Assessment of Measurable Privacy for IoT Consumer Products

Christoffer Ramsvig Thambirajah

Thesis submitted for the degree of
Master in Programming and Network
60 credits

Department of Informatics
Faculty of mathematics and natural sciences

UNIVERSITY OF OSLO

Spring 2019

Assessment of Measurable Privacy for IoT Consumer Products

Christoffer Ramsvig Thambirajah

Assessment of Measurable Privacy for IoT Consumer Products

http://www.duo.uio.no/

Printed: Reprosentralen, University of Oslo

Abstract

Recently, personal privacy has increasingly started coming to people's attention, as we are digitally more connected to each other. The development of new mobile products connected to the Internet are starting to take a larger place in people's everyday lives. Such products go by the term *"Internet of Things" (IoT)* and are now starting to concern more people with regards to the privacy issues. Regulations from EU like General Data Protection (GDPR) have been introduced, trying to make companies more responsible when processing sensitive data. Still, privacy concerns in common people's day to day living exist. Most of these concerns tend to arise because people do not process enough insight or knowledge on how their data are being treated within the IoT products. This is how the data is being distributed, stored and used by the company creating the product. In other words, a need for presenting technical information in a more understandable and precise manner should be provided. Even if people don't ask for a solution to this problem, we have earlier shown that a simple and understandable approach to this type of technical information is valuable to people when choosing a product. By presenting information previously unavailable to people in a more understandable way the consumer can take charge of choosing how his private data are to be treated.

This thesis will investigate possible ways to measure the level of privacy in a generic way so that said measurement can be used in presenting the privacy of each IoT product to the end customer. It also addresses a possible way of presenting the information to the end customer.

Another important part of this thesis is analyzing an actual IoT product. This analysis will deliver valuable information towards the mapping of different technical parameters, as well as looking at different privacy measurement methods.

Finally, the thesis will propose a measurement method applicable to the measuring of privacy in a generic way, as well as improvements and requirements for using this method on a general terms. Hopefully, the thesis will be a contribution to the research on IoT and privacy, and, how this may be presented in a better possible way to the end customer.

Acknowledgements

This thesis symbols the end of my Master's Degree in Informatics: Programming and Networks with the Department of Informatics at the University of Oslo. This thesis have been a work going on for two years and with the time gone by, several people have helped along the way and I would very much like to acknowledge their help.

Firstly, I would like to thank my supervisor Josef Noll for all the help along the way. Without your knowledge and perspectives of such a thesis as well as the field of work, this would, without a doubt, have been a much harder task. I would like to thank you for being available, patient and supportive during the period of this thesis. I would also like to acknowledge my co-supervisor Elahe Fazeldehkordi for your help as well. Your opinions for this thesis have helped me going in the right directions.

Furthermore, I would like to thank my family for giving motivational speaks, when needed, in order to finish the writing. You have truly helped me carry on writing when I really did not feel like doing so.

I would very much like to thank my fellow students for five unforgettable five years at the University of Oslo. It would not have been the same without you! A special thanks goes to my inner circle. Thank you for all the good times as well as pushing me forward in order to accomplish this work.

I hope you as a reader find this thesis interesting and that it may give a better insight in how to assess measurable privacy for IoT consumer products.

Thank you.

Contents

List of Figures

List of Tables

Part I

Introduction

Chapter 1

Introduction

1.1 Motivation

This thesis was motivated as the current understanding is that privacy and security concern are not taken into consideration when products are released from the IoT community to the consumer market. Do people actually consider privacy when purchasing a new smartwatch? Or do they just look at its functionality and what it is capable of doing?

As the world moves forward and becomes more digital, it is important to look at how we safeguard our privacy on the Internet. Consumers frequently ask for better functionality from the tech markets, which again push companies towards coming up with new and better solutions. We can in some way say that the market is driven forward because of the consumers. If we weren't asking for these products, why would anyone bother making them?

Because of the exponential growth of the IoT market, it is our understanding that the consumer in general values functionality over privacy. It is therefore of certain interest to look deeper into how each user's privacy is maintained as these products become more convenient to people and make their everyday lives easier. One way might be to simply set rules and classifications to each and every IoT product being released in the market. Such a classification would force each vendor to fulfill the requirements set (for example, a specific way of treating cardiac related data as these are extremely sensitive data) in order to keep their products on the market. If such requirements are forced on the market, there would probably be a revolution, as there are currently no specific criteria for how data should be treated as long as the user consents with the vendor's policy (plus being the General Data Protection (GDPR) complaint [17]). Another for such an approach is that this demand would probably set limitations to the expansion of the IoT community. This may be because IoT products often aim to solve one specific problem. As this would slow down development of such products, one should rather look at other possibilities in order to solve the issue at hand.

A second way towards maintaining the consumers' privacy is to put the consumer himself in the position of choosing how his data are to be treated.

As of today, any average person does not have the competence necessarily for making such a decision. In order to do so, he will need to be presented with some kind of information explaining how sensitive data will be used by the vendor. When a customer buys, for example, a smartwatch, it is clearly explained what kind of functionality is being offered. The consumer can quite easily tell the difference between the functionality of two different smartwatches. One example may be whether the watch is water proof or not. In other words; the consumer has a much more natural relationship with functionality.

The question should be; how may we make the consumer both more aware of his privacy, and, at the same time able to make a wise decision? One such proposed solution would be the concept of *"Privacy Labeling"*. Such a label may present basic information to the user, explaining how the privacy of the user will be treated *within the platform of the product*. Such a label should focus on being as presentable and understandable as possible, because one would expect that a non technical person should be able to make a decision based on the information provided by such a label.

When introducing said label, a lot of challenges appear. For example:

- *How shall the label be calculated?*
- *How can one generally measure privacy?*

These are questions difficult to answer and ought to be considered high level issues to the entire thesis. They will further be split into more specific questions, which together aim at answering these high level questions.

NOTE: The word 'data' is frequently used throughout the thesis and a we need to establish whether the word is singular or plural presented itself. An essay in The Guardian dating back to 2010, however, clearly supported our choice of applying the plural 'data' as this thesis is tentatively written in British English and not any of the other varieties of the language [49].

1.2 Problem Statement

The need for ensuring privacy has become increasingly larger with the years passing. This may be seen in context with the rise of small IoT products that offer closer monitoring of a person. By doing so, we give our consent to the vendor to treat our data in such a manner that they can offer their products and, hopefully, make our everyday lives even better and more efficient. A common saying is that a *"common"* person should not be afraid to give away his data, given that it is maintained in a safe manner. A politican, however, is an high prone position, and, should consider this issue specifically. An example would be the case of Angela Merkel and the claims of the NSA wiretapping of her phone from 2010 until 2013 [5].

Looking at cases like the one between Cambridge Analytica and Facebook in the American election back in 2016 [32] it is extremely interesting, because *"common"* or *"regular"* people were affected. This case was a professional and targeted attack aiming to influence people's understanding of what they should vote on Election. Each victim was not necessarily capable of understanding what kind of attack they had been exposed to, because the attack itself aimed at presenting targeted ads and thus influence the political thoughts of a person.

Given these attacks, awareness of personal privacy when browsing the Internet has seen regulations such as the GDPR [17]. These regulations are starting to have an effect on the market and one can expect more regulations to come with time. One of the solutions that may apply to this critical area is Privacy Labeling. In implementing Privacy Labeling, we need to address the core elements in order to assess the privacy of a product. There may be a number of ways of doing so, but some key points should be evaluated either way. This thesis will, among other things, address:

- **Transparency**: How transparent is this product/platform?

In order to present a transparent product or platform, a user should be able to "see through" the whole system regardless of the purpose of the system, meaning that the user should be able to map the full data flow within the system. The vendor should not need to hide anything from to the consumer.

- **Configurability**: How easy and accurate can a user configure his own privacy?

Given an IoT product that regularly talks with a large and interactive platform, the user may be exposing his personal data to unknown entities. This may be desirable to some, but still not the case for others. Given that the overall system offers good and clear configurability, the user is in a good position to control how his data will be treated.

Furthermore, there are *four* main elements that must be taken into consideration when measuring privacy, as well. These are:

- Controlled collection.
- Controlled processing.
- Controlled dissemination.
- Invasion prevention.

These are some of the elements that need to be transfered from a textual and general manner into an actual numeric value which represent the impact of each element and, that at the end may be used to evaluating a Privacy Label. As for now, we will not elaborate deeper into these elements. A broader introduction may, however, be found in section 3.6.2.

1.3 The method of the thesis

Throughout the thesis we will follow the *engineering design method*, which is defined in 8 steps. The explanations below are based on the references from *"Science Buddies"* [42].

- *Define the problem:* The problem is defined by asking several specific questions. We need to address *what* the problem is, *who* has the problem and specify *why* it is important to solve exactly *this* problem.
- *Do the background research:* There is no need to re-invent the wheel. Before stepping into the research, we should first do a background research to see if there are any similar solutions that might be helpful. This may also help us avoiding the mistakes of the past.
- *Specify the requirements:* This stage presents the different characteristics and requirements needed from the solution to succeed, and may be carried out by analyzing or mapping specific samples (products) and gather key information.
- *Brainstorm, evaluate and choose solution:* One should always look at different solutions towards solving a problem. There is a considerable possibility that earlier projects may have come up with solutions that could be applicable to this task. When all different solutions have been addressed, what is best for the task must be chosen.
- *Develop and prototype a solution:* Now, the development phase may start. This may be done over a great matter of time, even after it is delivered and presented. A prototype should also be created for the solution which is a working version of the solution.
- *Test the solution:* When testing the solution, we often address new problems, which again may result in a redesign (of the solution). Such tests are done iteratively.
- *Communicate the results:* The outcome of the solution should be presented in an understandable way and explain exactly which results the solution accomplished.

Those are the main steps for completing the research and, the thesis is therefore based on these criteria.

In section 1.1, we introduced two high-level issues for determining a Privacy Label. These questions are difficult to answer just by themselves and should therefore be expressed in several more specific questions. The problem statement was defined in the previous section, and we will focus on the following four research questions to further detail the analysis. The questions are stated as follow:

- **Q1. What challenges relate to privacy using IoT devices?**
- **Q2. What methods can be used to assess privacy?**
- **Q3. What are the challenges when applying measurable privacy?**
- **Q4. Which are the recommendations as result from the work in this thesis?**

In order to determine a Privacy Label, we first need a method with which to determine it. It turns out that calculating and evaluating privacy is quite a challenge to do in a specific, yet efficient way. This is because privacy is quite an abstract term and may vary from product to product. Even if one is able to narrow down the term "Privacy" to the different groups in question, how shall this be translatable to the actual numbers and values?

How can we be able to look at a single product and its functionality while still taking all its dependencies into consideration? Several projects related to measuring privacy have been done in the past years, but mostly with focus on the user instead of focusing on the product.

1.3.1 Possible measurement method for the thesis

There have not been completed much research with regard to measuring privacy. Still, there have been conducted one interesting research trying to measure privacy.

An interesting project within privacy measurement was conducted by of Srivastava et al. [47]. The project was titled *"Measuring Privacy Leaks in Online Social Networks"* and is a proposed method for measuring privacy in Online Social Networks (OSN) like Facebook, Twitter, etc... This measurement method is interesting to look into since it has been shown to be quite adaptable into any kind of system, and it delivers a measurement that can easily be translated to a Privacy Label. The main goal for the method is to establish a *"Privacy Quotient"*. The Privacy Quotient represent the overall result produced after the method has been applied. The focus for the method is quite user focused and tries to calculate how the user's privacy is taken care of. This is done by looking at different sensitive parameters (data) that people tend to share in OSN (e.g. *contact number, job details, political view*). Further on, Srivastava et al. have weight these different parameters with respect to the sensitivity. For example, Srivastava et al. have listed up a table presenting the different parameters with its sensitivity as follow:

SNo	Profile item	Sensitivity
1	Contact number	.6
2	E-mail	.1833
3	Address	.85
4	Birthdate	.1166
5	Hometown	.15
6	Current town	.1166
7	Job details	.2
8	Relationship status	.4166
9	Interests	.3
10	Religious views	.5666
11	Political views	.6833

Table 1.1: Sensitivity values for calculating the Privacy Quotient.

This information will be used to giving each person a Privacy Quotient which may be between 0 and 7, and where 0 is extreme privacy awareness and 7 is no privacy awareness whatsoever. The table below shows how the Privacy Quotient is presented after a completed survey.

