;

- for contact via mail, e-mail, mobile message or phone
- to customize user experience and determination of satisfaction
- to inform of new products, services, events of promotions and for other marketing purposes
- to personalize services
- to compute variables required for the use of the service
- to ensure functionality and security
- to investigate fraud and other misuse
- create aggregated data and statistics

In addition, Polar states that they may combine personal data collected in connection with use of the Polar product and/or service with other personal data they may hold, except where such personal data was collected for a different purpose [7].

Consent for Disclosure of Personal Data

This section in Polar's privacy policy deals with data transfers to other countries. This is a necessary specification by the company, as products and services offered are provided using resources and servers in different countries that may reside outside the user's residence, EU and the EEA. Where such transmissions is required, Polar states that they take needed actions to ensure adequate protection of personal user

data. In the case of international transfers of personal data, Polar rely on agreements based on Standard Contractual Clauses formed by the European Commission [7] [44].

Further, the section informs that Polar does not engage in selling or trading personal data to other companies for promotional purposes, and will not provide personal data to a third party without your permission. The exception is when it is necessary to process an order, fulfill requests or manage interactive customer programs [7]. If the local legislative allows it, Polar may transfer personal data to affiliates. In the case where subcontractors are involved it may also be necessary to exchange personal user data. In relation to this, Polar assures the user with that further use of the data, by the subcontractors, is prohibited and ensured by the use of confidentiality agreements.

Security

Although the risk factor is present when exchanging personal data, reasonable precautions is made by the Polar team in order to prevent unauthorized access to and improper use of personal data. This includes the use of encryption when collecting personal data about a user.

Other Information

Polar defines *Other Information* as data that does not reveal specific identity or does not directly relate the user as an individual. Examples of such information are:

- Browser and device information
- Application usage data
- Information collected through cookies, pixel tags and other technologies
- Demographic information and other information provided by a user
- Aggregated information

If a user enables certain services, it is a direct consequence that certain information is collected. One example is the use of location based services, then the physical location of the device will be collected. Further, Polar informs that they may use and disclose this type of information for any purpose. This also includes that they might share/sell the information to third parties. Also, the company may combine *other information* with personal data. The combination of data will be treated as personal data as long as it is combined.

Visitor Identification - Technical Information and Usage of "Cookies"

In the process of improving their sites, Polar normally collects certain technical information as a standard. Examples of such information are IP address, access times, the website the user linked from, pages a user visits, links used, ad banners

and other viewed content, device information and other such technical information that may be provided by the browser.

The use of services Polar offers, over a telecommunications network, also include collection of other information such as mobile subscription number. This information may be transmitted by the operator of the network as a standard.

Cookies are enabled on Polar websites, and may also include elements that set cookies on behalf of a third-party. The user is then referred to another website for more general information on how cookies work. Although cookies in use might be changed by Polar at any time, they inform specifically about which cookies are used on the Polar sites at the moment. Table 3.4 shows the active cookies on the Polar website and their function.

Cookies	**Function**
Google Analytics	Identification of unique visitors
Google Analytics	Track traffic sources & navigation
addthis.com	See footnote for explanation [6]
Play Framework	Identification of users in Polar Flow

Table 3.4: Active Cookies Polar [7].

In general, minors are requested to not make purchases or engage in other legal acts without consent of a parent or legal guardian. The age of minors is determined by local law where the user resides. Also, independent of the decision a user makes relative to different e-mail notifications from Polar, mailing lists will not be shared with third parties for promotional purposes. To review or update personal data it is possible to contact Polar via e-mail.

Comments on Polar's Privacy Policy

The document that represents Polar's privacy policy has few paragraphs and may be characterized by high textual density. My first impression was that the policy looks like a wall of text. It withholds large amounts of important information, but is relatively difficult to read. The document is to a small extent sectioned and each section therefore contains widely distributed information. This also contributes to the document being difficult to orientate, often a lot of text must be examined if you look for specific details.

[6] Created and read by *addthis.com* in the client side in order to make sure the user sees the updated count if they share a page and return to it before our share count cache is updated [7]

Further, phrases like "Information of you is typically collected when ..", "data such as" and "may" is used frequently throughout the policy. The use of this vague sentence structure does not provide precise information about what type of data is collected, nor when the data is used by Polar. In addition, the privacy policy does not include any information about which data is required to create a user account.

The privacy policy informs that a user must contact Polar by e-mail for updating or reviewing personal data. This could have been implemented more practically and as a more easy accessible feature.

On the positive note, Polar informs in an orderly manner which cookies are active on their websites, but adds that this might change at any time. Another positive addition is that the company actually informs, in writing, that they do not sell or exchange personal data to other companies for pure promotional purposes. Further, any changes or updates to the policy will be shared with all users via email. Polar's privacy policy does not inform a user about what will happen to user data and PII through sales, reorganization or acquisition.

Another positive element in the privacy policy is that Polar informs about their procedures when international data transfers are required. That they make use of the European Commission's Standard Contractual Agreements as a basis for agreements stands out as reassuring information from the company.

3.2 Evaluation

This chapter has reviewed three different privacy policies in order to figure out how the manufacturers protect their user's information. Here, I will present a summary of the findings.

The first difference between the manufacturers privacy policies is shown in how much user information they require for setting up accounts. Table 3.5 displays the information that is mandatory to register when setting up an account with the different manufacturers. Fitbit and Polar requires the most information while Garmin stands out with only three required informational fields. Although Garmin does not require the data upon registration, the opportunity for more input exists. This additional information will not be displayed on the user's public profile unless this is chosen.

[7] Full name not required

[8] Additional information may also be added

[9] Polar does not inform about what information is required for creating an user account. The ticks for Polar was retrieved by creating an actual account.

	First Name	Last Name	Gender	Email	Password	Phone Number	Date of Birth	Weight	Height
Garmin	✓ [7]			✓	✓				
Fitbit [8]	✓	✓	✓	✓	✓	✓	✓	✓	✓
Polar [9]	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 3.5: Comparison of Mandatory Information

The methods used for information retrieval is also similar both in respect to technical solution and prevalence. All manufacturers use their privacy policies to inform their users of applied data collection technologies enabled in their services. However, the degree of information presented varies. Some include small examples while others present insight into third-party providers of certain services. The method of referring to other sources for *learning more* or *get a deeper insight* is widely used by all companies. As a result of this, the privacy policies seem, to some degree, unfinished and thereby does not give the user maximum benefit by reading the policies.

Another aspect of the statements that are worth noting is the ability to review, correct, update or delete personal information. One side of this is that a user always can log into the user account and research what information is stored. Fitbit is the manufacturer that facilitates best the ability to check what information is stored. The company also provides a solution for downloading registered workout data. On the other hand, the isolated information itself may not be the most crucial to collect for a user. The recipients of the data with a complete overview of which data has been sent to who is more relevant and necessary. Moreover, this is much more difficult to obtain for a regular user. Either way, it is positive that Fitbit has included this feature in their services. Polar on the other hand, requires users to contact them by email both to update and/or review personal data. Garmin also requires that access, correction or deletion requests either can be placed via e-mail or mail. To completely delete a user profile, all actors requires this to be done via contacting customer support either via an available contact form or e-mail.

In the situation of sale, merger or acquisition both Fitbit and Garmin clearly states what might happen with a user's PII and user data. In both cases the firm retains the right to transfer data to third parties, subsidiaries and affiliates. Polar on the other hand, does not mention what happens to user data in this context. The companies does not go in detail whether these rules also applies to minor acquisitions and reorganizations. Is it for example possible for a company to buy shares in a firm in order to get access to the data? One might speculate that the motivation for acquisitions of companies with a large user base might be to get access to user information. Companies with popular applications, like Snapchat or WhatsApp are

often valued extremely high and acquired by large companies known for collecting data. Online users seem to be of great value and interest.

Transferring user data between several servers with different location is also a common practice. The servers may be located in different countries and the data protection laws varies accordingly. Data may also be cached at several servers in order to deliver specific data more efficient. Before the data has reached its destination, the reality may be that the legislation protecting the data may have changed not just one, but several times. Another question emerging due to this is; will the trace a user leaves also vary depending on location? In the case where data is cached for higher efficiency, for how long will the data be stored and to what extent is the data cleaned up after a user leaves the location?

All companies inform that they make use of multiple third parties for delivery of certain services. In addition, some of the companies are large and has a long list of subsidiaries. This implicates that data is distributed, but they do not inform about what extent. How many third-party companies are there and for what exact purpose are they involved? The distribution of information leads to increased vulnerability as the same is stored in multiple locations. A new question then arises, should not the main service supplier ensure the same privacy and security levels for all subcontractors? Or at least to some degree? Maybe they at least should document that they have access to the various guidelines for safety procedures and standards implemented by each company their services rely on? Then, there is also the question of trust between the main actor and all third parties involved. To what extent are the third parties acting within the policies and rules defined by the contractor? Is this based on pure faith or does it exist routines for auditing how the data is preserved and used?

Recent events involving Facebook and Cambridge Analytica, have shown an example of how data has been misused by a third-party exploiting leap holes in the user agreement. Cambridge Analytica payed customers to share their personal information via their Facebook profile with an app called *thisisyoudigitallife*. Because of an inadequacy in Facebook's agreement, Cambridge Analytica was also allowed to collect information from the voluntary user profile's networks. As a result, it is assumed that they have collected data from approximately 50 billion user accounts [45]. The analytic company did not have the privileges to utilize the data in any other way than to improve Facebook's interface. Regardless of this, the data was still utilized for entirely different purposes. It was used to form psychological profiles on actual individuals, allegedly used for political purposes in conjunction with the presidential election in the US as well as Great Britain's "Brexit" [46].

Chapter 4
Wearable Fitness Devices

This chapter presents the wearable fitness devices evaluated in this thesis. The devices are from different major manufacturers available on the Norwegian market. Two of the devices are fitness watches, whilst one activity band and one Heart Rate (HR) monitor also are included. For each device, the available smartphone application and website for tracking fitness activity is presented.

4.1 Fitbit Alta HR

The Fitbit Alta HR is produced by Fitbit Inc. and is is a slim activity wristband and was released in March 2017.

This model also allows the user to change the bracelet the smart band is attached to, thus making the tracker a stylish accessory rather than it just being a part of your training regime. The Alta HR has dimensions 0.6"x 0.5"x 1.6" (WxDxH) and weighs 0.81oz [47]. This makes the wearable a relatively small activity tracker. The device also has a built in Organic Light-Emitting Diode (OLED) display. The wearable's specifications also states that is is splash proof.

Figure 4.1: Fitbit Alta HR [1].

The essential features of the Fitbit Alta HR are shown in Table 4.1 and briefly explained here. *Steps, Calories* and *Distance* is the parameters constituting the daily

activity tracking. A quick double tap on the display of the Alta HR causes the device to display the status on how far away a user is from the desired activity goal.

Features
Steps
Calories
Distance
Smart Track
Reminders
Auto Sleep Tracking
Alarms

Table 4.1: Features, Fitbit Alta HR

SmartTrack is a feature that allows the device to automatically detect workouts like running, elliptical, biking and more. The activities registered are logged to the Fitbit dashboard. Further, the ecosystem provided by Fitbit, gives a user the opportunity to receive several *Reminders*. This functionality includes call, text and calendar notifications and also reminders to move. *Auto Sleep Tracking* is a feature that allows the Fitbit wearable to automatically track sleep duration and consistency. It also has a feature that wakes the user up with a silent *Alarm* that vibrates. By using the HR as a measure, the Alta HR produces a sleep report which highlights the periods with light, deep and Rapid Eye Movement (REM) sleep.