SNo	Range of Privacy Quotient	No of users
1	0.0 - 0.5	0
2	0.5 - 1.0	1
3	1.0 - 1.5	1
4	1.5 - 2.0	5
5	2.0 - 2.5	3
6	2.5 - 3.0	0
7	3.0 - 3.5	6
8	3.5 - 4.0	11
9	4.0 - 4.5	9
10	4.5 - 5.0	8
11	5.0 - 5.5	0
12	5.5 - 6.0	6
13	6.0 - 6.5	8
14	6.5 - 7.0	2

Table 1.2: Example of table showing users Privacy Quotient after a completed survey [47].

The method can be applied in order to determine a Privacy Label, but does not evaluate the actual product. It rather focuses on the user and just how he interacts with it. Therefore, we won't go any further on with this method.

It turns out that there are no other methods standing out that seem applicable at this moment. Below, the chosen method for this thesis will be presented.

1.3.2 Choice of measurement method

One of the very few scientific works looking into privacy measurement and assessment is the work by Garitano et al. [16]. As for this thesis, we will be focusing on the method provided by the project, namely the *"Multi-Metric approach"*. The reason for choosing this method is the fact that it is able to offer both a high-level assessment as well as an evaluation down to the core of each component. Though the Multi-Metric method provides a similar result as the *Privacy Quotient*, the Multi-Metric seems more precise with its possibility for careful assessment in all the different layers of the product.

The way this is done is to first map out the *"Overall System"* which may be a platform that the device uploads its data to. Such a platform may have may dependencies, and these may taken into consideration when applying the method. Furthermore, one needs to map out the different *"Subsystems"*. A subsystem includes the different parts of the overall system. One subsystem may be the actual device that is to be evaluated while another may be the platform. Furthermore, a subsystem contains different *"Components"*. A component may be different core functionalities of the subsystem (e.g. Wi-Fi, Bluetooth, etc...). Each component (has the possibility of being) can be configured in different ways (e.g. on and off). These configurations are presented in a metric where each configuration gets a so called *"Criticality"*, which represents how critical the specific configuration is with respect to the subsystem. Next step is to create different *"Scenarios"* which represent how a user can use the device with quite clear and specific explanations regarding the configurations of each component. The different scenarios may vary from a privacy aware person all the way to no privacy awareness (and everything in between). Each of these scenarios have a goal of what result we expect it to have after applying the full method.

As the final step, one should create different *"Configurations"* which represent how each component is configured (e.g. Wi-Fi is set to On). At the end these configurations are evaluated in what's called the Root Mean Square Weighted Data (RMSWD) (presented in Equation 4.1). This final result is then set up against the expected result for each configuration and gives us a good presentation of what privacy the device and overall system actually is able to deliver. The result can then be used for determining a Privacy Label.

There are still a few concepts that need to be addressed, but I will not go into details in this section. This is, however, more precisely presented in section 4.1.1.

1.4 Related work

Within the field of creating a Privacy Label, some projects have been going on for several years. One of the first projects mentioning "Privacy" and discussing issues related to this is a study carried out by Frederick Davis under the name *"What do we mean by "Right to Privacy"?"* back in 1959 [11]. He addresses concerns regarding people's privacy in a bit different manner than one would in 2019, but this still highly relevant. one of the problems Frederick is addressing is: *"An advertising agency uses a photograph of a school teacher, without her consent, to promote the sale of cough-drops, thereby subjecting her to bother- some questions, comments, and jokes, both in the classroom and the community."* If such a situation would appear, what kind of rights does the victim actually have? When looking at 2019, one can still find it representative. Speaking of IoT, what kind of rights does a person have if he chooses to share sensitive training data within a community and his data go astray?

Beyond that, we have seen quite a few projects related to the topic of Privacy Labeling. One of them is a project titled *"Designing a Privacy Label: Assisting Consumer Understanding of Online Privacy Practices"* and conducted by Patrick Gage Kelley [25]. His project aimed at presenting a label for presenting how the privacy is treated for a specific product. Kelley adds up parts of the motivation written for this thesis. Citing the abstract of the paper, we get a clear view of what the project aims for, namely: *"This project describes the continuing development of a Privacy Label to present to consumers the ways organizations collect, use, and share personal information."* Kelly presented an easily understandable label which was meant to put the consumer in a better position when deciding what product to buy. He addressed problems related to the current privacy policies and the difficulty of understanding these policies.

The paper was presented in 2009. In the years gone since that time (now 2019), there is even a larger need for such a label. Ten years have already passed since his paper was presented, but there is still no such label on the market. Kelley et al. have also presented another paper where they performed a development process in order to create a presentable Privacy Label for consumers [26]. Back in 2009, there were an estimated 0.9 billion IoT devices worldwide, while approximately 20 billion are are predicted in 2020 [23]. Such a rise in the number of new devices substantiates the importance of maintaining privacy in these products.

As of today, a collaborative project titled *"SCOTT" (Secure COnnected Trustable Things)*, is being performed by 57 parties from 12 different countries [43]. The project works on a wide specter with the overall goal of making more secure solutions within sensor driven solutions. The work of this thesis is part of this project and may be found under the name of *Building Block, "BB26.G"* [7]. Measurable privacy is a key factor within the project in order to be able to present such a Privacy Label.

1.5 Outline

The rest of the chapters are organized as follows:

- **Chapter 2:** Presents background information regarding the *Internet of Things* (IoT) and what domains it is influencing. The chapter also addresses what privacy issues may follows as a result of introducing IoT to these different areas. Furthermore, the chapter introduces the concepts *Security by Design* and *Privacy by Design*, discusses the relationship between these. As a wrap up, the chapter introduces *Privacy Labeling* and addresses what this is.

- **Chapter 3:** This chapter gives an introduction to how privacy is maintained in health monitoring as well as introducing the smartwatch Polar M600 and two possible platforms that the smartwatch may use, namely *Android Wear/WearOS* and *Polar Flow*. The chapter also discusses how privacy may be measured as well as how the different levels for a Privacy Label are proposed to be.

- **Chapter 4:** Gives a description of the *Multi-Metric* method and how it may be used in order to measure privacy. It is also discussed how this measurement method may be used when assigning a Privacy Label.

- **Chapter 5:** In this chapter, we apply the Multi-Metric method on our use-case in order to measure how the privacy is maintained for a user.

- **Chapter 6:** In this chapter, all the results from chapter 5 is evaluated as well as the measurement method (Multi-Metric). Critical questions are being discussed, whether this method is applicable when determining a Privacy Label.

- **Chapter 7:** Presents the conclusion, based on the results and evaluations provided by the earlier chapters. It is also given a recommendation of how the measurement method Multi-Metric may be improved so that it fully covers all aspects needed for assigning a Privacy Label as well as future work that should be conducted in order to validate or disqualify the measurement method.

1.6 Summary

This chapter has provided a broad introduction into what this thesis will focus on. The motivation for looking deeper into the field of *"Privacy Labeling"* has been presented and justified by the fact that privacy awareness is rising amongst actual people, while knowledge is still lacking. Introducing a label may be of great value to the consumer when making a choice of what product to buy, or not (going from functionality oriented towards more privacy oriented).

We have also (been) provided a short statement regarding issues related to privacy for customers and why it may be necessary to introduce some kind of label presenting how the product treats the customer's data. It may be possible to achieve the same goal in different ways, but my understanding is that by leaving the choice of privacy awareness to the consumer alone will not have that large an effect on the development processes in the market, but, however, still offer the focus needed within the field.

While this thesis is not the first to talk about the concept of introducing a Privacy Label, it is still rather important to address the uniqueness of this work, which focuses on validating the Multi-Metric method when assigning a Privacy Label. The reason for choosing exactly this method is the fact that it gives both a good birdseye look at the overall system whilst still taking core functionalities of a subsystem into consideration. By merging these two concepts into a single method, will be able to map the positioning of the product on the privacy scale. Whether the method is as applicable as this, or not, is the main goal that this thesis seeks to disclose.

The next chapter (*chapter 2*) will give an introduction into IoT and what exactly it is and what areas it is starting to become dominant. There will also be addressed background research regarding the concepts of both *security* and *privacy* as well as the relationship between them. As a wrap-up for chapter 2, there concept of *Privacy Labeling* will be further introduced and discussed.

Chapter 2

Background

2.1 The impact of Internet of Things (IoT) in specific domains

The world is becoming more digitalized. This has led to the ingress of IoT devices for private, as well as for professional use/applications. These devices aim to make their users' day-to-day lives easier. Because of their lightness and integrated sensors, the devices often aim to analyze the user's daily life. According to a study of user interactions with IoT devices, wearable smart devices has found its niche by offering accurate health information [27]. This is often done by connecting the device directly to the user's body, thus being able to monitor the user. By referring to a study done by Masaaki Kurosu: *"In other words, it is to stay connected more closely to users' body unlike smartphone."* [27], we get a clear indication of the overall goals for these IoT products. A typical device in this area is a pulse watch, e.g. a *smartwatch*. A pulse watch is meant to help people improve on their lifestyle, give a more monitored control of their everyday-life behaviour and the user improving on his exercise goals. Typical for a smartwatch on the market today is that it at least has a GPS, a pulse tracker and an accelerometer. Also, most of the watches are supported by a mobile application that monitors all the data and then presents an overview of what each person's everyday-life looks like. Such a smartwatch is suitably covered by the term *IoT*.

The term IoT is quite broad and covers a wide number of different devices. One common factor for all of these devices is that they often interconnected with a larger and more complex system. For the smartwatch, this could typically be a cloud or server that treat the data distributed. This has led to the use of such devices in, among others, the following domains:

- **Agriculture**
  - According to the American news and finance website *Business Insider*, the growth in food production is estimated to be rising with 70% from 2006 to 2050 in order to feed the population of the Earth [8]. In order to fulfill these needs, the entry of

IoT will have a large impact on the market. According to Business Insider, such IoT devices in agriculture may be sensors placed in the fields in order to obtain detailed overviews of the current temperature, acidity etc... This type of information may be valuable for each farmer who can then maximize his food production. A typical example (of this) may be when he wants to go on vacation. As for now, a farmer may have a hard time trying to fit in a vacation because he will need to water the fields on a regular basis. By introducing IoT the farmer may be able to remotely water the fields. Looking at it in a more proactive way, the farmer may be able to track the condition on the field and, based on that information, choose whether to water or not.

- **Health care**
  - Within health care, there are huge possibilities for the implementation of IoT devices. By introducing IoT into this field, many different security and privacy issues will have to be taken into consideration. This may be because of the sensitivity of the processed data. Some other possibilities within this field for IoT may be both in hospitals, nursing homes and home devices to be used by long term patients. Laplante et al. [28] proposed different types of areas of use in the health care, for example people suffering from Alzheimer or bulimia (eating disorder). One solution may be closely monitoring the patients when at home. If the pulse drastically decreases or the patient suddenly moves far away from his home, IoT technology can be able to alert people in time.
- **Retail**
  - The retail industry also sees a large growth of IoT. This may be sensors being able to track any person's activity in e.g. a grocery store. The sensors may be NFC sensors or, more specifically, iBeacons [30]. The use of such sensors open a whole new perspective for profiling any user and as his habits, and then present targeted marketing based on the data. According to a study by *Pawel Nowodzinski*, it is estimated that IoT will have a growth potential of *"up to 3.7 trillion dollars economic surplus"* in the retail industry alone [30].
- **Transportation**
  - The transportation industry is another sector where IoT has been on the rise for several years. Such technology opens up for the monitoring of vehicles and other transportation services from a separate geographical location. According to the *IoT Institute*, the use of IoT edge computing is on the rise also in helicopter transportation [20]. Such technology will be used to predict for example possible maintenance of a helicopter, based on real time

data, and they express them as follows: *"It can transmit the alerts via satellite communication systems, so maintenance crews can stay connected and track the health of a rotorcraft anywhere, at any time."* This is just one of the sectors within the transportation industry where the use of IoT is expanding.

- **Energy**
  - The energy industry is currently facing a total makeover in how end users deliver their data. The rise of smartmeters (AMS) is an ongoing project that will impact significantly on how energy companies operate. The AMS delivers a two-way communication and offers a variety of different possibilities. One is that the end user no longer will be responsible for reporting the energy consumption to the energy supplier. It occurs automatically through the smartmeter. Another big aspect arising as a security concern is a feature that allows for the remote controlling of the smartmeter [12]. This is advantageous for the power companies, but also disadvantageous if the feature were to come in the hands of badly intended people.

- **Manufacturing**
  - IoT is already well established within manufacturing. According to a report delivered by *ProQuest*, annual investment in IoT will rise from from US$ 6.17 billions (2016) to US$ 20.59 billions (2021) [9]. The growth shows that IoT is becoming important to the profit of production as this technology is able to streamline manual jobs that nowadays needs to done manually. IoT devices used in this field may be monitoring sensors that aim to analyze the efficiency of daily production. By collecting such data, companies will be able to address the specific changes that needs to be done in order to increase the efficiency of the production. This may be mapping out a certain place in production that may be streamlined.

- **Convenience**
  - As a unifying element, the convenience of IoT is starting to become a larger part of peoples everyday life. This may be wirelessly opening the garage door directly from the dashboard of the car or smartphone, or tuning the intensity of the lights in the living room via a smartphone. This is what IoT aims at doing, namely cutting edges and friction in peoples everyday life. As for retail, we have seen that personalized offers are an increasingly trend. There have been a discussion going on regarding IoT and whether this is a good or bad thing [21]. As of now, people are getting more dependent of these devices which not necessarily is a benefit.

The use of this technology raises several serious privacy and security concerns. How are data exchanged between the smart phone and the watch? How are data stored? How are data distributed between the various cloud services? There exist a great variety of mitigations that might lead to a more secure handling of this issue, but all of them won't be addressed. This thesis aims at end-user empowerment and will therefore focus on how the user himself can distinguish between sufficient and insufficient privacy practices. In the next section, there will be given a broad explanation of the suggested *"Privacy Labels"*. This will also be one of the main topics investigate during the rest of this thesis.

2.2 Security affecting Privacy

Security impacts privacy. This statement is inevitable as we would need security in order to maintain privacy. It would not make (any) sense to let each user choose what information should be publicly available or not if there is no security on the top. Being presented with such a system, a maliciously intended individual might be able to conduct *user profiling* (monitoring a user over a longer period of time and mapping of his habits). There is a great possibility of such attacks with IoT as these devices continuously deliver sensitive and precise data that can have a large impact for one individual. One does not want such information in the hand of unauthorized people. We therefore need security in order to deliver privacy.

There exists a variety of different mitigations against the vulnerabilities in the IoT industry. This thesis will not focus on all, but we will be taking a broader look at some.

2.2.1 Self-awareness

In general, an actual person does not have privacy concerns when buying a new device. Very often, the focus on the product lies in its functionality and not the privacy. Assuming that the level of privacy in the device is quite low, the user may be more prone to disclosing sensitive data than desired. The simplest privacy mitigation may thus be *self-awareness*. This can be as low-level as changing the default password of the IoT device or setting restrictions for what kind of network activity the device may perform. Another aspect is to gain control of all the devices that one actually owns. Currently, each person on the Earth in average owns 3 IoT devices [31]. Looking forward to what is expected for 2025, each person in average will own *9* different IoT devices. Both 3 and 9 devices may not sound like many, but assuming that most of these IoT devices are located in wealthy countries, the average in some regions rises quite drastically. There are approximately 23 billion IoT devices in 2018, and this number is estimated to rise to approximately 75 billion in 2025. This gives a perspective of how the industry is growing. Given that any person controls of each and every device he owns, the privacy vulnerabilities, however, drops drastically.

2.2.2 Security by Design (SbD)

The concept of *Security by Design* consists of ten different rules set by the Open Web Application Security Project *(OWASP)* for designing a secure system [44]. These rules apply both to software development and physical IoT architecture. The principles are as follows (as stated in the OWASP official description [44]):

- *Minimize attack surface area:* Every feature that is added to an application adds a certain amount of risk to the overall application. The aim for secure development is to reduce the overall risk by reducing the attack surface area.

- *Establish secure defaults:* There are many ways to deliver an "out of the box" experience for users. However, by default, the experience should be secure, and it should be up to the user to reduce their security – if they are allowed.

- *Principle of Least privilege:* The principle of least privilege recommends that accounts have the least amount of privilege required to perform their business processes. This encompasses user rights, resource permissions such as CPU limits, memory, network, and file system permissions.

- *Principle of Defense in depth:* The principle of defense in depth suggests that where one control would be reasonable, more controls that approach risks in different fashions are better. Controls, when used in depth, can make severe vulnerabilities extraordinarily difficult to exploit and thus unlikely to occur.

- *Fail securely:* Applications regularly fail to process transactions for many reasons. How they fail can determine if an application is secure or not.

- *Don't trust services:* Many organizations utilize the processing capabilities of third party partners, who more than likely have differing security policies and posture than you. It is unlikely that you can influence or control any external third party, whether they are home users or major suppliers or partners.

- *Separation of duties:* A key fraud control is separation of duties. For example, someone who requests a computer cannot also sign for it, nor should they directly receive the computer. This prevents the user from requesting many computers, and claiming they never arrived.

- *Avoid security by obscurity:* Security through obscurity is a weak security control, and nearly always fails when it is the only control. This is not to say that keeping secrets is a bad idea, it simply means that the security of key systems should not be reliant upon keeping details hidden.

- *Keep security simple:* Attack surface area and simplicity go hand in hand. Certain software engineering fads prefer overly complex approaches to what would otherwise be relatively straightforward and simple code.

- *Fix security issues correctly:* Once a security issue has been identified, it is important to develop a test for it, and to understand the root cause of the issue. When design patterns are used, it is likely that the security issue is widespread amongst all code bases, so developing the right fix without introducing regressions is essential.

All ten rules constitute sound general principles for a secure development. By taking privacy and security into consideration already in the design process, the company may be able to save time and money. This may also result in creating a more secure system. For IoT development, the principle *Defense in depth* may be quite important. Given a large industrial factory with a huge number of critical sensors connected to the Internet, one would also need them to operate fast. Very often there is a trade-off between speed and privacy. In order to minimize vulnerability for this type of system, one should implement security in the various layers. By establishing strict privacy regulations all the way from the beginning of the system, the need for high-end security may decrease the deeper one goes into the system. This may be done by implementing security in different layers. If we assume that 7 layers of security are implemented (in order to get to the core of the system), we would expect to disclose any breach before the seventh layer is broken. By doing so, one will be able to maintain the speed and availability that may be needed.

2.2.3 Security standards

In order to maintain control of the development for all existing products, there should be a general standard for creating and deploying products to the market. A report from NIST offers a clear statement regarding the standardization of the IoT market [19]. It appears that the current state of the art on standardization of the IoT market will not sufficiently maintain stable security for any given product. The report proposes different core values for a secure system, e.g. encryption, digital signatures and so on [22]. It is important to address these parameters in order to find a better relationship between security and functionality. To be able to standardize the whole IoT market, much work needs to be done. A technical privacy and security standard may be the most obvious way to go, but will take time to implement and might not be the correct solution because of inefficiency. Hence this topic is the closest to what this thesis will look deeper into; we will try to set a list of criteria for what a "secure" system should look like. Although this thesis focuses on privacy and, thus, *not* on security, it is important to address the fact that security has a large impact on privacy.

2.2.4 Privacy by Design (PbD)

PbD is a list of individual principles that should be taken into consideration when building a product. The ideas behind the principles were introduced by Alan F. Westin as early as in 1968 [41]. The different principles are presented as follows (as quoted from the paper *"Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems"* by Marc Langheinrich) [18]:

- *Openness and transparency:* There should be no secret record keeping. This includes both the publication of the existence of such collections, as well as their contents.
- *Individual participation:* The subject of a record should be able to see and correct the record.
- *Collection limitation:* Data collection should be proportional and not excessive compared to the purpose of the collection.
- *Data quality:* Data should be relevant to the purposes for which they are collected and should be kept up to date.
- *Use limitation:* Data should only be used for their specific purpose by authorized people
- *Reasonable security:* Adequate security safeguards should be put in place, according to the sensitivity of the data collected.
- *Accountability:* Record keepers must be accountable for compliance with the other principles.

Even though the essence of these principles have existed on the market since 1968, there are still issues related to the topic that need to be addressed. The need for better privacy is growing exponentially as IoT is increasing in people's everyday lives. While PbD focuses on how the developers design their products all the way from the beginning, this thesis will focus on how the end user can evaluate this by himself. It is nevertheless important to address the PbD as it lays the foundation for how a product should be structured.

The concept of *Privacy Labels* is then suggested as a way of presenting privacy in a more understandable manner to the end user [40]. This is further explained in the next section.

2.3 Introduction to Privacy Labels

In order to fully understand what Privacy Labeling is and why it might be helpful, we first need to define the concept *"privacy"*. According to the *Cambridge Dictionary*, privacy is defined as following: *"Someone's right to keep their personal matters and relationships secret"* [38]. This definition tells us that privacy is a concept of *"having personal data kept private"*. Or that confidential data be kept secret and visible only to authorized people.

The Privacy Label offers privacy in an understandable and non-technical way by labeling the product from e.g. A++ all the way down to F (where F is failed). The concept is based on many of the same principles as the European energy labels for appliances (as shown in figure 2.1). The labels provide a graphic presentation of the product's classification in a way that is understandable for each and everyone. The introduction of the label was a great success with regard to understandability and is one of the reasons for following the recipe with respect to privacy. The energy label is based on different criteria for appliances, and the goal is to create similarly measurable criteria for privacy when presenting a Privacy Label.

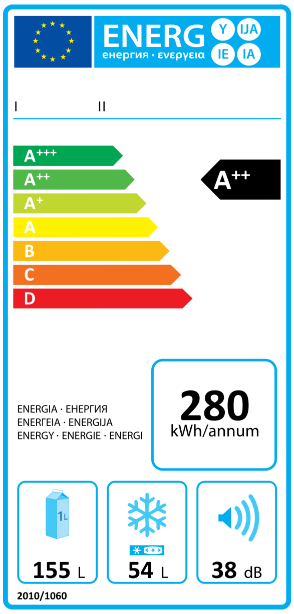


Figure 2.1: The European Energy Label.

As addressed earlier, similar work has been conducted regarding Privacy Labeling [26]. The fact that such work has been carried out earlier adds up to the need for such a label even more.

In other words the energy label is an approach that can be applied to the IoT market. In order to do so, four different aspects are needed to be taken into consideration in order to deliver a label, namely:

- *What data are collected?*
- *Where are the data shared?*
- *Data communication integrity and storage.*
- *Further distribution of data, ownership of data and further processing.*

Furthermore, a variety of aspects should be taken into account, for example the freshness of the data, a notion of data sensitivity, etc. This method could be applied to any product in the sectors described in section

2.1. By looking at the health care sector as an example, there is an absolute need for such labeling. Most of the devices being used are in conjunction with personal data that is to be kept secret or private. Given such a label, it would be easier for a company to choose which product is better suited. This would also apply to a typical individual when purchasing an IoT device for health monitoring.

The home nursing and care of Norway provides services to a range of elderly patients, often immobilized to a certain degree (e.g. Alzheimer). When suffering from such a disease, the person's memory will slowly fade [1]. As mentioned in section 2.1, this is an opportunity for the use of IoT, and one that may help keep track of the patient at all times. While this kind of technology offers a number of benefits, it also presents several privacy concerns. One should expect that all sensitive data are transferred over a secure and encrypted connection. One should also expect that no unauthorized people may become administrator of such a system, as it may inflict serious and fatal injuries to the patient. It should be possible for the end-user to maintain an overview on how the data are being handled.

By offering a Privacy Label, it will be easier for the end user to choose what service to use. The label might also push the manufacturer to improve on securing the data being collected. If a Privacy Label were to be introduced into the market, one would expect a health monitoring product to have a high labeling score (e.g. B). As of today, this information is hard to obtain when buying such a product.

2.4 Summary

In this chapter, we have taken a birdseye look at the term IoT and which areas it covers. The most common factor for an IoT device, independently of the area in which it is being used, is the purpose of the device and how the overall system is designed. Most of the time the purpose of an IoT device is the gathering of data, which it forwards to a endpoint for processing. The reason for forwarding the data rather than process them locally on the device is the lack of capability of the device. As discussed in chapter 2.1, we can see that IoT is being introduced into *agriculture*, *health care*, *retail*, *transportation*, *energy* and *manufacturing*. All of these industries are using IoT in order to become more independent in daily tasks. Such daily tasks may be as simple as monitoring the conditions inside a.

Furthermore, we have taken a broader look at the security mitigations, both from a user perspective, but also from a manufacturer's point of view. As pointed out, the easiest way of ensuring user security is self-awareness. Very often the issue is about becoming more skeptical when using a device. Just because a product has a common brand name, it does not necessarily follow that it's security has been taken care of. Even if the security is ensured, the user might be exposed to attacks if the product is improperly used. From a manufacturer's point of view we have looked at ten different concepts defined as by *Security by Design*. These are ten concepts that should be taken into consideration when designing a system.