4.1.1 Fitbit Application

The Fitbit application is particularly designed to work alongside Fitbit activity trackers and smart scales. Purely practical denoted, it gives a user the ability to sync devices wireless with their device. The app used in testing in this thesis has the latest update which was released March 1st 2018 by Fitbit. The functionality of the Fitbit application is categorized in the following way [8];

Features
Day & Night
Activity & Workouts
Motivation & Friends
Weight & Nutrition

Table 4.2: Features, Fitbit App, [8].

Firstly, the *Day & Night* category is used by Fitbit to express the wide functionality of the application in general. The statement from Fitbit is: *The Fitbit app has a*

purpose for every part of your day [8], and emphasizes exactly this. Listed in this category is *All-Day Activity* which gives the user an overview on the progress towards daily step goals, distance, calories burned and active minutes. It also gives an impression of user trends over time. Fitbit also informs that although the application is designed to work alongside a fitness tracker, it is possible to use the smartphone to record basic statistics like steps, distance and calories burned. Further, it is possible to synchronize these statistics to the Fitbit application.

The *Activity & Workouts* block includes features like "Mobile Run" where the GPS is used to accurately track, log and compare runs, walks and hikes. "Track Exercise" is also listed in the category, and enables the use of a Fitbit tracker to record workouts and further log them into the application. This gives a complete overview regarding exercise statistics, how they impact the day overall and also improvements in the statistics logged. The "Exercise Calendar" gives a more systematic view of accomplishments and also the ability to use data and trends to make progress towards a possible set goal. Via "Exercise Sharing" it is possible to share a selfie when the user has reached the peak of their workout. The picture can be sent together with other workout statistics on any social channel, or through email and text.

Further, *Motivation & Friends* concerns the feature where the Fitbit application pushes motivational notifications to the user's smartphone with the goal of inspiring to keep pursuing the fitness goal. The block also includes "Challenge Friends and Family". Here it is possible to compete with friends and family both in the short and long run. Whenever a user hits a milestone, they have set for themselves, a badge is received as a confirmation of achieving the goal. Also, the category includes features that helps a user to stay connected with Fitbit Friends. Here, Facebook an email are the two services included to achieve this functionality.

The last feature category is *Weight & Nutrition*. Here, it is possible to track weight changes with the use of a smart scale also delivered by Fitbit. The results from each weigh-in will be automatically sent to the website dashboard or to the Fitbit application. The bulk also describes a feature that concerns logging of calorie intake. A measurement of hydration is also available upon the registration of water intake by the user. The weight and nutrition services available in the app are supposed to give the user an easier and more straightforward road towards weight loss, if this is one of the targets.

4.1.2 Fitbit Dashboard Website

The Fitbit Dashboard is an online web portal which holds personal activity logs. The dashboard can be accessed with the user credentials as for the application. It has the same activity information as the smartphone application, where users can browse their training sessions and other sensor data gathered through the wearable

device. The activity data is synchronized to the web portal in the same manner as the smartphone application. This means that a user, at any time, will have the same data in the dashboard and on the smartphone. The user interface in the web portal is somewhat similar to the application.

4.2 Garmin Forerunner 235

The Garmin Forerunner 235 is a GPS running watch with a wrist-based HR monitor. This means that the watch itself registers the HR - there is no need for an additional HR sensor. Figure 4.2 shows the Garmin Forerunner 235 and Table 4.3 lists the main features available. A brief introduction to the features included in each table entry will also follow.

Features
Activity Tracking
Sleep Tracking
Indoor Training
Workouts
Heart Rate Features
Smart Features
Widgets
Bluetooth Connected Features

Table 4.3: Features, Forerunner 235 [9].

Activity Tracking is a feature that records daily step count, step goal, distance traveled and calories burned for the days the Forerunner 235 has been used. The activity tracking includes a feature called "Move Alert" which gives the user a reminder to move each hour. The Forerunner also creates an "Auto Goal", this is a daily step goal based upon previous activity levels. Also, a goal bar is available on the screen. Via the feature *Sleep Tracking*, the device automatically detects sleep and more specific monitors movement during sleep. A user can set normal sleep hours in the user settings. The sleep statistics available for review includes total hours of sleep, sleep levels and sleep movements.

Further, *Training Indoors* enables the user to register indoor training workout. Here, the GPS will automatically turn off in order to save the battery. *Workouts* gives the user a possibility to create custom workouts that may include separate goals for each of them. The *Heart Rate Features* on the Garmin Forerunner is enabled via the wrist-based HR monitor, but the wearable is also compatible with other sensors if desired by the user. The features include setting personal HR zones, or allowing the device to detect maximum heart rate and configure the HR-zones accordingly.

Figure 4.2: Garmin Forerunner 235 [2].

To make use of the *Smart Features*, the wearable must be paired with a smartphone. This gives access to several functions such as; phone notifications, music control of the music playing on the phone via the Forerunner 235, as well as the use of multiple widgets. A widget is *a module on a website, in an application, or in the interface of a device that allows users to access information or perform a function* [48]. Garmin has several widgets available [9], and they are as follows:

Calendar: upcoming events from the phone's calendar
Controls: turn on/off Bluetooth. Other features: "do not disturb", "find my phone" and "manual syncing"
Heart rate: current HR in Beats Per Minute (BPM) including graphical view of HR
Music Controls: music player controls for smartphone
Notifications: alerts incoming calls, texts, social network updates and more. Based on smartphone notification settings
Steps: tracks daily step count, step goal and data for the last 7 days
Weather: shows current temperature and weather forecast

Lastly, the *Bluetooth Connected Features* will be shortly presented. This service involves giving the user several Bluetooth connected features for the compatible smartphone using the Garmin Connect Mobile application. More information about this can be found online [49].

4.2.1 Garmin Connect

The Garmin Connect Mobile application is a free application available for download from the AppStore and Google Play. It is also available for devices running Microsoft OSs. It serves as an online training tool to store, analyze and share all personal

fitness activities and is compatible with Garmin fitness devices. According to Garmin, the application is designed to give the user an overview of all vital health statistics at a glance [50].

Features
My Day
Challenges
Calendar
News Feed
More

Table 4.4: Features, Garmin Connect.

Garmin has made a layout where different colors represent different activities. In this way a user easily can see which data is viewed. It is also possible to customize what type of "cards" that shows up on the dashboard where the activities is listed. Automatically, the "Last 7 Days"-view is available and shows the averages of steps, calories and sleep. This makes it possible for a user to easily see how the level of activity and abnormalities in the degree of exercise according to the user's personal training plan. Table 4.4 shows available features in the Garmin Connect Mobile application.

My Day gives an overview over activity during the current day. The content is editable, but as a starting point, HR, steps, number of active minutes, calories burned, and sleep are viewed. It is also possible to choose a comparative view, where the results from the day before also is visible.

The next bulk, *Challenges*, shows the history of challenges the user has participated in. It is also possible to create new challenges or join a standardized challenge based on total step count in a week. It is also possible to "friend" acquaintances that uses the application, then their steps will also be visible in the application.

Calendar shows a summary of all activities in the current month. The various completed activities and workouts is displayed using the same color coding as mentioned earlier in this section.

The *News Feed* enables the possibility to connect with friends and contacts from Facebook and Google.

The category *More* in Table 4.4 is comprehensive in terms of functionality included. Shortly described, this is the bulk in the table that covers most of the "freedom" and possibilities in the app. A summary of a particular activity may be viewed with a historical perspective of 7 days, 4 weeks or 12 months. The average daily

distance, total distance or total calories burned over the time period is also calculated. The creation of manual activities is also present. Activation of *Smart Notifications* enables the user to stay connected at all times, receiving notifications directly from the connected mobile device. For more information on the Garmin Connect Mobile app, visit Garmin's websites.

4.2.2 Garmin Connect Dashboard

In same fashion as the Fitbit dashboard, the Garmin Connect website requires login and shows all activities and sensor data recorded by the smartphone application. The user interface is similar to the application and the data is synchronized with the app.

4.3 Polar M400

Polar has several wearable fitness products available on the market, two of them will be included in this thesis. Also, different solutions for tracking fitness activity exists. In this thesis testing with a Polar fitness watch, the Polar M400, will be conducted. In addition, I will test a new solution provided by Polar. Namely the opportunity to only use a HR sensor that monitors the user and from there will perform a direct transfer of sensor data to the connected smartphone. The HR sensor used for testing in this thesis is the Polar H7 HR sensor, and will be presented in Section 4.4.

Figure 4.3: Polar M400 [3].

The Polar M400 is a wearable fitness device that is designed for enthusiastic athletes and has built in GPS as well as features as Smart Coaching and activity tracking. A user can track their training data including heart rate, pace, speed, distance and route.

The watch is delivered with the Polar H7 Heart Rate sensor. This gives the user a possibility to oversee their heart rate in real-time on the watch whilst training.

Further, the heart rate information may be used to analyze how the workout session went. For more information about the H7 HR sensor, see Section 4.4. Figure 4.3 shows the Polar M400 fitness device. Table 4.5 will give an overview of the main features from the menu on the M400 and a short description of them will follow.

Features
Today's Activity
Diary
Fitness Test
Timers
Favorites

Table 4.5: Features, Polar M400 [10].

Today's Activity shows the daily activity and is visualized by the use of an activity bar. Details like total active time, calories and steps are available. The *Diary* views statistics from the last week, past four weeks and next four months. The *Fitness Test* is available to measure the fitness level and is supposed to be performed when the user is lying down and is relaxing. *Timers* includes two different timers; an interval timer, where time and/or distance based interval timers can be set, and a finish time estimator. Here, the target time is for a set distance. *Favorites* is a label in the menu where it is possible to review training targets that the user has saved as favorites in the Flow web service.

The M400 used in testing in this thesis has the newest firmware installed (version 1.9.681). The firmware update was released by Polar December 13$^{\text{th}}$, 2017.

4.3.1 Polar Flow

The Polar Flow is the standard application available for fitness tracking if a user enables a fitness watch. The application registers daily activity, sleep, burned calories and training activities. It also gives a user knowledge about activity goals and provides the user with a progress overview related to personal goals. Based on the specified goals a user may register, the application is designed to achieve more and also help the user stay motivated. Some of the possible features is presented in Table 4.6.

The *Polar Group* feature makes it possible for users to share and discuss exercise-related topics or conversations with other users of this service. *Polar Flow Events* takes the group function even further by letting the users share a specific session and also share their activities with other like minded people. A *Daily Activity Goal* is set based on a user's activity level, personal settings as well as general health

Features
Polar Groups
Polar Flow Events
Daily Activity Goal
Flow Diary
Long-term Activity Analysis
Sport Profiles
Running Programs
Training Load
Recovery Status

Table 4.6: Features Polar Flow Application

recommendations. In addition, an activity goal bar will be displayed at the screen of the connected device and will fill up during measured activity during the day.