This chapter is a contribution to Q1 (*What challenges relate to privacy using IoT devices?*) explaining the current state of the art within the IoT community. Several contributions for this question have been presented:

- It is fair to say that the use of IoT will increase in the coming years [23]. The need for standardization of privacy is also increasing. A possibility for forcing a privacy standardization to the vendors in the market was mentioned, but it falls short because of by the implementation overhead costs. Implementing such a standardization will take time as well as slow down innovation. A proposed way of doing this is by introducing Privacy Labeling.
- The concept of *Privacy Labels* was introduced. In order to set such a label, we need to look at the system as a whole. This may have to start with the data collection by a sensor and continue all the way to processing at the endpoint. Later in the thesis we will go deeper into what methods may be applicable in order to calculate and measure such a label. An explanation of what criteria each level within such a label may consist of will also be addressed.
- Another aspect is the fact that such IoT devices collect sensitive data very often and on a large scale (big data). As machine learning is growing, the risk of for user profiling may increase if privacy is not assured.
- As IoT grows larger and becomes more accessible, the more it becomes relevant in more domains. This introduces a threat to any individual's privacy as we become more dependent on these devices in any given domain.

The following chapter (*chapter 3*) will give an introduction to privacy related to health-monitoring within IoT. The chapter will also address a use-case that later in this thesis will be used when applying the privacy measurement method (Multi-Metric method) in order to determine its privacy.

Chapter 3

Privacy in Health Monitoring

The previous chapter addressed different domains where IoT is represented, as well as the need for a privacy standardization. The chapter concluded with a suggestion for the use of a *"Privacy Labeling"*. This chapter will present a use-case for testing the proposed measurement method *"The Multi-Metric approach"* in order to determine a Privacy Label.

3.1 High level functional aspects

As of today, most IoT devices are either wireless or with a cord connected to a platform that monitors its data, thus giving the product the possibility for being more complementary. This, however, also raises several privacy concerns. Many different IoT devices exist on the worldwide market. Vendors such as *Fitbit* or *Polar* deliver a variety of products that may be characterized as IoT. Some vendors want to create a central platform for all their products and then connect them to one central user profile, and so enabling a more complete range of products that talk with each other, and that also may utilize functionality from the other devices in order to deliver a more precise overall analysis. If a user is happy with one of the products from named vendor, the customer may continue buying other products from the same vendor, using the same platform. This is obviously presented as an advantage to the customer. Simultaneously, as vendors are able to offer more products on the same platform, the vendor may end up in quite a vulnerable position where it will have to treat all data in a safe manner. Given that a data breach on such a platform may lead to a *single point failure*, the outcome can be quite dramatic if the data are considered sensitive.

A possible data flow in a typical IoT environment can be as follows: Data are collected via a *pulse belt* that is attached to the user's chest during a training session. As soon as the session is finished, the pulse belt transmits collected data directly to a *smartphone* via e.g. Bluetooth. As soon as data have been received by the smartphone, the user might have the possibility to further synchronize the data to a *cloud*. Once data have been transmitted to the cloud, the user may access the training results from any device. Such a system requires that privacy is ensured in each step. For each new transmission of data, the risk of eavesdropping increases. Below, we will look at one specific product and carefully explain its different functionalities.

3.2 Use-case: Polar M600

We have chosen to look at privacy in health monitoring and therefore elected a representative product, namely the smartwatch *Polar M600* (hereafter called *the M600*). The smartwatch was introduced into the market in 2016 and is still highly relevant for the consumer market today. According to Statistica, the number of smartwatches sold have increased from 5 million units to 141 million on a worldwide scale (end of 2018) [46], thus proving that these products are starting to become a part of any person's day-to-day lives, more and more.

The M600 can use either the *Android Wear* (now *WearOS by Google*) or *Polar Flow* apps. The watch aims towards making its users more efficient, as well as healthier. This is done by constantly monitoring the user, presenting the data in an understandable way so that the user can make decisions based on what's presented. Simultaneously, as the market for *IoT* devices is expected to grow exponentially (in the foreseeable future), privacy is not necessarily taken into consideration. This may apply to the manufacturer's point of view, but also from the user's perspective.

Figure 3.1: Polar M600.

3.3 Functional architecture

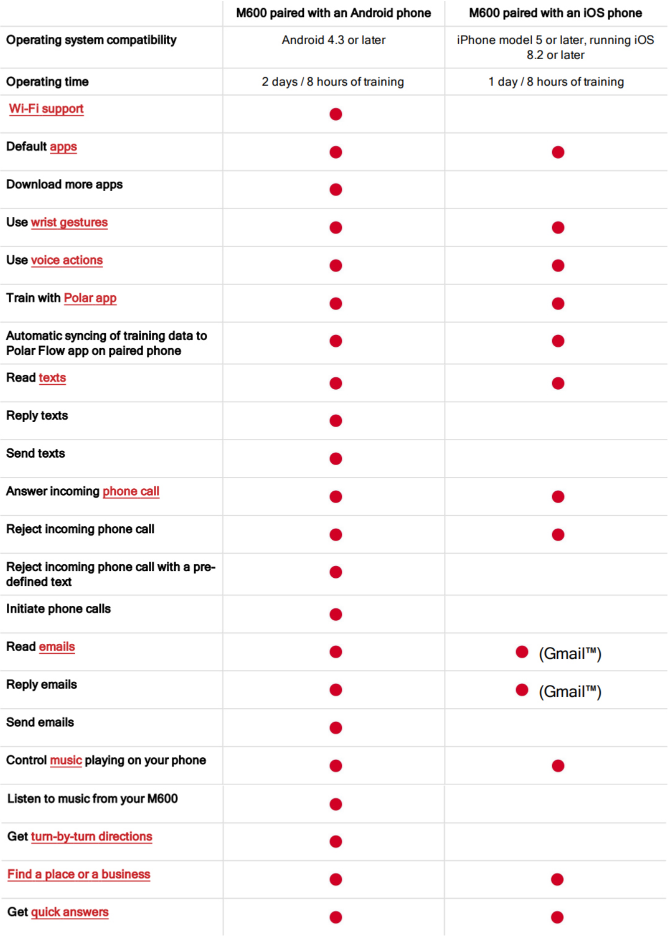
The M600 was, as mentioned, released in 2016. According to Polar's official site the watch has a variety of different specifications [48]. As we can see from Table 3.3 (page 25), the watch is quite representative for most smartwatches being marketed today. This watch supports both *Android Wear* and *Polar Flow*. Android Wear is a generic platform that supports a variety of different wearables, in this case, *smartwatches* [29]. Given that this is a platform supporting a wide range of devices, it seeks to offer more generalized functions. This may be advantageous, as well as disadvantageous, as the system does not specialize in any single product. On the other hand it can be of advantage as the user only needs to focus on familiarization with one platform, regardless of what product (e.g. smartwatch) he has bought.

Operating system: Android Wear
Processor: MediaTek MT2601, Dual-Core 1.2GHz processor based on ARM Cortex-A7
GPS accuracy: Distance ±2%, speed ±2 km/h
Sensors: Accelerometer, Ambient Light Sensor, Gyroscope, Vibration motor, Microphone
Storage: 4GB internal storage + 512MB RAM
Data transfer technology: Bluetooth® Smart wireless technology, Wi-Fi

Table 3.1: Technical specifications - Polar M600.

3.3.1 Polar M600: Technical features

The Polar M600 processes sensitive data, e.g. health information (pulse activity, weight) and GPS location.



	M600 paired with an Android phone	M600 paired with an iOS phone
Operating system compatibility	Android 4.3 or later	iPhone model 5 or later, running iOS 8.2 or later
Operating time	2 days / 8 hours of training	1 day / 8 hours of training
Wi-Fi support	●	
Default apps	●	●
Download more apps	●	
Use wrist gestures	●	●
Use voice actions	●	●
Train with Polar app	●	●
Automatic syncing of training data to Polar Flow app on paired phone	●	●
Read texts	●	●
Reply texts	●	
Send texts	●	
Answer incoming phone call	●	●
Reject incoming phone call	●	●
Reject incoming phone call with a pre-defined text	●	
Initiate phone calls	●	
Read emails	●	● (Gmail™)
Reply emails	●	● (Gmail™)
Send emails	●	
Control music playing on your phone	●	●
Listen to music from your M600	●	
Get turn-by-turn directions	●	
Find a place or a business	●	●
Get quick answers	●	●

Figure 3.2: The Polar M600 Features.

According to the M600 user manual, both functions are mentioned, but also many more (figure 3.2, page 25) [15]. The manual describes how the watch supports a direct Wi-Fi connection, which allows for the watch talking directly with Android Wear or Polar Flow, regardless of the distance between smartphone and the watch, rather than via Bluetooth (which is also supported). Another interesting element supported by the watch, is the GPS feature. The watch can log *altitude, distance* and *speed*. All information is delivered real-time to the smartphone app while the user is working out. According to the user manual, data are automatically synchronized with the Polar Flow app after a training session. The watch gives an "inactivity alert" if the daily goal is not met. If the daily goal, however, is met, the user will get another notification. The data are subsequently synchronized between the smartphone and Polar's web services. Another feature not mentioned in Figure 3.2, is the support for the monitoring of sleep. The M600 supports monitoring the user's sleeping rhythm if the watch is being used at night. According to the user manual, it is not necessary to turn on "sleep mode" in order to continue monitoring during sleep. The watch will automatically detect that the user is in fact asleep and start monitoring the sleep rhythm. The data are synchronized both to the Polar Flow app and web service. This naturally raises some privacy concerns on how data are being managed and safeguarded.

3.4 Technology details Polar M600

Two monitoring systems are available to the M600. One is the *Android Wear/WearOS*, and the other, the *Polar Flow*. Android Wear is a generic platform which has a general support for all watches running the Android OS/WearOS. The clear advantage of Android Wear is that the user will only need to relate to one specific platform, regardless of the type of watch. It obviously also introduces some limitations, as presented below.

The other platform is Polar Flow. This is a custom made platform for all the Polar smartwatches. It comes with several features and is tailor made to fit Polar watches. Android Wear delivers an app for monitoring data, while Polar Flow delivers both an app and a web service. These services both deliver a user friendly overview of the data, as described in section 3.3.

3.4.1 Android Wear/Wear OS by Google

Android Wear *(now marketed under the name "Wear OS by Google")* was released in March 2014 by Google. The Android Wear supports a variety of different smartwatches, including the M600. The current version of the platform is "Wear OS By Google - Smartwatch v3" [3]. This is a platform aiming to support both the Android and iPhone smartphones, even though it is based on the Android OS. According to Android's official web page, Android Wear: *"Make every minute matter with Wear OS by Google. Smartwatches that keep you connected to your health, the people and info you care* *about, and your Google Assistant — all from your wrist [3]."*

As of today, almost 2,5 billion people own a smartphone [45]. This device is far more capable of processing data than a smartwatch (e.g. Polar M600), which is one of the reasons Android Wear was introduced. It is, however, also possible to make an application run perfectly well on a wearable device without any connection with the smartphone.

Android Wear aims for third party developers to create both applications and devices on their platform. This has led to a variety of companies making their way onto the market. According to Android Wear's official web page, companies like *Nixon, Hugo Boss Watches, Fossil, Polar, etc.,* have created watches running Android Wear OS [4]. As these worldwide companies make their way to the market, it will naturally follow that people will buy the devices. Such demand requires that the vendors take security and privacy into consideration when creating devices, as they process very sensitive data.

Figure 3.3: Wear OS by Google.

3.4.2 Android Wear: Security and privacy aspects

Android OS for smartwatches introduces both advantageous functions, as well as less so. As Android has been on the market for a long period of time, the core of the operating system is already well developed. Many security mechanisms have been implemented and can automatically be adapted into the smartwatch [13]. One advantage is that applications are sandboxed, meaning that no other applications can access its internal storage. Looking at the disadvantages, however, we can expect the smartwatch to inherit security the flaws that already exist in the Android OS. Such flaws might be hard to bypass as a large and complex operating system like Android has a high number of dependencies.

Other security concerns include how data are being treated. In order to address security concerns, we should distinguish between data stored locally and data being transmitted from the device (and most likely to a smartphone). If we consider that the data are being stored locally, we can remove attack surfaces. Since the applications running on the watch are sandboxed, it follows implicitly that this application and no other can access its internal storage. Other users and applications can access the storage only under specific circumstances [2]. According to Android's official web page, all internal storage will be removed when the application is uninstalled [2]. In other words, data considered to be sensitive (i.e. not to be accessible or visible to others), should be stored here. An application will also be able to save data in an *external storage*. This is a public environment which is world accessible to all applications. Data may for example be stored on an SD card. An application can use this functionality for e.g. storing images. A user may, however, still want to re-use the images after uninstalling the application. The security aspects of external storage will, of course, be that this is world-readable for all other applications on the device. When considering the fact that Android ensures privacy in the internal storage, one can to some extent say that it is the developer that needs to ensure the privacy.