Further, the list of features has an entry, named *Flow Diary*, this is a built-in diary that holds information about tracked steps, distance, calories burned, active time, inactivity stamps, the quality and time duration of sleep. A user may also use the diary for planning future training sessions. The *Long-term activity analysis* is given by a *Progress* tab that produces a long-term activity report. This report may be viewed based upon weekly or monthly activity statistics. A *Sport Profile* feature enables the possibility for a user to tailor own sport profiles. A user may also use this function to modify which fields with information that should be displayed on the connected device during training. Different configurations is also possible from this service, including configuration of automatic laps, customization of heart rate and speed zone settings.

A *Running Program* may be created. This makes it possible for a user to train accordingly to a plan. Four distance running goals are available. Based upon training history and current activity level, a program will be created. This may range from 9 weeks to 20 months duration. The two last rows have two features listed, namely *Training Load & Recovery Status*. These features show how strained a user is after a completed workout and uses this information to estimate recovery time. With this figures as background, the user is given recommendations on how long one should rest before participating in a new training session.

4.3.2 Polar Flow Website

The Polar Flow website shows a diary of all training sessions and registered activities. The sessions are logged from the device when synchronized with the smartphone

application. As for the other web portals, this site also requires log in with the same user credentials as for the application.

4.4 Polar H7 Heart Rate Sensor

Polar H7 HR sensor is compatible with Bluetooth smart ready devices that support heart rate service. A separate application is required to view heart rate data on the receiving device [4]. By Polar, it is recommended to use the H7 HR sensor along with the Polar Beat application, which is described in Section 4.4.1. Figure 4.4 shows the device.

Figure 4.4: Polar H7 Heart Rate Sensor [4].

4.4.1 Polar Beat

The Polar Beat application makes it possible to use a Polar heart rate sensor and get sensor data transferred in real-time to a phone with the application installed. Polar describes the application in the following manner: *Turn your smartphone into a personal trainer* [11]. There is no need for any other accessories than a heart rate sensor and a smartphone with the Polar Beat application installed. In this thesis, the Polar H7 Heart Rate Sensor is used for monitoring heart rate, see Section 4.4 for more information about that wearable.

The features of Polar Beat are built around four keywords; *plan, train, analyze* and *share*. These are explained further in Table 4.7.

Features	Description
Plan	Set and pick training target Polar Beat functions guide to reach the goals
Train & Workouts	A user may choose between 100+ sport profiles During workouts: real-time voice training is available Tracking of distance and mapping of route
Analyze	A quick work out summary is given in application For deeper analysis, Polar refers to Polar Flow application
Share	The application has built-in functionality for sharing workout sessions A user may participate in a challenge with friends or choose to share their own accomplishments

Table 4.7: Polar Beat Features, [11].

The application has also in-app purchases which gives the user the possibility to purchase more extended functionality. The premium features are only available if used together with a specified Polar heart rate sensor. This sensor is not used for testing in this thesis, so further information about the available purchases is not relevant.

Further, key-functionality of the Polar Beat application is that it provides a new sleek and intuitive interface - meaning that the application is more beneficial in use regarding reaching personal goals and training effect. All of the available sport profiles is also mentioned as something unique and very efficient. When signed in to a Polar account, Polar also states that the training data is safe when switching devices. The training data gets transferred to the cloud, and if a user then switches device, the Polar Beat data and history is synced back to the new phone.

Chapter 5
Methodology

This chapter describes the methods used to investigate the thesis' research questions and the reasons for the choices I have made.

The main objective for the research is is to gather network traffic from smart phone applications. This, in order to evaluate the destinations of data sent from associated wearable fitness gear when synchronized with the application. The study also evaluates which permissions each application requests during installation and execution.

In addition, the testing evaluates active trackers on the manufacturers websites available for registered users. Here, more "old-fashioned" web tracking mechanisms may become visible.

The study has been organized into three different stages:

- Document Analysis
- Data Collection
- Data Evaluation

5.1 Document Analysis

Document analysis is the method of reviewing and evaluating documents to receive a qualitative understanding of the analyzed subjects [51]. In this study, the document analysis includes reviewing the privacy policies accompanying the smartphone fitness devices. This, to identify given information about whether data is shared from the applications to other destinations on the Internet. By evaluating the different types of documentation given by Garmin, Fitbit and Polar, it may be possible to gain insight into how these large firms process and store user information.

5.2 Data Collection

The main goal of the data collection is to retrieve as much information as possible about data sharing, both for the mobile applications and the available web interfaces. This is in order to form an overview of correlations between the information given by the companies about sharing and the actual data shared. The collected data is presented in Chapter 6.

5.2.1 Data From Applications

The main component of the data collection consists of capturing network traffic from a smart phone application while it retrieves sensor data from a connected wearable device. The collection setup will only capture incoming and outgoing network data of the running application after it has been synchronized with the fitness device. The complete network capture log will be saved for later analysis. The same procedure will be performed for all three different wearable fitness devices and associated smart phone applications.

For capturing network traffic between the application and the Internet, I have decided to use an Android application named *tPacketCapture Pro*. This is because it allows for application filtering, which makes it possible to isolate traffic for a selected application. The tool is also easy to use and serves the purpose of this study.

An additional goal is to retrieve the different permissions required by each application installed on the smartphone. App permissions are usually listed in the bottom section of the installation page for a given app in Play Store. In order to verify this information, I have chosen another approach for retrieving the permission information from an Android Package Kit (APK). For some of the applications, the list of permissions is available in an online database maintained by the non-profit organization ϵxodus. For the remaining apps, the permissions are obtained with use of the Android build-tool Android Asset Packaging Tool (AAPT). This is a command-line tool that can read meta data from an APK.

5.2.2 Data From Web Portals

For each web page, the data retrieval has been performed when logged into a personal user account. Further, data is collected while navigating different available views in the web portal. The information is collected by the Ghostery browser extension, which lists all active trackers for the page currently viewed. The tool is chosen based upon recommendations from the Norwegian DPA [34].

5.3 Data Evaluation

In the data evaluation, the captured network traffic data sets have been parsed and filtered in order to identify the different network destinations. This is done by the use of Wireshark. Further, the set of different IP address destinations were investigated to gather information about the owner and geographical location. The information is then categorized in tables for comparison with the information from the document analysis.

Each online tracker identified in the data collection is investigated to identify the owner and the purpose of the active tracker. This is mainly done through the database available from Ghostery, with additional information retrieved from other web pages on the topic. Information about the trackers is categorized and presented in tables, see Appendix B. The information is meant to give a general overview of the present tracking companies.

5.4 Challenges and Limitations

5.4.1 Method

When it comes to the application testing, I only look at the traffic flow and not the data concealed in each data packet. One reason for this is encryption, but also because of limited time resources and the scope of the thesis itself. As a result of this, the thesis can not conclude on what specific data is sent where, as I only consider destinations for data exchange. Another effect of this, is that it is hard to comment on the role of each actor.

The method used in this thesis, only considers first-hand data exchange. If or to what degree data is being transferred beyond these destinations is not known. In addition, the apps tested in this thesis are all running on an Android phone. The possible inequalities in the results that may be dependent on the OS are not considered in this thesis.

Regarding the websites; tests are only done in one browser which is Firefox. The policies of when data from third-party cookies may be transferred varies from one browser to another. This may also influence the results of the testing.

Also, the investigations on the websites is performed by only looking at the presence of tracker companies. The thesis will not look into the details of which specific trackers are active from each of these providers.

5.4.2 Thesis

The main challenges when writing a thesis, single handed, is to define objectives and scope which meats prerequisites and time limitations. At the same time, the topic must be in relevance to the technology and development at the time being. This requires some prioritization regarding which aspects to include or exclude from the scope. Identifying areas to focus on is challenging with respect to time limitations and available tools. Good planning and structure is required in order to reach a conclusion in the objectives set early in the process of writing a thesis. To combine several methods to research different aspects is a challenging ordeal and may also be time-consuming.

Also, the topic of this thesis is highly relevant in today's society and dominated by many strong but different opinions. An effect of this might be that some sources referred to in this thesis are biased by political or commercial incentives. Another implication of this is that the process of finding relevant and objective sources can be more challenging.

When evaluating information retrieved from manufacturers of wearable fitness devices, it is hard not to be influenced by personal assumptions related to their intentions with the data collected. When evaluating this in the context of informational privacy leakage, one might jump to the conclusion of data being misused and exploited for the companies' own benefits.

Chapter 6
Results

This chapter presents the tests performed in this thesis. This includes what tools have been used, how the tests are executed and presentation of the results. As presented in Chapter 4, most manufacturers of wearable fitness devices provide both smartphone applications and websites for handling personal activity data. Both these platforms are subject to the testing. This, in order to investigate the the extent of information leakage from the wearable fitness device. The scope of the tests are as follows:

- Application:
  - Access permissions requested on the smartphone
  - First-hand network data propagation from the application to the Internet
- Website:
  - Identification of active trackers embedded in the website

All smartphone applications in the test are installed and evaluated on a Samsung Galaxy S7 Edge with Android 7.0-*Nougat*.

6.1 Application Testing

6.1.1 Tools

In order to test the different fitness applications several tools were required. Table 6.1 gives an overview of all applied tools used for this purpose. The following sections will also give a short introduction to the tools and their associated functionality.

tPacketCapture Pro

tPacketCapture is an Android application and is available for download in Google Play [52]. The application does packet capturing without using any root permissions.

Tool	Objective
tPacketCapture Pro	Obtaining network traffic from the applications
Wireshark	Viewing and analyzing application data flow
exodus	Obtaining permissions in applications
Android Asset Packaging Tool	Obtaining permissions in applications

Table 6.1: Tools used to obtain and analyze data

It enables a Virtual Private Network (VPN) service provided by the Android OS. The pro version, utilized in this thesis, includes a feature called *Application Filtering*. When the filter function is active, this enables to capture communication specific to the chosen application. All captured data is saved in a .pcap file in the external storage of the device running the application. Detailed analysis is obtained by transferring the data to software that handles the file format of the data. In this thesis, Wireshark is chosen to perform this job.

Wireshark

Wireshark is a network packet analyzer. The software displays captured network packets as detailed as possible. In this thesis, Wireshark have been used to import files (.pcap) from the tPacketCapture Pro application in order to give a virtual understanding of the application network traffic communicated from the application. Further, this data has been analyzed and the direct recipients of data from the application is considered [53].

ϵxodus

Exodus privacy is a French non-profit organization that works to protect privacy everywhere. The firm is partnered up with Yale Privacy Lab [54] and F-Droid [55]. Further, the ϵxodus functions as a privacy auditing platform for Android applications and detects behaviors that may be dangerous for user privacy [56]. Examples of such behaviors may be ads, tracking and analytics. The platform provides a report for each analyzed application which shows a list of detected trackers, permissions and suspicious network traffic. With each tracker the platform detects, a brief informational description follows. ϵxodus is able to detect presence of tracker code directly in the APK file. An APK is the package file format used by the Android OS for distribution of mobile apps [57]. The APK files used in analysis by ϵxodus, all originates from Google Play. In this way, they ensure that the applications analyzed, are available for any other user [56].

Android Asset Packaging Tool (AAPT)

AAPT is a tool for viewing, creating and update ZIP-compatible archives (zip, jar, apk) for Android [58]. The tool as a part of the standard Android SDK build-tools, which can be downloaded through the Android SDK manager in Android Studio [59]. In this study, AAPT is used to extract required access permissions for an APK.

6.1.2 Application Permissions

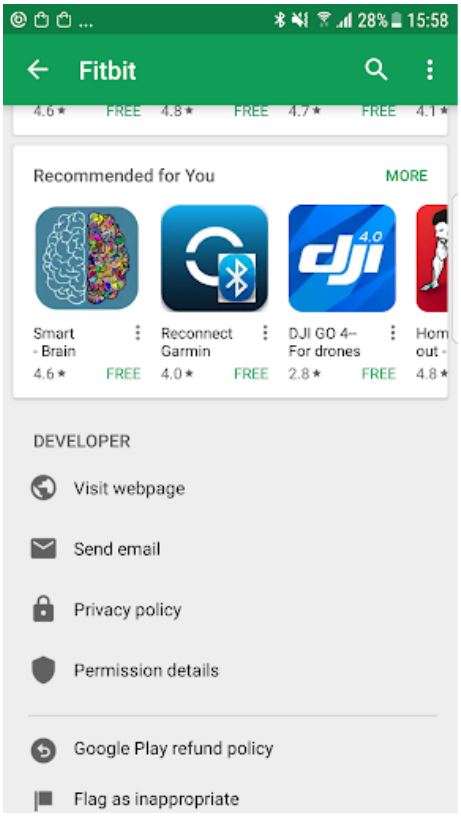
Application permissions are a core part of the security system in Android. All applications are required to request permissions before they can access certain resources or features. The sensitivity of the resource determines whether the request is granted automatically, or whether it requires user approval.

Permissions exist to provide enhanced protection of an Android user's privacy. Android applications must request permissions to access sensitive user data and certain system features [60]. Permissions are divided into several protection levels. For third party applications, two levels exist; *Normal permissions* and *Dangerous permissions*.

The *Normal* permissions represent areas where an application needs to access data or resources outside the application's sandbox, but where there is very little risk to the user's privacy or the operation of other apps [60]. A *Dangerous* permission may be described as a permission that cover areas where the application wants data or resources that involves a user's private information, or could potentially affect the user's stored data or the operation of other apps [60].

The application permissions are evaluated to give an indication of how sensitive user data may be accessed through an application. To get information about the required permissions for a given app, the user must scroll to the bottom of the installation page in Play Store, see Figure 6.1. This may easily be voided when installing a new app. When running the application, each dangerous permission request is prompted to the user, e.g. access to Bluetooth, location, or external storage.

The permissions are retrieved for the apps in this study, either from the research database, [61] or by evaluating the APK with AAPT. All permissions for the respective app are presented in tables below. The permissions contained in red table rows, are permissions that are defined as *dangerous*. The remaining are *normal* permissions. A more detailed description of the different dangerous permissions are described in Appendix A.



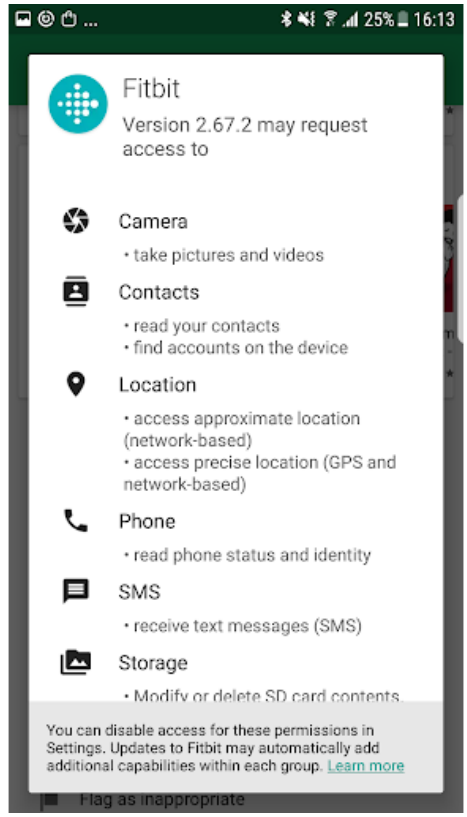


Figure 6.1: Example: Permission Details in Google Play Store

6.1.3 Permissions Results

The permissions for the Fitbit application are presented in Table 6.2. The app requires a set of *dangerous* permissions. Some are related to the core functionality, such as location due to lack of GPS in the Fitbit Alta HR. Further, Bluetooth and Internet are used for data communication. On the other hand, some requests are more difficult to understand at first sight. For example, the permission for camera, contacts, and access to external storage might seem unnecessary for this type of application. When looking closer into different application features, it is shown that these requests are necessary for social networking related to the Fitbit account. In the end, we see that there are some custom permissions included in the table. These are related to communication between servers and the Android device [62].

For the Garmin Connect application, presented in Table 6.3, the list is somewhat more extensive compared to Fitbit. Without looking into the details, this is expected because the Garmin device is a watch with more features and functionality. This

Permission
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_NETWORK_STATE
android.permission.BLUETOOTH
android.permission.BLUETOOTH_ADMIN
android.permission.CAMERA
android.permission.GET_ACCOUNTS
android.permission.INTERNET
android.permission.NFC
android.permission.READ_CONTACTS
android.permission.READ_EXTERNAL_STORAGE
android.permission.READ_PHONE_STATE
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.RECEIVE_SMS
android.permission.USE_FINGERPRINT
android.permission.WAKE_LOCK
android.permission.WRITE_EXTERNAL_STORAGE
com.fitbit.FitbitMobile.permission.C2D_MESSAGE
com.google.android.c2dm.permission.RECEIVE
com.google.android.providers.gsf.permission.READ_GSERVICES

Table 6.2: Permissions Fitbit Application, [12].

includes some extended controls for the phone, such as answering calls and sending Short Message Services (SMSs) with pre-configured text. Other than that, the permissions are quite similar to the ones for Fitbit. The Garmin connect also has a social network platform embedded with interfaces for well known Social Networking Sites (SNSs) such as Facebook and Google. Of other notable entries, Garmin has a set of custom permissions and there is a permission for checking licences with Google Play. Since Garmin Connect is a free app, this is most likely for in-app expansion downloads through Play Store [63].

The Polar Beat application is the one that requires fewest permissions of all the apps. This is expected since the app is a more "light-weight" application for connecting peripheral HR sensors. It does not need access for doing smart watch features as the others. In Table 6.4, we see that this list is the subset of requirements we have seen for the other apps for communication. Another difference between Beat and the others is it does not provide support for social networking within the

application. This is also seen from the lack of permissions such as, access to contacts and camera. As a final observation, we see that the list of permissions includes access to billing for in-app purchases.

Finally, the Polar Flow permissions are presented in Table 6.5. This list does not contain any notable differences from the previous presented. The application features are quite similar to the ones present in the Fitbit app, which explains why their permissions are almost identical. As a note, this application is the only one not using custom permissions.

Permission
android.Manifest.permission.MEDIA_CONTENT_CONTROL
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.BLUETOOTH
android.permission.BLUETOOTH_ADMIN
android.permission.BROADCAST_STICKY
android.permission.CALL_PHONE
android.permission.CAMERA
android.permission.CHANGE_NETWORK_STATE
android.permission.CHANGE_WIFI_STATE
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION
android.permission.GET_ACCOUNTS
android.permission.INTERNET
android.permission.MEDIA_CONTENT_CONTROL
android.permission.MODIFY_AUDIO_SETTINGS
android.permission.MOUNT_UNMOUNT_FILESYSTEMS
android.permission.READ_CALENDAR
android.permission.READ_CALL_LOG
android.permission.READ_CONTACTS
android.permission.READ_EXTERNAL_STORAGE
android.permission.READ_PHONE_STATE
android.permission.READ_SETTINGS
android.permission.READ_SMS
android.permission.RECEIVE_BOOT_COMPLETED

Table 6.3 continued from previous page

Permission
android.permission.RECEIVE_MMS
android.permission.RECEIVE_SMS
android.permission.SEND_SMS
android.permission.SYSTEM_ALERT_WINDOW
android.permission.VIBRATE
android.permission.WAKE_LOCK
android.permission.WRITE_CALL_LOG
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.WRITE_SETTINGS
baidu.push.permission.WRITE_PUSHINFOPROVIDER.com.garmin.android.apps.connectmobile
com.android.vending.CHECK_LICENSE
com.garmin.android.apps.connectmobile.permission.C2D_MESSAGE
com.garmin.android.apps.connectmobile.permission.MAPS_RECEIVE
com.garmin.android.apps.connectmobile.permission.RECEIVE_BROADCASTS
com.garmin.android.apps.connectmobile.permission.RECEIVE_THIRD_PARTY_BROADCASTS
com.google.android.c2dm.permission.RECEIVE
com.google.android.providers.gsf.permission.READ_GSERVICES
org.simalliance.openmobileapi.SMARTCARD

Table 6.3: Permissions Garmin Connect Application, [13].

The permission requests in Table 6.5 are issued from the Polar Beat application. The app requires permissions at a total of 15 permissions. Here, 11 out of 15 permissions are listed as *Dangerous*, while the rest is classified as *Normal*.

In general, it is reasonable to expect that all the applications request the required permissions for regular network socket communication. That is both for Bluetooth communication and network communication including Wi-Fi and Internet access. Even though several of these are defined as dangerous, they are common permissions for all Android applications that either use Bluetooth or network communication. With that said, these resources enable the data propagation from the personal wearable device to the public domain of Internet. Here, the users have to rely on the security measures and protocols used by the developers and manufacturers. In

Permission
android.permission.INTERNET
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_FINE_LOCATION
android.permission.BLUETOOTH_ADMIN
android.permission.BLUETOOTH
android.permission.BLUETOOTH_PRIVILEGED
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.GET_ACCOUNTS
android.permission.VIBRATE
android.permission.WAKE_LOCK
fi.polar.beat.permission.MAPS_RECEIVE
com.google.android.providers.gsf.permission.READ_GSERVICES
com.android.vending.BILLING
android.permission.ACCESS_COARSE_LOCATION

Table 6.4: Permissions Polar Beat Application.

addition, they have to rely on trust and be aware of any risk related to network communication. More questionable are the permissions that request sources for your existing personal information on your smartphone, such as calendar, call logs and contacts. Their reasons for requesting these resources may be justifiable, but they seem highly unnecessary for the core functionality of these applications. Of course, the integration of social networking might bring some value the user, but is not required for the main functionality of a personal wearable fitness device. At the end of the day, the Android permissions has been created as a security mechanism for the end-user, and they all requires the user to grant permission upon installation and usage of the application.

6.1.4 Application Network Traffic

This section will present findings from the network traffic analysis. More specific, the different network destinations for the traffic from a given application has been identified and investigated. The test procedure has been performed with the following steps;

1. Start network capture procedure (tPakcetCapture Pro) for the specific app
2. Create new workout session and gather some sensor data[1]
3. Synchronize the peripheral device with the connected smartphone application

[1]Note that a general running workout is the workout session started on each device.