Given that data are being transmitted to a smartphone, which again transmits data to a server, we are left with a much bigger attack surface. This opens up to a larger use area for the application, but it also requires more security in the handling of the data. We will discuss how some of the watches handle this later in the thesis.

3.4.3 Polar Flow

The other application that can be used, is Polar's own app, the *Polar Flow*. As seen in Figure 3.2, the app supports a variety of possibilities for the end user. According to the Polar Flow official website, their application is able to *"Give feedback about activity, sleep and exercise. Train with friends or register sessions on your own to reach your goals"* [33]. When reading on in the user manual, we are met with the following summary for the app: *"In the Polar Flow mobile app, you can see an instant visual interpretation of your training and activity data. You can also change some settings and plan your training in the app."* Further ahead in the manual, we are told that the training data automatically will appear in the Polar Flow application, which can share data with specific people within the *"Flow Feed"*. The app not only shows training data, but the user's daily activity in detail (including sleeping rhythm).

Figure 3.4: Polar Flow.

In order to use the Polar Flow app, the user has to create a Polar account with basic information *(e-mail, first name, surname)*. The account provides for adding additional specific data, such as *gender, birthdate, height, weight, maximum heart rate, minimum heart rate, as well as aerobic* and *anaerobic* *thresholds*. Based on these data, Polar Flow will calculate the user's Body Mass Index (BMI). The BMI is calculated as follows:

$$BMI = \frac{KG(weight)}{m^2(height)} \tag{3.1}$$

It is possible to change to some data in the app, but not all. The rest has to be done via Polar Flow's web service. This web service also provides a variety of other services. According to the user manual, the user is allowed to both plan and analyze his training details. He may also connect with other people in the Polar network, where users can share training data with each other, as well as creating a public training program for the group.

Regarding the Polar Feed, and as mentioned earlier, the users can also monitor how friends' workout sessions have been lately. It is also possible to share *best achievement* for one user. Another interesting feature in the Polar Flow app is the *"Explore"* function. This feature lets each user, among others, share favorite running routes. Routing information can be published publicly to all Polar users, with specific information regarding training sessions. Information is subsequently made visible in the Polar web service where one may study in detail the route, how long it took, the heart rate (highest, lowest and, average), and calories burnt during the session. As shown in Figure 3.5 on page 29, the user is also presented with a graphical overview of a variety of data from the workout session.

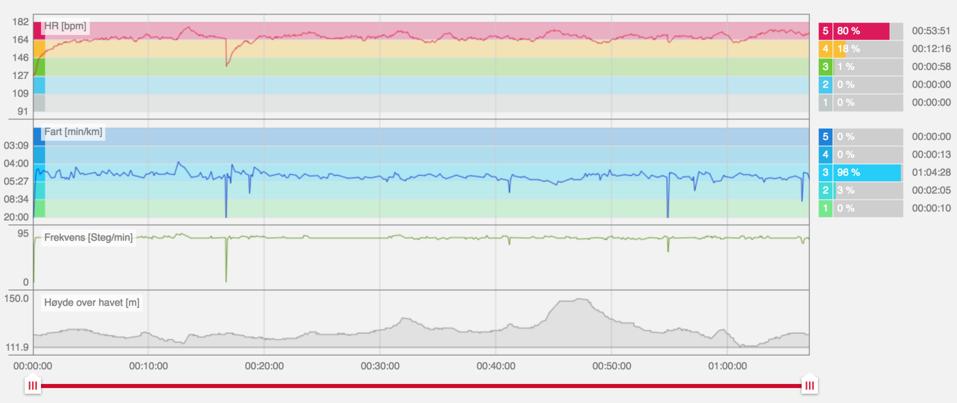


Figure 3.5: The Polar Flow Explore.

Not only does Explore present graphics explaining the training session, Polar also delivers a feature named *"Relive"*. This feature lets the user relive the session by video. The video contains information about the session, geographical location, duration, current distance ran, current heart rate and also current speed (at each specific part of the video). It also offers *Google Street View* in order to show surroundings. Highest heart rate during the session is also shown in the video. Furthermore, the web service provides a *"Diary"* feature, which is a calendar that logs all activities for any given day, with possibilities to review all past sessions.

3.4.4 Polar Flow: Security and privacy aspects

Almost all information gathered is considered sensitive data and should not under any circumstances be made available to unauthorized users. Leaving the Explore functionality open to any user raises a privacy concern regarding how the feature may be abused in everyday life. Referring to the Polar M600 official user manual, the Explore feature provides the following functionality: *"In Explore you can browse the map and see other users' shared training sessions with route information. You can also relive other people's routes and see where the highlights happened* [37]*."* These two sentences give no direct information about who will be able to see the data, and the data should thus be understood to be public. Assuming that the data are indeed public, the vendor may say that the responsibility for ensuring privacy belongs with the user.

Polar offers the *Relive* function, and any person registered in Polar Flow can study all sessions that have been set to public, and is then able to map the behavior of any given user very precisely by looking at the data provided (GPS, pulse, speed, etc...). It is possible to create a visualization of each person's everyday life by mapping the data. Assuming that the data were made available to a maliciously intended user, it would for example be possible for an illegitimate individual to see the training pattern of any specific person. Based on this pattern, it may be easier to conduct a burglary in the victim's home just by assuming that the person is not at home at any given time, based on these data.

3.5 Technological challenges: Polar M600

With the various types of information stored in and distributed with the M600, several technological challenges regarding privacy will arise. Most of the processed information is personal and should under no circumstances be made available to unauthorized people. Another aspect is the software bundled with the watch, the *Polar Flow*. This software offers, as before mentioned, a variety of functionalities. It is mainly intended to benefit the customer, if used correctly. Regardless of the benefits of the service, there is, however, also a social privacy issue present. This will be discussed in the following subsections.

3.5.1 Privacy and the Measurability of Privacy

The M600 supports a variety of ways to track the user's behavior. Figure 3.2 shows the possibility for collecting a variety of information from the user (e.g. voice and pulse). The data are either stored locally on the watch or distributed to the cloud, via a smartphone or directly via Wi-Fi.

Given that the user *"Bob"* publishes all his training data directly to the Polar Flow community each time he goes for a run, it may be possible to profile "Bob" just by looking at his historical data. Assuming that "Bob" goes running every Tuesday and Thursday at 17:30-19:00, and by looking at his historical data, one may see a pattern for the last year. This would not be a possible issue if the information was shared only with the friends that "Bob" trusts. The problems arise when "Bob" makes his data public for everyone to see. Polar Flow offers this function as a social medium to its users.

3.5.2 What do the privacy numbers mean?

8 different levels of Privacy Labels have been proposed [40]. These levels go from A++ to F, where F is fail. Below, we will have a look at the requirements proposed for each level. In order to make a specific privacy level, different parameters must be taken into consideration (e.g. configurability). This means that to a certain extent the system can be evaluated to both level B and D (given the configuration made by the end user). As of now, we are presented with a proposal of what criteria each level should have (as directly quoted from the *IoTSec:Consortium Nov.2017*)[40] [24]:

- *Level A++:* One should expect that no data are shared and the data that is being recorded, is stored in a safe way, locally on the device. If an unauthorized entity gets hold of the device, he/she should under no circumstances be able to collect/get access the data that is stored.

- *Level A+:* Data is stored securely. May allow for transmission, but in a way that makes it close to 100% safe.

- *Level A:* The data that is being stored shall only be used for a set of functions that is 100% relatable to the device's purpose. Data may be transmitted across different platforms in order to deliver a more complex solution for the customer. If any of the data comes to a halt, the producer will have to inform the user within 72 hours (GDPR). In other words, the supplier will be responsible if anything goes wrong.

- *Level B:* The supplier may be able to re-use the data, but only under given circumstances. The supplier needs to clearly inform the user where this information will be used and for what purpose. The data should under no circumstances be used for anything else than statistical use. The supplier should furthermore ensure the integrity of the customer, meaning that the data should be in a safe environment. The user should be able to customize what information that is to be stored and how it is being used.

- *Level C:* The user is being watched at all time and information like heart rate, GPS location, acceleration etc. is being logged. The user needs to give consent and he is able to withdraw this at any time. The user should furthermore be able to delete all private data and get a confirmation that the deletion was successful.

- *Level D:* The supplier has the right to sell the information that is being stored. The customer must, however have full insight in which information is being sold/distributed, to whom and for what purpose (transparency). The information should only be used for the purpose that the user has consented.

- *Level E:* The supplier has the right to sell/distribute the information that is stored. The customer has no insight in this (no transparency). The user must, however be alerted if any data comes to a halt and the solutions must be GDPR compliant.

- *Level F:* The user has no insight in how the data are being treated. There is no restriction for what unauthorized people can see/edit. The solution is not GDPR compliant.

These different levels constitute a draft provided by the different representatives within the field of privacy. In order to complete the list, there is still a need for adjustments and harmonization. Given the technical background of this work, the focus will rather be on validating a measurement method for determining on which Privacy Label level the product should be placed. Whether one shall assign level A++ to F is up for discussion, but this thesis will only be focusing on measurement for the products.

3.6 Evaluation of the data

In order to evaluate the data, we need to break them down to the core. What data are being stored? What is the purpose of collecting the data? How are the data being distributed? By combining all these aspects, we may be able to characterize the privacy of the system.

3.6.1 Measurability of Privacy

When we look at privacy, there are many parameters that need to be taken into consideration. What information is stored? How sensitive is it? How is the information distributed? The assessment method for measuring privacy (Multi-Metric) will be used for evaluating these data [16]. Later in the thesis, we will look closer into this approach, describing it and, applying it on the use-case. The approach evaluates each level of the system and will lay the foundations for converting the privacy parameters into actual measurable values. In order to measure these data, we have to consider four different aspects, namely "*Controlled collection*", "*Controlled processing*", "*Controlled dissemination*" and "*Invasion prevention*", as mentioned in section 1.2 [16]. This will be more clearly explained in subsection 3.6.2.

A central element of the use-case is the Polar Flow. This service stores a variety of data. Below, they are described with respect to the "*Controlled collection*":

- General information:

  - Basic information (**full name, town, country, e-mail, gender** and **birthdate**). Each of these data elements may not be considered sensitive just by themself, but by combining them, they are to be considered sensitive. In order to determine the privacy of the user, one should expect that the data are kept secret and unreachable to unauthorized entities. **Mandatory information.*
  - **Height & Weight**: This data alone by itself may not be considered sensitive, but can have an impact in association with all the other data being stored. **Mandatory information.*
  - **Training background**: This is not to be considered sensitive by itself, but may be sensitive in association with the other data being stored. One should therefore expect these to be kept in a safe environment, unavailable to unauthorized entities. **Mandatory information.*
  - There are different other data being stored, but they are not mandatory. This may be information like **max & min heart rate, BMI, sleeping time** and **profile picture**. Some of this information alone is to be considered sensitive (e.g. profile picture).

- Information gathered while training:
  - **Heart rate**: When using the M600, Polar Flow will receive the user's heart rate from each training session.
  - **GPS**: The M600 continuously stores the GPS information of the user. This information is to be considered sensitive in itself and should be kept and managed in a strict and secure way.
  - **Duration of training session**: The user is able to both start and stop the session.
  - **Length**: The M600 continuously monitors the GPS location of the watch during a training session. Based on this, Polar Flow presents both the distance and exactly where the session took place.
  - **Calories burnt**: This information is a combination of the different data values that have been stored. It is a combination of age, workout duration, heart rate and distance. This information, in association with the basic information, may be sensitive.

Those are all sensitive data, at least when seen in connection with each other. They should therefore be treated in a safe manner. Below are the four different elements that should be considered when systems such as Polar M600 and Polar Flow treat data like these.