Permission
android.permission.INTERNET
android.permission.BLUETOOTH
android.permission.BLUETOOTH_ADMIN
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.ACCESS_COARSE_LOCATION
com.google.android.providers.gsf.permission.READ_GSERVICES
android.permission.WAKE_LOCK
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_FINE_LOCATION
android.permission.READ_PHONE_STATE
android.permission.READ_CONTACTS
android.permission.READ_CALENDAR
android.permission.WRITE_CALENDAR
android.permission.GET_ACCOUNTS
android.permission.BLUETOOTH_PRIVILEGED

Table 6.5: Permissions Polar Flow Application.

4. Stop the capture procedure
5. Filter data by destination IP address (Wireshark)
6. Investigate IP address owner

The different destinations captured from the Fitbit network stream are presented in Table 6.6. Firstly, we see that the larger portion of the data goes to Cloudflare. According to a bug report released by Fitbit, they use the Cloudflare platform as their Content Delivery Network (CDN). All their web and Application Programming Interface (API) traffic routes through the Cloudflare domain [64]. Apart from this report, I was not able to find any official information on the relationship between Fitbit and Cloudflare.

The bug, which was revealed by the Google Project Zero in 2017 and named *Cloudbleed*, was a major security issue in the Cloudflare platform. It was caused by a buffer region read violation, and led to exposure wrong memory region to some types of queries. This memory contained private information such as HTTP cookies, authentication tokens, HTTP POST bodies and other sensitive data. The bug was serious because the leaked information was cached by numerous search engines [65]. Among others, Fitbit was named as one of the major customers that might have been affected by the leak. Fitbit themselves claimed that the likelihood of the issue affecting their customers is incredibly low, but that they also have taken actions for

IP	Registered to	Country	%
104.16.66.50	Cloudflare	United States	42,6
104.16.65.50	Cloudflare	United States	29,6
159.122.19.189	SoftLayer Technologies	United States	12,3
151.101.86.110	Fastly	Sweden	5,4
159.122.19.193	SoftLayer Technologies	United States	3,4
54.243.112.173	Amazon.com	United States	3,4
54.243.156.240	Amazon.com	United States	3,3

Table 6.6: Destination lookup for Fitbit Alta HR

counter measures [64].

Further, we see that Fitbit also uses the Swedish company Fastly as a CDN. From the table, it also follows that Fitbit makes use of services from Amazon and SoftLayer Technologies. These are both companies that provide data storage and cloud computing services. What kind of services Fitbit utilize, or what data that is shared, is not known.

The test results for the Garmin Connect application is shown in Table 6.7. Here, we see that Akamai Technologies holds the larger part of the traffic. Akamai is one of the world's largest platforms for content delivery and cloud services, and delivers somewhere between 15 and 20% of all web traffic [66]. Other than Akamai, we see both AT&T, Google and Amazon on the list. It is known that AT&T earlier has provided Garmin with 2G/3G access, but whether this is the reason for their presence in the traffic analysis is not known. I was not able to retrieve any information on the Garmin website about why these destination receive data. The two other companies might be involved for pure analytic purposes, but that would only be a speculation. In the end, Telenor Norway AS also retrieve a small amount of data. As this test was performed in Norway, with both locally bought devices and a Norwegian Internet Service Provider (ISP), this might be related to the location and used for local analytics. Again, this would only be speculations without any public information available from Garmin. Still it is an interesting observation that our current location influences the first-hand data propagation.

Polar Flow has the largest list of different network destinations. As shown in Table 6.8, the major network traffic goes to a domain owned by Polar themselves. This might indicate that Polar hosts their own content service delivery and possibly their own servers. Of the remaining entries in the list, we again see both Google and Amazon. On the other hand, we also see some new entries which receives small amounts of data. Lost Oasis SARL is a French company which delivers shared

IP	Registered to	Country	%
23.52.32.146	Akamai Technologies	Netherlands	47,3
23.13.41.227	Akamai Technologies	Netherlands	36,5
31.13.72.8	AT&T	United Kingdom	3,9
216.58.211.138	Google	United States	1,2
193.212.174.97	Telenor Norge AS	Norway	3,3
193.212.174.131	Telenor Norge AS	Norway	1,6
50.16.243.70	Amazon.com	United States	5,5

Table 6.7: Destination lookup for Garmin Connect

hosting services. Their web page is in French only, and gives very limited information about their services. Next, we have PE Fnutt Consulting, a one person company owned by a Norwegian named Daniel Husand. Further investigation shows that PE Fnutt is a Norwegian ISP. The last one is LeaseWeb Netherlands B.V, which is a cloud hosting provider and CDN [67].

IP	Registered to	Country	%
62.165.171.211	Polar Electro Oy	Finland	72,7
62.165.171.26	Polar Electro Oy	Finland	13,9
216.58.207.234	Google	United States	5,4
13.33.99.128	Amazon.com	United States	3,7
216.58.211.142	Google	United States	1,5
216.58.211.14	Google	United States	0,5
216.58.209.138	Google	United States	0,4
64.233.162.147	Google	United States	0,4
216.58.211.13	Google	United States	0,4
212.85.158.10	Lost Oasis SARL	France	0,3
193.150.22.36	PE Fnutt Consulting Daniel Husand	Norway	0,3
95.211.212.5	LeaseWeb Netherlands B.V.	Netherlands	0,3

Table 6.8: Destination lookup for Polar Flow

As the last application, the Polar Beat application has a rather short list of destinations. The largest amount of data is communicated between an address owned by Google and the app, as Table 6.9 shows. The second largest entry is a Finish telecommunication company called DNA Oyj. Whether Google or DNA Oyj hosts the server for this application is hard to say. It is an interesting observation that the two application offered by Polar does not share any back-end destination addresses.

IP	Registered to	Country	%
216.58.211.14	Google	United States	80,3
62.165.171.211	DNA Oyj	Finland	14,9
172.217.20.67	Google	United States	4,1

Table 6.9: Destination lookup Polar Beat

6.2 Browser Testing

This section describes the testing of the web interfaces available for the wearable fitness equipment used in this thesis. That is, the respective websites from Garmin, Polar and Fitbit.

The browser testing was done by creating a user account on each of the dashboards available from the equipment producers. Further, the account was used to log into their online dashboards for viewing your personal activity data. While doing this, a browser extension, named Ghostery, was used to register all active trackers and cookies on the sites. The observed trackers were registered and further researched.

6.2.1 Tools

Ghostery is a free extension available for several known browsers. In this study, Firefox was used. The software was chosen based on easy access and recommendations by the Norwegian DPA [68]. The following section gives a brief introduction to the tool.

Ghostery Browser Extension

Ghostery is a plug-in extension which is directly installed in the browser. This extends the features provided by the browser. In this case, it provides visible information about cookies and trackers, which usually are obfuscated for the user. The extension supports both desktop and mobile browsers an from 2017 the extension has been available for Mozilla Firefox, Google Chrome, Internet Explorer, Microsoft Edge, Opera, Safari, iOS (Apple's mobile OS), Android and Firefox for Android. Previously, the company was owned by Evidon, Inc., but since February 2017 it got acquired by a German company called Cliqz.

How it works Ghostery monitors all the different web servers that are being called from a particular website, and matches those with a library of data collection tools (trackers) [69]. If a match is found, the add-on extension will categorize the hits into categories and also give information about the cookie-issuing company. Table 6.10 shows the tracker categories defined by the company.

Category	Description
Advertising	Advertising services: Data collection, behavior analysis, retargeting
Comments	Enables comments sections for articles and product reviews
Customer Interaction	Includes chat, email messaging, customer support, and other interaction tools
Essential	Includes tag managers, privacy notices, and technologies that are critical to the functionality of a website
Adult Advertising	Delivers advertisements that generally appear on adult content sites
Site Analytics	Collects and analyzes data related to site usage and performance
Social Media	Integrates features related to social media sites
Audio/Video Player	Enables websites to publish, distribute, and optimize video and audio content

Table 6.10: Tracker Categories, Ghostery [14].

By settings, a user is able to completely block communication with certain web servers. This service is different than opting-out or simply just blocking the actual cookies, this strategy still allows altered communication between the parties.

6.2.2 Results

The results from the website testing is shown in Table 6.11. The first observation of the results is that Fitbit stands out when it comes to number of active trackers. The majority of them belongs to the *Advertising* category, but also has more active trackers in other domains, compared to the other two manufacturers. At the other hand, Polar only has four active trackers on their websites. Garmin is noted with five active trackers. However, a note here, is that the trackers have a certain spread in which categories they are located within. This may be an indication of a minimization of active parties and can further mean that only the parties that are necessary for getting the statistics needed, is involved on the website. Although this is a possibility, it is just a speculation.

In their privacy policies, the manufacturers informs users about their active

Category	Active Trackers	Garmin	Fitbit	Polar
Advertising	AddThis	✓		
	Facebook Impressions	✓		
	Bing Ads		✓	
	Turn Inc.		✓	
	Rocket Fuel		✓	
	DoubleClick Floodlight		✓	
	DoubleClick			✓
	SaleCycle		✓	
	Facebook Custom Audience		✓	
	DoubleClick Ad Exchange		✓	
	Yahoo DOT tag		✓	
	Facebook Pixel		✓	
	IPG Mediabrands		✓	
	TV Squared		✓	
Essential	Tealium	✓		
	Google Tag Manager		✓	✓
	Evidon Site Notice		✓	
Social Media	Facebook Connect	✓	✓	
Site Analytics	Google Analytics		✓	✓
	Yahoo Analytics		✓	
	New Relic			✓
	Mixpanel		✓	
	SessionCam		✓	
	AppDynamics	✓		
#		**5**	**18**	**4**

Table 6.11: Active Trackers Fitness Websites

tracking technologies. Some of them gave concrete examples whereas Polar gave a complete list of their active cookies, see Table 3.4[2]. Polar also noted that their cookies could be changed by them at any time. As my results differ from the list Polar gave in their statement, this indicates that changes have taken place. Although, my results shows fewer active cookies than the policy stated.

Fitbit opens their privacy policy with the following:

-*We believe that transparency is the key to any healthy relationship. At Fitbit, we are*

[2]The list dates back to August 1st, when the policy was set effective

all about healthy attitudes. We appreciate that you are trusting us with information that is important to you, and we want to be transparent about how we use it- [42].

The high number of active trackers on Fitbit's dashboard does not seem to be well reflected in their policy. A high number of trackers is not necessarily an indication that user information is being misused, but if transparency is a goal for the company, there should not be any reason for not informing about which parties are involved on their sites.

In their privacy policy, Garmin give specific examples of their involved third-party providers [5]. This is done to show how tracking a variety of technologies may be used. The results in this thesis are almost in correspondence with their presented examples, see Table 3.2. My results include *AddThis* who was not mentioned in their policy at all. On the other hand, *Splunk* does not show up in my results.

The three providers of fitness gear this thesis concerns about are Garmin, Fitbit and Polar. All of them are global companies with a large user group. Therefore, I would expect that the most-known third parties also is present on these fitness sites. The large companies known for collection large amounts of user data are present on all sites. Google Tag Manager and Google Analytics is present for both Fitbit and Polar, while Facebook is an observed party on Garmin's website.

Another observation is that several tracking companies within the same categorization are active on Fitbit's website. One might speculate why it is necessary to include two separate large actors as Google and Yahoo for site analytics. One reason might be that they provide different services, another reason could be that they use different analytic models and thus produce different results. If you look at the data as your assets, it might make sense to hedge your investment with the major actors on the market to get a maximum return. It might also be the other way around, that both Google and Yahoo has taken the initiative to get access to the data. They are both known for showing interest in collecting big data.

6.2.3 Tracking Companies

In 2016, the project *Princeton Web Census* main goal was to log all the cookies, scripts, and trackers in the various corners of the Internet. The research showed that Google and Facebook is in a more dominant position than ever. Google Analytics was the most popular third party and was present on a total of 61% of all sampled websites in the study [70].

Third-party social networks, like Facebook and Google, may also provide interactive plug-ins or social networking features on websites. Such plug-ins may for example be allowing a user to connect other accounts to Facebook in order to find

friends to add as connections or to "Like" a page. The involvement of third-party social networks may involve that information collection spans to also include the third-party services used. The other way around, first-party services may obtain information about users from the third-party sites. Therefore, use of third-party services on a site, may lead to that a user must deal with separate privacy policies in order to make use of a built-in service.

The results from the mapping of active trackers on the websites shows several active tracker companies. A short description of the companies present in this thesis can be found in Appendix B.

Chapter 7
Discussion

Throughout the thesis I have studied different aspects of privacy leakage in the context of wearable fitness devices and their associated applications. This is done by an evaluation of permissions needed in order to download and use the connected applications belonging to each fitness wearable. The available websites from the manufacturers have also been studied in order to map the active tracking technologies on these sites. The results from this part of the analysis are also seen in context of the privacy policies provided by each manufacturer.

By studying several privacy policies and comparing the provided information with the results of my testing, the thesis aims to give an indication of whether the data exchange is what to be assumed from a user point of view. The following section will discuss the findings from previous chapters and relate this to the research questions listed in Section 1.1.

7.1 Is the information provided by the manufacturers sufficient for the users to fully understand the extent of the data sharing?

In general, the privacy policies are quite easy to read and the information is often well organized. The technical information included in these policies, may be of great importance and have the tendency to be tucked away in the textual representation. In several cases, the text references to information that may be found in a completely different document. In this way, the compact representation may fool the reader to the impression that the document is not a complex document at all. The reality is however, that a referral in the privacy policy may lead the user into a maze of several documents to be considered. If this is the precedence of how privacy policies are defined, then it is hard to know if the maze even has an ending. In addition, the documents appear as compact, but are meant to embrace all the services offered by the provider. They are written in such a way that all responsibilities and requirements

are covered with short vague statements. From a legal point of view, the policies may be sound and robust, but from a user perspective they are not very informative.

Related to the analysis of the websites, it turns out that only one agreement specifically lists the cookies active in their website domain. The other policies only mention use of different tracking mechanisms that *may* be enabled. All policies state that the trackers may be changed at any time. This is reasonable as the dynamics of the websites involves new features and technologies that requires some sort of trackers. Although, in my opinion, the policies should be more transparent on the coarse purposes for tracking mechanisms used in their websites.

The myth that the agreements themselves do not provide intelligible information may have some truth to it.

A scenario may be that a user wishes to build up a complete overview of all different parties that receive information, and just as important; how the information is used. The user will most likely do this by reading relevant privacy polices. Initially, the starting point will be to look at the policy of the main service provider. Based on experience from this study, the user will have to navigate through a chain of documents from different affiliates. An average user will probably not take the effort to traverse the tree of documents that avails. Another problem that arises when a user wishes to investigate involved third parties is that is is hard to explore policies of a party that is not mentioned in the first place. How is a user meant to read the privacy policy of an unknown source? And utter and foremost, is the user supposed to reconcile with the reality of other companies ruling over their data when they know that other guidelines for handling it applies?

Another property of the privacy policies is that they are written to cover all the services offered by the company. This may be problematic when companies provide many services. Not only is it harder to define the policies in the first place, but updates would also be significantly more work as this would lead to very rapid update-rates. This especially goes if the companies actually would include lists of involved third parties in their policies. Moreover, the use of company-wide privacy policies and terms of use, which often apply to a variety different devices and services, makes is harder for end users to determine which specific aspects of the policies apply to the different parts of the services offered.

7.2 Are there any undisclosed parties that receive information about the users?

To answer the research question directly; yes, there are undisclosed parties that receive information about the users. This is because there is given little or none

information about the individual recipient in the first place. Of course, this depends on how you define undisclosed parties.

All privacy policies reviewed in this thesis informs of third-party service providers and they all confirm such intervention in their services. Some give examples of how the technology may be used, some even name providers involved and also what role they play. Common to these, however, is that they also announce that the third parties involved may be changed at any time. So, what is really the point of giving concrete examples if there are frequent changes to the list of third-party providers? How is the user beneficial of knowing outdated information? Even though more specific examples are given, they do not give information about which tracking technology is enabled in the different services they offer. Dependent on the frequency of change among third parties, it is to some extent understandable if the privacy policies do not maintain a complete list of third-parties. Another reason may also be that this is sensitive information in context of business and collaborations. However, this study has shown that it is fairly easy to disclose some information about the parties involved. In this way, a user at least can be able to reach the relevant privacy policy.

Another aspect of involved third parties, is to understand who they really are and which services they actually provide. Given a list of named third-party companies, it has shown to still be quite challenging to retrieve specific information about objective and purpose in the given context. Their websites usually all state high-level information about their services involving keywords such as; analytics, big data, software as a service etc.. For a normal user with no technical background, this could mean anything (or nothing).

Throughout this research, a recurring observation has been that available information about all involved parties are somewhat limited. Given all results from this thesis, it is still seem insurmountable to gain a full understanding of the complete data flow and its purpose. In my opinion, the device manufacturer should be responsible for enlightening the type of third parties involved, their role, and the type of data sent to each of them. This should also include the third-party's responsibility of the data. All of this should be available and easy to perceive in their privacy policy.

The presence of social networks embedded in all applications is something that also should be noted. Although all privacy policies mention this to some extent, it is still an open question of whether these networks imply some sort of personal data aggregation. Especially interesting is the question of whether the fitness device sensor data becomes available for the social network providers. In that case it will enrich their already extensive data profiles on individuals.

7.3 What incentives do the manufacturers have for collecting user data?

First of all, it reasonable to assume that some of the involved data are used for analyzing their service performance. This is often services provided by third parties, which explains the data sharing to such site analytic companies. Further, it is also in the manufacturers interest to establish an understanding of how their users utilize their products. For this, one might speculate about the extent of the data used to evaluate the user behavior. All devices evaluated in this study requires some sensitive information in order to provide all available services. In combination, the manufacturers are in position to build quite detailed profiles on their users, including their activity data.

Another aspect is whether the manufacturers sell data to other parties. In later time it has become a known practice for tech companies to sell information and data. There is a big market for data in general, varying from user specific data to other non-specific sensor data. Wearable fitness device manufacturers are in position of both user and sensor data which may represent a great value in an open market. One may speculate whether data has become a major component in their business model if there are great revenues in selling data. It might even be of greater value than the revenue from the device itself. Of the three companies evaluated, Polar is the only one talking explicitly about selling personally identifiable information. They state that they do not sell this type of information for promotional purposes. It is hard to say what *promotional purposes* comprises, and does this mean that they might sell for other purposes?

7.4 How is the distribution of responsibility for handling the personal data in question?

An important question is how the responsibility for securing data is agrees between multiple chains of third-parties and affiliates. This is something that is completely opaque to the end-user where we have to rely on the soundness of agreements and protocols between the parties involved. How they define these rules and agreements should be more transparent to the end user. This includes information about how the propagated data is securely stored and what responsibility entities have in the transmission of the data. That is especially important for the sharing of sensitive user data. This is also relevant in the context of a request for deleting user information. Will the aggregated data be deleted from all parties, or just by the manufacturer. The recent events of the Facebook scandal has shown that there even seem to be some discrepancy on the meaning of such agreements.

The GDPR has clearly defined that binding agreements between the different

actors involved in data processing should exist. When a controller decides that a processor should be involved, the controller needs to have a written contract in place. So far, no template-contract has been developed. Nor specific requirements for what the contract should include. However, what is written is clear; A processor may only utilize data processed on behalf of a controller as instructed.

No matter how much responsibility is sought to be imposed on providers of services, it is also important to remember that in almost any case the user willingly has shared the information in the first place. One responsibility that should be placed on the providers is however, the commitments related to informing their users in the best an most understandable manner. A user should at least be given the possibility to easily understand the implications by using a service.

In general, it seems like a leak or data breach is a prerequisite for revealing relationships and collaborations between first and third parties. At least before such information is presented to the majority of end users, often through the media. It is fair to assume that the average user would like to know about collaborations early on in the procurement of a product. The assessment of a product should include sufficient information about the product as a whole. The reality is that a fitness device includes several different suppliers of services than the brand itself. As this may also affect a user's attitude towards specific devices, such information should also be provided.

This master thesis has shed light on several flaws in the current state of how data sharing is communicated through the manufacturers to the end users. There privacy policies do not give sufficient information in order to give an average user an understanding of how data is propagated and preserved. This is something that should be improved, mainly by the manufacturers, through implementation of stricter requirements and regulations on companies that provide such services. The recent introduction of resolutions such as GDPR shows that the topic has been brought to the attention of authorities on a global scale. Hopefully, new regulations will be enforced and thereby bring important changes to the future.

References

[1] Inc. Fitbit. Fitbit Alta HR. https://www.fitbit.com/altahr, 2017. [Online; accessed 31-October-2017].

[2] Garmin Ltd. Garmin Forerunner 235 Overview. https://buy.garmin.com/en-US/US/p/529988, 2017. [Online; accessed 23-October-2017].

[3] https://www.amazon.com/Polar-M400-Smart-Sports-Watch/dp/B00Q6TPRV6. [Last accessed: 07-March-2018].

[4] Polar. Polar h7 user manual. https://support.polar.com/e_manuals/H7_Heart_Rate_Sensor/Polar_H7_Heart_Rate_Sensor_accessory_manual_English___.pdf. [Last accessed: 07-March-2018].

[5] Garmin Ltd. Privacy Statement for Garmin Connect and Compatible Garmin Devices. https://connect.garmin.com/en-US/privacy#waysGarminCollects, 2017. [Online; accessed 25-October-2017].

[6] Fitbit. Cookies and similar technologies. https://www.fitbit.com/no/legal/cookie-policy. [Last accessed: 11-March-2018].

[7] Polar. Polar Privacy Policy. https://flow.polar.com/privacyPolicy. [Last accessed: 06-February-2018].

[8] Fitbit Inc. Fitbit app. https://www.fitbit.com/no/app#. [Last accessed: 09-March-2018].

[9] Garmin. Garmin forerunner 230/235 user manual. http://static.garmin.com/pumac/Forerunner_230_OM_EN.pdf. [Last accessed: 08-March-2018].

[10] Polar. Polar m400 user manual. https://support.polar.com/e_manuals/M400/Polar_M400_user_manual_English/manual.pdf. [Last accessed: 10-March-2018].

[11] Polar. Products. https://www.polar.com/us-en/products. [Last accessed: 06-March-2018].

[12] Fitbit Results Exodus Privacy Tool. https://reports.exodus-privacy.eu.org/reports/115/. [Last accessed: 13-March-2018].