3.6.2 The four main elements for measuring privacy

When measuring privacy, we need to map out what *data* are collected, what the *purpose* is for using them, if the system is *sharing* the data or not, if this is done in a safe manner, and, finally, map out the *security* provided by the system. The different areas are presented below:

- **Controlled collection (Data)**
  - The first element to consider is how the collection of data are controlled. As described above, Polar (Polar Flow) stores different data that may often be considered sensitive when seen together. Both the way that data are being processed and how the client is offered to modify the use of the data will have an impact on the user's privacy.
- **Controlled processing (Purpose)**
  - As stated by Polar in their privacy statement, their purpose for using the data are to offer *"a personalized experience with our services. For example, we use your age info to give you a more accurate calculation of burnt calories"* [34]. In order to ensure user privacy, the purpose for using the data needs to be specific and strict. It should under no circumstance be used for any other purpose, other than for what the user has given his consent to. As a total evaluation, this element should be set in context with the other three criteria.
- **Controlled dissemination (Sharing)**
  - Controlled dissemination may be a crucial criterium for the privacy of the user. This information can be used by a third party, to for example, make a more narrow profiling of the user. As it turns out in Polar's case, they tend to be strict on how data are being distributed. Referring to Polar's privacy statement; *"You are responsible for managing the information you share or transfer out of the system"*. We see that the user is made responsible for how his data are handled outside Polar's services.
- **Invasion prevention (Security)**
  - In order to ensure privacy, we will naturally have to rely on the security. If there is no security on the top, one can't ensure that the privacy of the user remains intact. This will, however, not be the focus of this thesis. We will assume that the security is ensured by default, though.

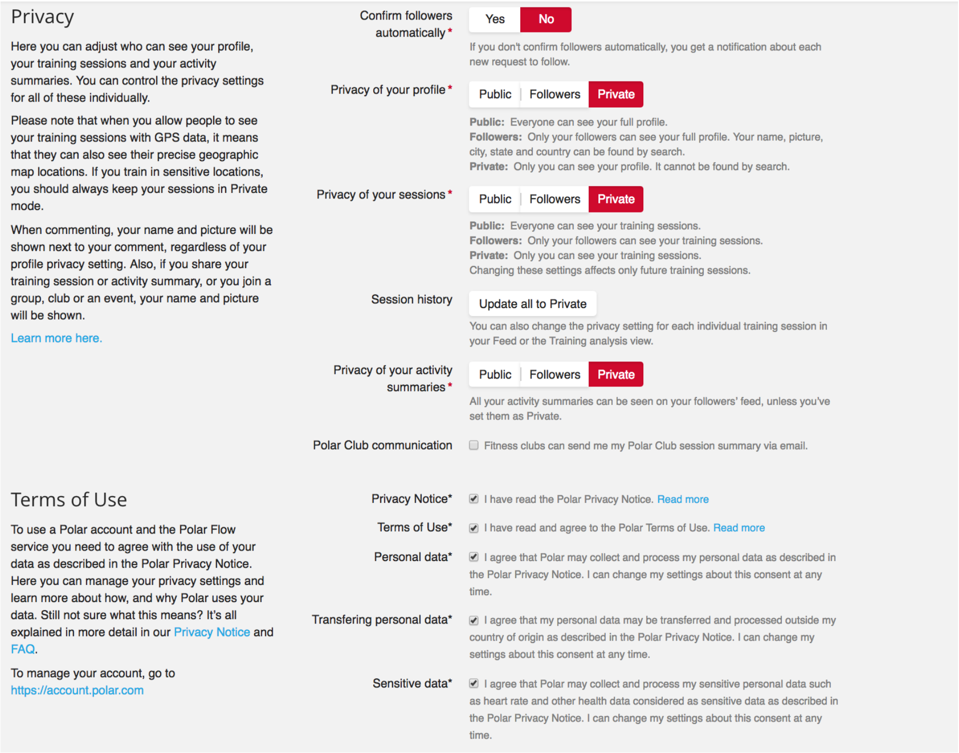
To give a complete overview on how the privacy of the user is safeguarded, all these four different criteria should be compared to each other. Below, we will look closer into the first criterium, namely *Controlled collection*.

3.6.3 Controlled collection

To evaluate the data, we first need to address them all. As discussed above, a lot of the data are not to be considered sensitive by themselves, but will be so in context with other data.

When looking at the training data being synchronized between the watch and *Polar Flow*, a quite clear *transparency* is offered. Figure 3.6 on page 36 shows that all privacy settings are default set to private. There are three different options, namely *Public, Followers* and *Private*. The Public function gives everyone access to view all the information on the user's profile. This *configurability* will result in a more positive evaluation of the system. While the user is offered a chance to configure his privacy settings, he is automatically made more aware of how the data are processed. The user is able to specify a privacy setting for a single training session. This gives the opportunity for sharing some sessions, while setting others to private. As a configuration, the user can update all its session history to private.

Based on the configurability options, it seems that the Polar Flow offers good privacy options for the users. *But is this actually the case?* As discussed in section 3.4, Polar Flow offers the *Explore* function. As we have already seen that privacy is ensured by design, no data are shared publicly to this function by default. Given the configurability that the user is offered, it is possible to argue that this function is acceptable, both to users and to Polar itself. As it turns out, this function has become very popular. This may not be because people actually want to use this function, but simply because they are not aware of what kind of data they are distributing. As a result, Polar has temporarily disabled the function [35]. As it turns out in the statement, Polar clearly states that no leakage of data has occurred. It still raises some concern on how public data may be used. As the Explore function offers very detailed user information, there may exist a potential threat to the user. This may for example be the profiling of any user based on various data. It would not necessarily be that hard for a maliciously intended person to form a clear view of when a person is out for a training session on a regular basis. People tend to maintain regular training habits. Just by evaluating this, a malicious person would be able to, and, most likely find out, *where the person lives*, *when he or she is at home*, *the health condition of the person*, and so on. This is one of the reasons why Polar chose to temporarily disable the service.



Privacy

Here you can adjust who can see your profile, your training sessions and your activity summaries. You can control the privacy settings for all of these individually.

Please note that when you allow people to see your training sessions with GPS data, it means that they can also see their precise geographic map locations. If you train in sensitive locations, you should always keep your sessions in Private mode.

When commenting, your name and picture will be shown next to your comment, regardless of your profile privacy setting. Also, if you share your training session or activity summary, or you join a group, club or an event, your name and picture will be shown.

Learn more here.

Confirm followers automatically*: Yes [✓ No]

If you don't confirm followers automatically, you get a notification about each new request to follow.

Privacy of your profile*: Public Followers [✓ Private]

Public: Everyone can see your full profile.
Followers: Only your followers can see your full profile. Your name, picture, city, state and country can be found by search.
Private: Only you can see your profile. It cannot be found by search.

Privacy of your sessions*: Public Followers [✓ Private]

Public: Everyone can see your training sessions.
Followers: Only your followers can see your training sessions.
Private: Only you can see your training sessions.
Changing these settings affects only future training sessions.

Session history: Update all to Private

You can also change the privacy setting for each individual training session in your Feed or the Training analysis view.

Privacy of your activity summaries*: Public Followers [✓ Private]

All your activity summaries can be seen on your followers' feed, unless you've set them as Private.

Polar Club communication: □ Fitness clubs can send me my Polar Club session summary via email.

Terms of Use

To use a Polar account and the Polar Flow service you need to agree with the use of your data as described in the Polar Privacy Notice. Here you can manage your privacy settings and learn more about how, and why Polar uses your data. Still not sure what this means? It's all explained in more detail in our Privacy Notice and FAQ.

To manage your account, go to https://account.polar.com

Privacy Notice*: ☑ I have read the Polar Privacy Notice. Read more

Terms of Use*: ☑ I have read and agree to the Polar Terms of Use. Read more

Personal data*: ☑ I agree that Polar may collect and process my personal data as described in the Polar Privacy Notice. I can change my settings about this consent at any time.

Transfering personal data*: ☑ I agree that my personal data may be transferred and processed outside my country of origin as described in the Polar Privacy Notice. I can change my settings about this consent at any time.

Sensitive data*: ☑ I agree that Polar may collect and process my sensitive personal data such as heart rate and other health data considered as sensitive data as described in the Polar Privacy Notice. I can change my settings about this consent at any time.

Figure 3.6: The Polar Flow Privacy Settings.

3.7 Summary

In this chapter we have studied the smartwatch Polar M600 and its endpoints (Polar Flow/Android Wear), as well as looked at general regulations for measuring privacy. This watch can be considered representative to the smartwatch market and, we have therefore elaborated on its functionality and architecture. A possible data flow for such a system has been presented, and we can see that by introducing such a flow, responsibilities associated with privacy follow.

Both the endpoints Polar Flow and Android Wear have been explained quite specifically with focus on security and privacy.

The Privacy Labeling has been presented on a scale from A++ (top score) to F (fail). In order to precisely determine a label, we have also introduced four main elements that need to be considered, namely *Controlled collection*, *Controlled processing*, *Controlled dissemination* and *Invasion prevention*.

This chapter is a contribution to Q2 (*What methods can be used to assess privacy?*) as we have discovered what data need to be measured in order to evaluate the system. The findings are:

- A privacy measurement needs to include several parameters. This needs to be minimized into general terms so that it can be applied to any kind of system.

- Another challenge that seems to appear, is the translation from technical parameters into actual numbers. The Multi-Metric method states that an "expert within the field" [16] should calculate these values. As for now, this is the best option, but might not work on a larger scale, as there would most likely be large variations between the experts. Therefore, my recommendation is to introduce some centralized database where privacy values are presented so that an expert can use these within the metrics.

The next chapter (*chapter 4*) will address the methodology (the Multi-Metric method) that is to be used for measuring a Privacy Label. We will present a step-by-step guidance of exactly how the method translates technical parameters into measurable privacy values.

Chapter 4

Assesment methodology for privacy

This chapter will address the Multi-Metric method and explain how it may be used for measuring privacy for a specific product. An example of how the method is applied will be provided, and how the method may be used for determining a Privacy Label will also be discussed.

4.1 A translation from the technical parameters

As discussed in section 3.6.1, we have to find a way of measuring the privacy. As we look further, we will also need to find a way for translating these measurements from technical parameters into actual privacy values. This translation is done mostly by applying the Multi-Metric approach. Later in chapter five, the Multi-Metric method will be applied to the Polar M600.

4.1.1 The Multi-Metric approach explained

The Multi-Metric approach is a methodology for measuring the *Security*, *Privacy* and *Dependability* (SPD) of a system. The methodology takes both a birdseye look at the system from a general perspective, and combines this with the core functionalities of the system. By combining all the values together, we will end up with a result between 0 and 100, which will be the $\text{SPD}_{\text{System}}$ and, in this case, will be focused on privacy only. At the very beginning of the methodology, we will set an SPD_{Goal} for the privacy. This value will be what we expect to be the outcome.

This function gives a much more precise overview of which privacy issues the system may have and exactly where the issues are located. In order to present a more precise overview, we will need to divide the system into *Subsystems*. Each subsystem consists of different *Components* and their privacy is measured as a *Criticality* value. For each subsystem we will set up a variety of different *Scenarios*. Each scenario will have its own SPD_{Goal}. Furthermore, we will make a variety of *Configurations* which may apply to all scenarios. Finally, different metrics need to be defined for each component (e.g. Wi-Fi connectivity). Assuming that we are describing the component encryption, two possibilities for how this component can be used exist, namely *On* or *Off*. We will also be adding a *Weight* to each component, based on what impact the component will have (in this case, the privacy). Both outcomes will have a criticality value for *Security*, *Privacy* and *Dependability* (in this case, just privacy). Each component's criticality value is calculated together in order to create the criticality value of the subsystem. By combining the results from all the subsystems, we will finally get a total $\text{SPD}_{\text{System}}$.

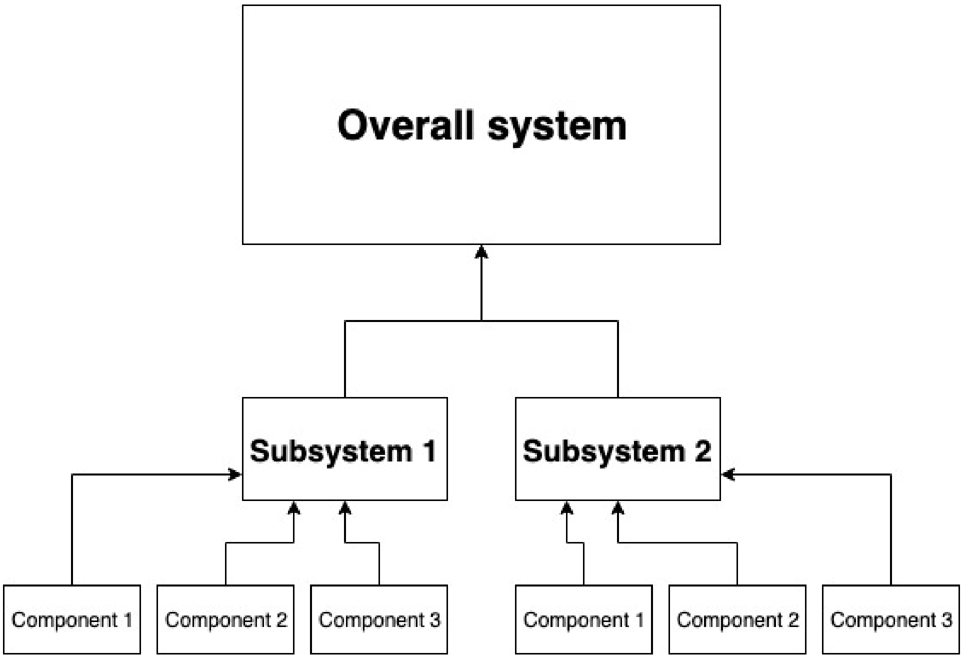


Figure 4.1: The Multi-Metric method visualized.

4.1.2 Example: Applying the Multi-Metric method

In order to apply the Multi-Metric method, we will need to address one *Overall system*, at least two *Subsystems* and at least one *Component* for each subsystem. These components receive different *weights*, as well as *criticality values*, explaining its impact on the overall system.

Below, a short and simple example on how the calculation of these criticality values and weights are conducted, is presented. Two hypothetical metrics for *Component A* and *Component B* will be provided.

Component 1	$\mathbf{C_p}$
On	60
Off	5
Weight	**40**

Table 4.1: Component 1: Example of how a metric for a component (*component 1*) could have been presented.

Component 2	**Cp**
Public	70
Private	10
Weight	**50**

Table 4.2: Component 2: Example of how a metric for a component (*component 2*) could have been presented.

These values are calculated by applying the RMSWD (Root Mean Square Weighted Data) function as presented in Equation 4.1. The function presents how the criticality, C, is calculated. It is based on the actual criticality, x_i, and the weight, W_i.

$$C = \sqrt{(}\sum_i (\frac{x_i^2 W_i}{\sum_i^n W_i}))) \tag{4.1}$$

The function is applied for each *Configuration* which explains what/which components are to be used, or not. These configurations may be presented as follows:

- **Configuration A:** Component 1 is turned On. Component 2 is set to Private.
- **Configuration B:** Component 1 is turned Off. Component 2 is set to Public.

The measurement is conducted as follows when applying the RMSWD function. (We also need to subtract the result from the function by *100* in order to present it in a correct way.):

- **Configuration A:**

$$C_\mathrm{A} = \sqrt{(}\sum_i (\frac{(60^2 40)(10^2 50)}{40+50}))) \tag{4.2}$$

$$C_\mathrm{A} = 100 - 41 \tag{4.3}$$

$$C_\mathrm{A} = \mathbf{59} \tag{4.4}$$

- **Configuration. B:**

$$C_\mathrm{B} = \sqrt{(}\sum_i (\frac{(5^2 40)(70^2 50)}{40+50}))) \tag{4.5}$$

$$C_\mathrm{B} = 100 - 52 \tag{4.6}$$

$$C_\mathrm{B} = \mathbf{48} \tag{4.7}$$

Following calculation, we will see that the criticality of *Configuration A* ends up at *59*, while *Configuration B* receives a value of *48*. As this is done in a *quadratic manner*, we will be able to favour the higher and more critical parameters compared to doing it linearly. If we were to do it linearly, our results would have been as follows:

- **Configuration A:**

$$C_A = \frac{60 + 10}{2} \tag{4.8}$$

$$C_A = 100 - 35 \tag{4.9}$$

$$C_A = \mathbf{65} \tag{4.10}$$

- **Configuration B:**

$$C_B = \frac{5 + 70}{2} \tag{4.11}$$

$$C_B = 100 - 38 \tag{4.12}$$

$$C_B = \mathbf{62} \tag{4.13}$$

By doing it linearly, our result is slightly weighted in a more positive direction, which is not necessarily the reality when using the system according to our configurations.

When calculating the metrics linearly, we can see that the result is weighted in a slightly more positive way. This may not be the case in reality, as the system is most likely to disclose sensitive data in some way with the presence of critical component configurations (e.g. the configuration *Public* in component 2 with criticality value of 70).

4.1.3 Evaluation of the methodology

When applying the Multi-Metric methodology, the outcome will be a result based on the *actual criticality* of the device as compared to the assumptions made before applying the function. The overall goal is to come as close as possible to the original SPD_{Goal}, but this may vary.

In order to assign a Privacy Label to the product, we will use the outcome of the Multi-Metric method as the foundation for calculating the specific label. As mentioned, the outcome of the Multi-Metric method for each scenario ($\text{SPD}_{\text{System}}$) will be a value between *0* and *100*. We will get a result for each configuration with respect to a single scenario. This may be presented in a matrix in order to give a good overview. After obtaining a result, we will categorize it with respect to the original SPD_{Goal}. The result will be categorized with 3 different colors, namely green (passed), orange (medium) and red (fail). The criteria are as follows (compared to the SPD_{Goal}):

- Green: Within the range of ± *10*. Symbols the most suited configuration for a scenario.
- Orange: Within the range of ± *20*. Symbols the second most suited configuration for a scenario.
- Red: Everything else. Symbols the least suitable configuration for a scenario.

4.2 Key points in determining a Privacy Label

In order to establish a Privacy Label, this should be done with respect to the outcome of the Multi-Metric approach. When applying the Multi-Metric methodology, we will get a privacy score between 0 and 100. There will be a score for each configuration with respect to the given scenario. This score needs to be evaluated with regard to the *configurability* and *transparency* of the system. Such a system puts the user in charge of choosing between *functionality* and *privacy*. In order to measure this, we should have a look at all the results provided by the Multi-Metric method. Assuming that the results vary from *20* to *90*, we have a good indication that the system offers its users configurability so that they may configure their own privacy well. Assuming that all default privacy settings are set to private, this might also be weighted in a positive way. We may do this by combining all the final results and present an average privacy score. The function is shown in Equation 4.14. This equation calculates the privacy value P where x symbols the result for a given configuration, i, with respect to a scenario, divided by the total privacy results, x.

$$P = \frac{x^{i} + x^{i+1} + x^{i+n}}{\sum x} \tag{4.14}$$

There should be some relationship between the average result, P, and which Privacy Label the product ends up getting. In order to validate this method properly, we will need to apply it on more than one product. To say that an average result, P, of 100 is what it takes to get a Privacy Label A, does not make any sense, as no system is likely to meet this demand. This would also apply to Privacy Label F, which should not expect to get an average result P of 0. The result should be somewhere between 0 and 100, and so should the label be placed. This would mean that a system with an average score between 40 and 60 should be evaluated in a positive way when setting a Privacy Label.

On the other hand, this may not apply to all kinds of systems. If we for example have a system with very few configuration options for the end user, we should expect that most of the results would fall within the same range. Given a privacy aware system, we would expect higher scores. When looking at the average score for this system, we will most likely end up with a high average score. This should, obviously, be weighted in a positive way, but the Privacy Label should also here take the presence of *configurability* and *transparency* into consideration. If a system only offers high results for privacy measurement, we would expect the user not to be able configure his own privacy very well, as that would most likely have resulted in a more negative result.

The same holds for a system that only produces results in the middle (between 40 and 60). If we were to follow the statement above, the result ought to be weighted in a positive way, but in reality it should be weighted more negatively, as the presence of *configurability* and *transparency* is close to zero.

One way of solving this issue might be to introduce *configurability* and *transparency* as parameters for a metric. This could be done in the same way as with all other parameters, namely by giving them a score between 0 and 100 for the specific metric.

Either way, this issue needs to be met with some solution in order to use the Multi-Metric method for determining a Privacy Label.

4.2.1 Privacy Label as seen from a user perspective

In order to establish this Privacy Label, we must evaluate not only the product's functionality, but also consider how this label is presented to the user. In doing so, we will need to understand what the user perceives. The currently ongoing project SCOTT:BB26.G reads the following: *"The main purpose of Privacy Labeling is to present the outcome of the privacy certification to Users. However, privacy is highly difficult to present, compared to classical aspects like the Energy Consumption labels where the range is the number of consumed KW/hour"* [39]. As it points out, the value of privacy may be different from one person to another. This is because one person may not consider any given data as private, while another may.

If we look at a highly profiled person, for example a prime minister, he or she may have extremely high demands on how his or her data are handled. On the other hand, 40 year old "Ben" works as an accountant and has no such demands. Where the prime minister cannot accept that his data are being stored for more than 6 months, "Ben" might want to have his data stored for a longer time so that he can browse through his history. In other words, privacy can be perceived relative to each person. Therefore, it is difficult to define a Privacy Label based on just the user's demands. The evaluation will rather need to focus on the product's functionality and how the data are treated.

4.2.2 Privacy Label seen from a vendor perspective

As of today, there are different regulations for deploying a product on the European market. The newest regulation is the GDPR (General Data Protection Regulation) from the EU. This regulation took place in the European market on May 25th, 2018. In summary, the goal of this regulation is to give the users more control over their own data, and they can at any point demand to (electronically) have all the information that has ever been stored about them. Furthermore, each user can demand to get all private information deleted from the platform/service. If a company fails to meet these demands, it may face a fine of up to 4% of their yearly revenue or up to €20 million (which one is higher). These are just some of the demands that have been set by the European Union [17]. The regulation gives each vendor a larger responsibility for how they shall treat data connected to a EU citizen. This means that a company in the US will also be affected by the regulation, given that it offers a service where sensitive information belonging to a EU citizen is stored.

Another demand that is currently in process in the European Union, is a regulation called the *"ePrivacy Regulation"* [14]. No further details regarding this regulation will be explained in this thesis, but a short description will be provided. The regulation will replace the current *"Privacy and Electronic Communications Directive 2002"*. Its main focus is to ensure the confidentiality of the user when transmitting messages on a communication channel. In order to understand this, we first need to understand the meaning of *"confidentiality"*. The concept can be expressed as follows: *"Access must be restricted to those authorized to view the data in question"* [10]. This means that information shall not be made available to any unauthorized entity. Data can be secured in various ways, typically by encryption and access control.

The regulation may also apply to communication channels such as *Facebook* or entirely new interactive communication platforms in the future. As of today, there are no clear requirements for how the confidentiality of each user should be ensured. With the new regulation, there will be a set of specific criteria and rules for how user confidentiality should be ensured. If a company, or a platform, fails to fulfill the demands, it may face the same fines as set in the GDPR, namely up to 4% of the annual revenue or up to €20 million (whichever is higher).

Both the GDPR and the ePrivacy Regulation are EU directives that each vendor will have to observe in order to be allowed to provide services to the citizens of the EU. These demands, at least the GDPR, will be extremely central if a Privacy Label is to be set for a given product. Shortly summarized, one would expect the vendor to emphasize the user's right to privacy and safeguard the confidentiality of the data transmitted and stored.

4.3 Two different privacy aspects to evaluate

To set a Privacy Label we need to consider different parameters. Many of these parameters have been covered above in the previous section, but some important aspects should still be evaluated. These criteria may be extremely important, as seen from a user's perspective. Given a top score on each of the following criteria, one may argue that the product should be awarded the *Privacy Label A*. While the product may be given label A, there may still exist a possibility for configuring the product in a way that will suit label C. What *configurability* is there? How is the *transparency* of the system? This will be described more extensively in the following subsections.

4.3.1 Transparency

One important element to consider when evaluating the privacy of a system, is how *transparent* the overall system is. According to the Cambridge Dictionary, *"transparency"* is defined as *"the characteristic of being easy to see through"* [50]. This means that we want to know for exactly what purpose the system or product want to collect specific data. We may say that the privacy level fall if transparency is lowered. In order to maintain privacy, the user should be able to "see right through" the system and be clearly presented for what purpose the system or product collect specific data as well as how it is being processed. One can compare the transparency of a program or a system to open-source programming. The vendor should not feel that the system needs to "hide" anything, rather it should show everything directly to the end user. Transparency adds up the second element for measuring privacy, namely controlled processing.

4.3.2 Configurability

Another aspect to evaluate is the *"configurability"* of the system. As mentioned earlier, a system can both be classified as Privacy Label A and C if we just focus on how data are treated. The aspect of configurability impacts how we may classify a certain privacy level. In order to be classified as for example label A, one will expect that the user is able to configure the product or system in such a way that the user has full control over his data, and that they are being kept private. This means that the privacy is defined by the user, rather than the vendor. As earlier discussed in section 4.2.1, the value of privacy may be relative to any given person, possibly based on his perceived status in society.

4.4 Summary

In order to be able to set a Privacy Label, we have seen that there are certain areas we must take into consideration. The main tool for translating the technical parameters into actual values may be the "Multi-Metric" function while we will have to take both users and vendors into consideration.