[13] Fitbit Results Exodus Privacy Tool. https://reports.exodus-privacy.eu.org/reports/1832/. [Last accessed: 15-March-2018].

[14] Ghostery Chrisopher Tino. What are the new tracker categories? https://ghostery.zendesk.com/hc/en-us/articles/115000740394-What-are-the-new-tracker-categories-. [Last accessed: 01-March-2018].

[15] Stiftelsen Elektronikkbransjen. Bransjetall og statistikk. https://www.elektronikkbransjen.no/artikler/bransjetall-og-statistikk/375828. [Last accessed: 25-March-2018].

[16] Alex Hern at The Guardian. Fitness tracking app strava gives away location of secret us army bases. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases. [Last accessed: 25-March-2018].

[17] Jon Russel at TechCrunch. Fitness app strava exposes the location of military bases. https://techcrunch.com/2018/01/28/strava-exposes-military-bases/. [Last accessed: 25-March-2018].

[18] Oxford English Dictionary. Privacy. http://www.dictionary.com/browse/privacy. [Last accessed: 28-March-2018].

[19] General data protection regulation (gdpr). https://gdpr-info.eu/. [Last accessed: 01-March-2018].

[20] Norwegian Data Protection Authority. About Us. https://www.datatilsynet.no/en/about-us/. [Last accessed: 24-February-2018].

[21] Personopplysningsloven. https://lovdata.no/dokument/NL/lov/2000-04-14-31?q=personopplysningsloven. [Last accessed: 01-March-2018].

[22] Personopplysningsforskriften. https://lovdata.no/dokument/SF/forskrift/2000-12-15-1265. [Last accessed: 01-March-2018].

[23] Official Journal of the European Communities. Directive 95/46/ec of the european parliament and of the council. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en. [Last accessed: 28-March-2018].

[24] EUGDPR. Gdpr key changes. https://www.eugdpr.org/key-changes.html. [Last accessed: 01-March-2018].

[25] Information Commissioner's Office. Guide to the general data protection regulation - key definitions. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/. [Last accessed: 26-March-2018].

[26] General data protection regulation (gdpr), chapter 3. https://gdpr-info.eu/chapter-3/. [Last accessed: 02-March-2018].

[27] Information Commissioner's Office. Guide to the general data protection regulation - data protection officers. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/. [Last accessed: 26-March-2018].

[28] Janice C. Sipior, Burke T. Ward, and Ruben A. Medoza. Online privacy concerns associated with cookies, flash cookies, and web beacons. *Journal of Internet Commerce*, 2011. [Last accessed: 02-March-2018].

[29] European Commission. Cookies. http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm. [Last accessed: 24-February-2018].

[30] Internet Engineering Task Force (IETF). HTTP State Management Mechanism. https://tools.ietf.org/pdf/rfc6265.pdf. [Last accessed: 24-February-2018].

[31] Lov om elektronisk kommunikasjon. https://lovdata.no/dokument/NL/lov/2003-07-04-83?q=e-kom. [Last accessed: 24-February-2018].

[32] Steven Englehardt and Arvind Narayanan. Online tracking: A 1-million-site measurement and analysis. Technical report, Princeton University, http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf, 2016. [Last accessed: 28-February-2018].

[33] Ashkan Soltani, Shannon Canty, Quentin Mayo, Lauren Thomas, and Chris Jay Hoofnagle. Flash cookies and privacy. Technical report, University of Berkeley, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.401.7830&rep=rep1&type=pdf, 2009. [Last accessed: 03-March-2018].

[34] Datatilsynet. Det store datakappløpet. https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/kommersialisering-norsk-endelig.pdf. [Last accessed: 13-March-2018].

[35] Datatilsynet and Teknologirådet. Personvern 2018 - tillit og følelser. https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/Tilstand-og-trender-2018.pdf. [Last accessed: 27-March-2018].

[36] Andrew Hilts and Christopher Parsonsand Jeffrey Knockel. Every step you fake: A comparative analysis of fitness tracker privacy and security. https://openeffect.ca/reports/Every_Step_You_Fake.pdf. [Last accessed: 27-March-2018].

[37] WhatIs.com. privacy policy. http://whatis.techtarget.com/definition/privacy-policy. [Last accessed: 21-March-2018].

[38] Adyen. Privacy Policy. https://www.adyen.com/policies-and-disclaimer/privacy-policy. [Last accessed: 21-February-2018].

[39] Garmin. Garmin Companies. https://www.garmin.com/en-US/legal/garmin-companies. [Last accessed: 21-February-2018].

[40] Garmin. Keeping Data Safe at Garmin. https://www.garmin.com/en-US/legal/security. [Last accessed: 22-February-2018].

[41] Inc. Fitbit. Updates to our Privcy Policy and Terms of Service. https://help.fitbit.com/articles/en_US/Help_article/2243, 2017. [Online; accessed 01-November-2017].

[42] Inc. Fitbit. Fitbit Privacy Policy. https://www.fitbit.com/no/legal/privacy-policy, 2017. [Online; accessed 31-October-2017].

[43] Privacy Shield Framework. Privacy shield overview. https://www.privacyshield.gov/Program-Overview. [Last accessed: 12-March-2018].

[44] European Commission. What are binding corporate rules. https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en. [Last accessed: 28-March-2018].

[45] The Guardian. Revealed: 50 million facebook profiles harvested for cambridge analytica in major data breach. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. [Last accessed: 22-March-2018].

[46] The Guardian. The cambridge analytica files 'i made steve bannon's psychological warfare tool': meet the data war whistleblower. https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump. [Last accessed: 22-March-2018].

[47] CNET. Fitbit alta hr specification. https://www.cnet.com/products/fitbit-alta-hr/specs/. [Last accessed: 06-March-2018].

[48] Dictionary.com. Widget. http://www.dictionary.com/browse/widget. [Last accessed: 09-March-2018].

[49] Manuals for forerunner 235. https://support.garmin.com/support/manuals/manuals.htm?partNo=010-03717-54. [Last accessed: 28-March-2018].

[50] Garmin. Garmin connect mobile. https://buy.garmin.com/en-US/US/p/125677. [Last accessed: 09-March-2018].

[51] Glenn A. Bowen. Document Analysis as a Qualitative Research Method. http://www.emeraldinsight.com/doi/pdfplus/10.3316/QRJ0902027. [Last accessed: 15-January-2018].

[52] Google Play. tpacketcapture pro. https://play.google.com/store/apps/details?id=jp.co.taosoftware.android.packetcapturepro. [Last accessed: 15-March-2018].

[53] About wireshark. https://www.wireshark.org. [Last accessed: 28-March-2018].

[54] Yale University. Information society project yale law school - privacy lab. https://privacylab.yale.edu. [Last accessed: 15-March-2018].

[55] F-Droid. What is f-droid. https://f-droid.org. [Last accessed: 15-March-2018].

[56] Exodus. Exodus privacy. https://exodus-privacy.eu.org. [Last accessed: 15-March-2018].

[57] AndroidPit. What is and apk file and how do you install one? https://www.androidpit.com/android-for-beginners-what-is-an-apk-file. [Last accessed: 15-March-2018].

[58] Embedded Linux Wiki. Android aapt. https://elinux.org/Android_aapt. [Last accessed: 17-March-2018].

[59] Android Developer. Android studio. https://developer.android.com/studio/index.html. [Last accessed: 17-March-2018].

[60] Android Developers. Permissions overview. https://developer.android.com/guide/topics/permissions/overview.html. [Last accessed: 14-March-2018].

[61] Exodus Privacy Tool. https://reports.exodus-privacy.eu.org. [Last accessed: 13-March-2018].

[62] Google Cloud Messaging. Migration from c2dm. https://developers.google.com/cloud-messaging/c2dm. [Last accessed: 17-March-2018].

[63] Android Developers. App app licensing. https://developer.android.com/google/play/licensing/index.html. [Last accessed: 17-March-2018].

[64] Fitbit. Fitbit response to cloudflare security issue. https://eng.fitbit.com/fitbit-response-to-cloudbleed/. [Last accessed: 18-March-2018].

[65] Cloudflare. Incident report on memory leak caused by cloudflare parser bug. https://blog.cloudflare.com/incident-report-on-memory-leak-caused-by-cloudflare-parser-bug/. [Last accessed: 18-March-2018].

[66] Reuters. Strong dollar hurts akamais' profit forecast, shares fall. https://www.reuters.com/article/us-akamai-tech-results/-strong-dollar-hurts-akamais-profit-forecast-shares-fall-idUSKBN0NJ2IV20150428. [Last accessed: 18-March-2018].

[67] LeaseWeb. www.leaseweb.com. [Last accessed: 18-March-2018].

[68] Datatilsynet. Personvern - tilstand og trender 2016. https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/personvernrapport/personvernrapporten-2016.pdf. [Last accessed: 22-March-2018].

[69] Christopher Tino at Ghostery. How does Ghostery work? https://ghostery.zendesk.com/hc/en-us/articles/115000733453-How-does-Ghostery-work-. [Last accessed: 26-February-2018].

[70] Russel Brandom at The Verge. Google and facebook still dominate tracking on the web. https://www.theverge.com/2016/5/18/11692228/google-facebook-web-tracking-survey-advertising. [Last accessed: 28-February-2018].

[71] Android Developers. Manifest.permission. https://developer.android.com/reference/android/Manifest.permission.html#SYSTEM_ALERT_WINDOW. [Last accessed: 15-March-2018].

[72] Facebook. Impressions. https://www.facebook.com/business/help/675615482516035?helpref=search&sr=2&query=facebook%20impressions. [Last accessed: 28-February-2018].

[73] Microsoft. Faq. https://secure.bingads.microsoft.com. [Last accessed: 28-February-2018].

[74] About rocket fuel. http://rocketfuel.com/se/old/about-rocket-fuel#what-we-do. [Last accessed: 24-March-2018].

[75] Google. Types of cookies used by google. https://policies.google.com/technologies/types?hl=en. [Last accessed: 24-March-2018].

[76] Google Inc. About Floodlight. https://support.google.com/dcm/partner/answer/2823388?hl=en. [Last accessed: 26-February-2018].

[77] Google Inc. What is Floodlight. https://support.google.com/ds/answer/7298761?hl=en. [Last accessed: 26-February-2018].

[78] Google. The doubleclick ad exchange. https://static.googleusercontent.com/media/www.google.com/no//adexchange/AdExchangeOverview.pdf. [Last accessed: 28-February-2018].

[79] About salecycle. https://apps.ghostery.com/apps/salecycle. [Last accessed: 01-March-2018].

[80] Dot tags. https://developer.yahoo.com/gemini/guide/v1-api/dottags/. [Last accessed: 24-March-2018].

[81] About facebook pixel. https://www.facebook.com/business/help/742478679120153. [Last accessed: 24-March-2018].

[82] Interpublic group of companies. https://en.wikipedia.org/wiki/Interpublic_Group_of_Companies. [Last accessed: 24-March-2018].

[83] Tv squared. https://tvsquared.com/. [Last accessed: 24-March-2018].

[84] Ghostery. About AddThis. https://apps.ghostery.com/en/apps/addthis. [Last accessed: 26-February-2018].

[85] What is site notice. https://www.evidon.com/resources/glossary/gs-product/what-is-site-notice/. [Last accessed: 24-March-2018].

[86] Google. Google tag manager. https://developers.google.com/tag-manager/. [Last accessed: 24-March-2018].

[87] Google Analytics. Tracking Code Overview. https://developers.google.com/analytics/resources/concepts/gaConceptsTrackingOverview. [Last accessed: 27-February-2018].

[88] Yahoo! Yahoo analytics. https://policies.yahoo.com/ie/nb/yahoo/privacy/topics/analytics/index.htm. [Last accessed: 24-March-2018].

[89] Google. How is mixpanel different? https://help.mixpanel.com/hc/en-us/articles/115004702483-Getting-started. [Last accessed: 24-March-2018].

[90] About sessioncam - in their own words. https://apps.ghostery.com/apps/sessioncam. [Last accessed: 24-March-2018].

[91] Reuters. New relic inc (newr.n). https://www.reuters.com/finance/stocks/companyProfile/NEWR.N. [Last accessed: 28-February-2018].

[92] Appdynamics. https://en.wikipedia.org/wiki/AppDynamics. [Last accessed: 24-March-2018].

[93] About appdynamics - in their own words. https://apps.ghostery.com/en/apps/appdynamics. [Last accessed: 24-March-2018].

Appendix A
Dangerous Permissions

This appendix gives a description of the *Dangerous* permissions present in the applications tested in this thesis. Information about the different permissions is taken from Android's developer pages [60].

- **android.permission.ACCESS_COARSE_LOCATION**: allows an application to access the device's approximate location by the use of different sources, i.e. mobile network database [12].
- **android.permission.ACCESS_FINE_LOCATION**: gives the application access to the fine location of the device, i.e. by using the GPS on the device.
- **android.permission.BLUETOOTH**: this permission allows an application to view the configuration of the local Bluetooth connections on the connected device and to make/accept connections with paired devices.
- **android.permission.BLUETOOTH_ADMIN**: this lets the application configure the local Bluetooth configurations. This includes discovery and establish pairing with remote devices.
- **android.permission.CALL_PHONE**: to initiate calls without going through the Dialer user interface for the user to confirm the call.
- **android.permission.CAMERA**: This permission is required to be able to access the camera device. Allows the application to take pictures and videos with the camera. Also gives the application permission to collect images that the camera is seeing at any time.
- **android.permission.CHANGE_WIFI_STATE**: permission that grants the application to connect and disconnect from Wi-Fi access points and also to make changes to configured Wi-Fi networks.
- **android.permission.INTERNET**: Allows an application to create network sockets.
- **android.permission.READ_CALENDAR**: this gives the application permission to read all calendar events stored on the device running the application. A malicious application can use this to send calendar events to other people [13].

- **android.permission.WRITE_CALENDAR**: Allows an application to write the user's calendar data.
- **android.permission.READ_CALL_LOG**: This permission allows an application to read the user's call log.
- **android.permission.READ_CONTACTS**: Gives an application the permission to read the user's contacts data.
- **android.permission.READ_PHONE_STATE**: allows read only access to the phone state. This includes the phone number of the device, current cellular network information, status of any ongoing calls and a list of any phone accounts that are registered on the device.
- **android.permission.READ_SMS**: gives an application allowance to read SMS messages.
- **android.permission.RECEIVE_MMS**: Allows an application to monitor incoming Multimedia Messaging Service (MMS) messages.
- **android.permission.RECEIVE_SMS**: Allows an application to receive SMS messages.
- **android.permission.SEND_SMS**: The application is given permission to send SMS messages.
- **android.permission.SYSTEM_ALERT_WINDOW**: Allows an app to create windows on the device. These windows are shown on top of all other apps. Very few applications should use this permissions; these windows are intended for system-level interaction with the user [71].
- **android.permission.WRITE_CALL_LOG**: Gives the application permission to write (but not read) the user's call log data.
- **android.permission.WRITE_EXTERNAL_STORAGE**: Allows an application to write to external storage (i.e. SD Card)
- **android.permission.GET_ACCOUNTS**: Allows access to the list of accounts in the Accounts Service.

Appendix B
Tracking Companies

This appendix briefly informs about each tracking company observed in the website testing of this thesis. Organized according to functionality as defined by Ghostery, see Table 6.10.

B.1 Advertising

Facebook Impressions is a common metric used by the online marketing industry [72]. The metric logs how many times an instance of an ad is shown on a screen for the first time. Impressions are counted in the same way, regardless of advertising type (e.g. picture or video). This means that a video does not need to be clicked in order to be counted as an impression.

Bing Ads formerly named Microsoft adCenter and MSN adCenter, is a Pay-Per-Click (PPC) advertising system [73]. According to the Bing Ads FAQ-site, their customer's business can reach a large an unique audience made up of millions of people who search every day. Advertisers bid on how much they are willing to pay per click on their ads. The placement of the advertisements may on the top or to the right of Bing, Yahoo and MSN search results. An advertiser may also choose to target the ads towards different geographic regions, times or days of the week, and even demographics. Due to the system being based upon PPC, an advertiser places bids based on how much they are willing to pay per click on an ad. Further, the show space of an ad is auctioned out. The position of the ad itself is based on several factors [73];

1. How closely the ad an website fit with the terms that are searched (relevance)
2. How the bid compares to other bids in the Bing Ads auction
3. How strongly the ad has performed in the past and how often it has been clicked (Click-Through Rate (CTR))

The stronger the position the ad has in relation to these factors, the better chances of winning the best placement position.

Turn Inc. Turn is an online data-driven technology and software services company. Every interaction with mobile apps, web content or activity on social networks creates valuable new consumer data. The firm collects and centralizes data about who the users are, their purchasing preferences and their geographic location.

Anonymous, Pseudonymous and PII is collected, whereas the anonymous and the PII is shared with third parties.

Rocket Fuel Rocket Fuel Inc. is a technology company based in the United States, which provides solutions for digital advertisement. They specialize in services within Big Data and artificial intelligence for targeted advertising [74].

DoubleClick is a subsdiary of Google, and has been since 2007. When founded, DoubleClick was known as one of the earliest *Application Service Provider*. Google makes use of different cookie names to link user activity across devices if the user previously has signed in to their Google account on another device [75].

DoubleClick Floodlight (Google) DoubleClick Floodlight is a conversation tracking system, [76]. The system consists of tags that track activity on a web site, along with features for adding conversation data to a conversation report. Floodlight uses a cookie to be made aware of repeating visits from a specific browser. The recognition of users may happen by analyzing a user's cookie ID or mobile ID, which becomes the user ID, [77].

DoubleClick Ad Exchange DoubleClick Ad Exchange is a real-time marketplace for buying and selling display advertising space [78].

SaleCycle is a United Kingdom (UK) based company. With their focus on returning potential customers to a website in order to complete their transaction, they are enabling a site owner to recover what could have been lost sales [79].

Facebook Custom Audience is a service that any advertiser on Facebook can make use of. The service allows advertisers to *retarget* their websites, this means that an advertiser can target people who have previously visited the advertiser's website. The *custom* part of the service name gives the advertiser the ability to set their own preferences regarding who Facebook more specifically should target with the active advertisement. In this way, the audience an advertiser reaches is the people who is of greatest interest.

Yahoo DOT Tag The DOT tag is the universal tag of Yahoo. It is a single pixel that may be utilized both on websites and mobile apps. By using one DOT tag it is possible to record all events for conversation and tracking an retargeting. A tag is identified with the advertiser, the same tag can then be used across multiple Yahoo systems [80].

Facebook Pixel Facebook Pixel is a web beacon (pixel) provided by Facebook. The beacon is a small code snippet which is embedded into a third party website or email. The beacon is connected to a back-end hosted by Facebook where the owner can configure what user activity to monitor for the site where the pixel is located. This includes activities such as searches, purchases and content views. Facebook Pixels are mainly used for targeted advertisement provided by Facebook [81].

IPG Mediabrands The Intepublic Group of Companies (IPG) is a world leading American advertising company. The IPG Mediabrands entity consisting of several subsidiary media agencies withing different domains such as marketing, public relations, sports marketing, talent representation, and health care [82].

TV Squared TV Squared is a company specialized in analytic for Direct Response Television (DRTV) advertising. They provide solutions for tracking the immediate digital impact of an advertisement broadcast across different devices. This enables brands to plan and analyze results of TV campaigns [83].

AddThis is one of the largest social infrastructure and data platform creating easy ways for users to share content [84]. The company provides publishers with a small amount of HTML and JavaScript code that displays sharing tools on pages and captures information about their usage.

The providers of websites in this thesis, states that services from addthis.com is implemented to make sure that a user sees the updated count if they share a page and return to is before their own share count cache is updated.

The privacy information from Ghostery shows that AddThis collects *Anonymous data*, *Pseudonymous data* and *PII*. Both aggregate data and anonymous data is shared with third parties whilst the data retention is four to five years [84].

B.2 Essential

Evidon Site Notice A site notice from Evidon ensures that the website complies with EU ePrivacy Directive. The site notice enables a user to receive a warning, and to give consent, before any tracking technologies is installed [85].

Google Tag Manager A Google Tag Manager is used to manage tags and makes it possible to add and update tags without editing the source code of the website [86]. It is possible to enable the management both on Google tags such as AdWords or Google Analytics but also on non-Google tags [86].

Tealium is also a US company and provides tag management technology. The Tealium Universal Tag is a simplified tag that can work with various combinations of web analytics and digital marketing solution providers. Tealium IQ Tag Management is used to help manage various analytic services and cookie and pixel tag technologies enabled by a company [5].

B.3 Site Analytics

Google Analytics tracks and reports website traffic and is integrated with the company's ad-targeting systems. It works by by the inclusion of a block of JavaScript code on pages on the website. When a visitor enters a website, the JavaScript code references a JavaScript file which then executes the tracking for Analytics. Further, the information retrieved from the website is sent to the Analytics server via a list of parameters attached to a single-pixel image [87]. The data collected by Google Analytics stems from the following sources;

- The HTTP request of the user
- Browser/system information
- First-party cookies

This means that Google Analytics is used to track site statistics and user demographics, interests and behavior on websites.

Yahoo Analytics A tool used to collect data about users on websites. The data normally include cookie data, device ID, IP address, clicked links, position, apps installed on the device and ads shown on the websites and apps [88]. The data does not include PII.

MixPanel MixPanel is a software tool that provide services for online business analytics. Their services tracks user interaction with websites and mobile applications. In detail, the tool let you monitor certain specific events of interest in the site or app, such as image uploads or button click patterns [89].

SessionCam SessionCam delivers services within Visible Web Analytics, Session Replay and Heatmap technology. Their services is used to gain insight into previously unseen customer behavior. The company collects anonymous data and does not share data with third parties [90].

New Relic is an American software analytic company based in San Francisco. The company delivers solutions to its customers enabling them to collect, store and analyze software data in real time [91].

AppDynamics AppDynamics provides applications performance management and IT operations analytics. This includes monitoring and control of websites and applications in order to provide services at the expected level [92].

According to Ghostery's privacy information, appDynamics collects both *Anonymous* and PII. Aggregate data is shared with third parties [93].

B.4 Social Media

Facebook Connect gives a user the possibility to connect their Facebook account and credentials across the web. When Facebook Connect is utilized by users, this allows that website to collect information that they have placed on the SNS themselves.