As discussed before, the actual privacy value for each person may vary and needs to be seen as *subjective*. We therefore concluded that the privacy measurement cannot be based on how a certain person will evaluate it, but rather look at the general functionality of the product. Regarding the functionality, we have covered four areas, namely *Controlled collection, Controlled processing, Controlled dissemination and Invasion prevention*. These four areas will impact the weighting for a Privacy Label. These findings adds up the choice (*Multi-Metric vs Privacy Quotient*) of the method even more.

The vendors will, with a Privacy Label regulation, be held more responsible for how the privacy of each user is ensured. As mentioned earlier, the vendors are already obligated to follow the requirements of the GDPR. This regulation very much adds up to the concept of *controlled collection*, as it focuses on how the data are being stored. It also supports the concept of *controlled processing*, as it demands the vendor to clearly specify which data are being stored as well as how the data are being treated. The new and upcoming *ePrivacy* regulation was also shortly mentioned. This regulation focuses on the confidentiality of the data being processed on the vendor's platform. The Privacy Labeling should also cover this area from the vendor's perspective, as a confidentiality breach may affect the privacy of the user. This may apply to both element one and three (*controlled collection* and *controlled dissemination*). To summarize the chapter, we have covered which method will be used to translate the technical parameters to actual values.

This chapter is a contribution to Q3 (*What are the challenges when applying measurable privacy?*). How the technical parameters may be translated into actual privacy values was the topic being discussed. The chapter has addressed the following:

- This chapter also points out the need for a centralized database of privacy values in order for the Multi-Metric method to be applied on a more general basis. This will make the method more consistent as we will exclude large variations of privacy values from expert to expert.

- This chapter also pointed out that both *transparency* and *configurability* should be taken into consideration when measuring the Privacy Label for a product. Given that the product offers high configurability, this should be weighted in a positive way. This holds for the transparency, too. Looking at a system that processes sensitive data and presents high configurability for the end user, we may expect the outcome result of the Multi-Metric method to vary on quite a large scale. This is because the end user is able to configure his profile to either full privacy, no privacy or somewhere in between. Assuming that all configurations are set to private by default, this system should be evaluated in a positive way. The results from the Multi-Metric method will then vary quite a bit. This would mean that if the average of all scores are somewhere between the middle of 40 and 60, the system should be weighted in a positive way.

  An issue when calculating the average score for systems that lack *transparency* and *configurability* (was also mentioned in section 4.2). Even though these systems would receive an average score between 40 and 60, they would not necessarily be weighted in a positive way. As for now, there are no clear guidelines regarding this aspect of the method. One suggested way of doing this is to simply introduce configurability and transparency as parameters for each metric. These parameters will be weighted with a criticality value between 0 and 100, as with all other parameters. Nevertheless, this issue needs to be solved in order to use the Multi-Metric method for measuring privacy.

The following chapter (*chapter 5*) initiates the next section of this thesis, the Use-case scenario. Chapter 5 will apply the measurement method (Multi-Metric) on the chosen use-scenario (Polar, focusing on Polar M600 and Polar Flow).

Part II

Use-case scenario

Chapter 5

Applying the Multi-Metric method

In this chapter we will apply the Multi-Metric method. The purpose of doing so is to use the result from the method to set a Privacy Label. When applying the method, we will first need to point out the overall system, then the different subsystems (the smaller parts of the overall system). In this case, the overall system will be the *Polar* platform, or brand, which is, a combination of two subsystems. These are *Polar Flow* and *Polar M600*.

5.1 Description of the different subsystems

The Polar Flow is, as pointed out earlier, a platform that combines and processes various health data. In order to evaluate the privacy level of the system, configurability and transparency will be two important elements. Polar Flow is an online accessible platform which offers a variety of functionalities, based on the user's training data. Given that the configurability of the service is not well maintained, this service has a potential for causing huge damage to any given user (e.g. through monitoring by unauthorized entities).

Polar M600, on the other hand, will collect the data and transmit to Polar Flow. When applying the Multi-Metric method to this sub-system, we should also look at the physical dimensions of the watch. Additionally, we will have to look at the four main elements for measuring privacy, especially the *Controlled dissemination* and the *Controlled collection*.

One may argue that *Android Wear* should have been chosen as a subsystem, as well. This is because it is possible to use the Polar M600 without the Polar Flow. We have made a choice, though, to focus more on the Polar M600 and the Polar Flow. One proposal, however, is that a stand alone project should look deeper into the data flow between Polar M600 and Android Wear.

5.2 Scenarios

Below, four different scenarios for the use of the Polar M600 and Polar Flow will be presented. All four scenarios will present a different view on privacy. Four different scenarios have been created, because these mainly describe various ways of using the system with regard to privacy. There are obviously different ways to using the system, but these four scenarios should be sufficient towards evaluating the system. Each scenario will be assigned a SPD_{Goal} with respect to *Privacy*. The goal of each scenario is a value between 0 and 100, where 100 is considered the highest and best. As stated earlier, this function is capable of evaluating both *Security* and *Dependability*. As we will be ignoring these two elements, we will have to leave the fields for *"S"* and *"D"* blank.

5.2.1 Scenario 1: Extreme privacy awareness

"John" is a privacy aware person who wants to ensure that all his sensitive data are being handled in a safe manner. Although being extra aware, he still wants to utilize the full functionality of the watch. He therefore chooses to use the watch in stand-alone mode without connecting it to the Polar Flow web service. His choice may lead to a more limited functionality, seeing the system from an overall perspective, but "John" will still be able to monitor his training sessions as captured by the watch. Since "John" chooses not to connect his watch to any external endpoint (e.g. smartphone), he also chooses to deactivate all wireless connectivity to the watch (e.g. Wi-Fi and Bluetooth). He also sets a screen lock for unlocking it.

$\mathbf{SPD_{Goal} = (S, 90, D)}$

For this scenario, we are aiming at a privacy goal of 90. This is quite high, but we would expect that leaving all the data on the watch will ensure privacy at the highest possible level. The risk of physically stealing the data are the larger drawback, but since the watch also offers a possibility for setting a pin code, one may expect that the privacy is sufficiently safeguarded. Since the possibility of connecting the watch via Wi-Fi or Bluetooth is also disabled, we assume that no unauthorized entities will be able to connect to or eavesdrop the watch.

5.2.2 Scenario 2: Medium privacy awareness

"Kate" has what we would call an average awareness of privacy. This means that she would want to use most of the functionality in the overall system but at the same time takes her privacy into consideration. She therefore chooses to synchronize all data from the watch directly to Polar Flow on her smartphone, via Wi-Fi or Bluetooth. She then maintains the possibility for using most of the functionality that the overall system offers. As pointed out above, "Kate" would then be "medium privacy aware" of her privacy, which means that she configures Polar Flow to the highest privacy setting. All of her data will be private and inaccessible to anyone in the

Polar Flow community. She also chooses to add a screen lock to her watch to unlock it.

SPD_{Goal} = (S, 80, D)

The privacy goal of this scenario is set to 80. This is because of the fact that "Kate" chooses to synchronize the data with Polar Flow, which extends the attack surface and also the value chain for where data are flowing. The SPD_{Goal} is still set pretty high because one should expect Polar Flow to handle the data in a safe way when all privacy settings are set to private. Another aspect which occurs when synchronizing data, is the possibility for eavesdropping on transmitted data. "Kate" connects via a third party, which automatically decreases the privacy level. However, one would again expect both Polar M600 and Polar Flow to handle the transmissions in a secure way.

5.2.3 Scenario 3: Regular privacy awareness

"Nancy" could be classified as a *"regular person"*. The statement *"regular"* means that she will use most of the functionality coming with the overall system. She chooses to synchronize all data captured with the watch directly to Polar Flow via her smartphone. This means that all data are stored in the overall Polar system. Furthermore, she chooses to open up to the possibility of sharing data with her friends. This is a privacy option offered by Polar Flow which means that the people "Nancy" accepts as friends, will be able to monitor all her training results as they are uploaded to Polar Flow. She also chooses to join a public group within the Polar Community that offers the possibility for sharing training sessions with all the people of the group.

SPD_{Goal} = (S, 60, D)

"Nancy" receives a privacy score of 60 in this scenario, because she gives access to all of her privately monitored data to her friends (as accepted personally by "Nancy"). This, however, also introduces an ethical or social question, namely the implicit trust of sharing information with people she already knows. Most likely none of her friends will abuse the information, but there is a possibility for a maliciously intended person to attempt a *social engineering* attack. This may be conducted by someone pretending to be a friend and who she accepts, following a follower's request. Another element to consider is "Nancy's" choice of joining a public group. By joining a group, she reveals all the data that she herself uploads to the group. Anyone joining the group will be able to stay on as a spectator, monitoring all activities. Such a spectator will be able to even *"relive"* her training sessions. "Nancy" also leaves a possibility for eavesdropping by transmitting data between watch and smartphone.

5.2.4 Scenario 4: No privacy awareness

In this scenario, "Alice" chooses to fully disclose all her data on a public level. She configures all privacy settings to public, which means that basically everyone will be able to have a look at her training data, as synchronized with Polar Flow. In other words, people registered within the Polar Community do not need an acceptance from "Alice" to monitor her data. They can look at them directly via her profile. Furthermore, she chooses to join a public group and regularly posts new training sessions to the group. This means that she is able to use the full functionality of the overall Polar platform.

$\mathbf{SPD_{Goal}}$ = (S, 30, D)

"Alice" receives a score of 30 for this approach. The scenario aims to utilize the functionality of Polar Flow and the Polar M600 as much as possible. With that said, the privacy will automatically decrease. This is because "Alice" chooses to fully disclose all personal data as monitored by the watch. In doing so, she can use the overall system at its most, but it also leaves her in a possibly harmful position. This is because anyone registered in the Polar Community will be able to fully monitor all her data as they are uploaded, and even relive them. This may lead to the *profiling* of "Alice" by a maliciously intended person. By regularly watching her training behaviour over time, a malicious person can possibly map and predict where "Alice" will be at any given time in the future. This information can be used for further malicious purposes. Her privacy score also falls because she joins a public group and regularly posts her training data, which broadcasts her public profile to all the people in the group.

5.3 Device configurations

A device configuration is meant to present how the system can be used. The configuration defines what components are to be used, as well as configuring the components' parameters. One scenario should at least have *two* configurations that aim to fulfill the specifications presented by the scenario. Still, all configurations may be applied to any scenario, but we want each scenario to have at least two configurations that are especially configured to meet the specifications.

Below, *8* different possible device configurations are presented. These configurations are determined with respect to the four different scenarios. This means that each scenario will be assigned two different configurations.

- **Configuration A:** Screen is unlocked with a custom drawn pattern on the watch. Bluetooth is turned off. Wi-Fi is turned off.

- **Configuration B:** Screen is unlocked with a custom 6 digit PIN code. Bluetooth is turned off. Wi-Fi is turned off.

- **Configuration C:** Screen is unlocked with a custom 6 digit PIN code. Bluetooth is turned on. Wi-Fi is turned on. Data are automatically synchronized to Polar Flow via app. The privacy of the profile is set to private. Privacy of sessions is set to private. Privacy of activity summaries is set to private. Not joining a group. Manually confirms new followers.

- **Configuration D:** Screen is unlocked with a custom password. Bluetooth is turned on. Wi-Fi is turned on. Data are automatically synchronized to Polar Flow via app. The privacy of the profile is set to private. Privacy of sessions is set to private. Privacy of activity summaries is set to private. Joins a public group, but does not publish. Automatically confirms new followers.

- **Configuration E:** No screen lock. Bluetooth is turned on. Wi-Fi is turned on. Data are automatically synchronized to Polar Flow via app. The privacy of the profile is set to followers. Privacy of sessions is set to followers. Privacy of activity summaries is set to followers. Joins a public group, but does not publish. Manually confirms new followers.

- **Configuration F:** Screen is unlocked with a custom 6 digit PIN code. Bluetooth is turned on. Wi-Fi is turned on. Data are automatically synchronized to Polar Flow via app. The privacy of the profile is set to followers. Privacy of sessions is set to followers. Privacy of activity summaries is set to followers. Joins a public group and regularly publishes to the group. Automatically confirms new followers.

- **Configuration G:** Screen is unlocked with a custom 6 digit PIN code. Bluetooth is turned on. Wi-Fi is turned on. Data are automatically synchronized to Polar Flow via app. The privacy of the profile is set to public. Privacy of sessions are set to public. Privacy of activity summaries is set to public. Joins a public group, but never publishes. Automatically confirms new followers.

- **Configuration H:** No screen lock. Bluetooth is turned on. Wi-Fi is turned on. Data are automatically synchronized to Polar Flow via app. The privacy of the profile is set to public. Privacy of sessions is set to public. Privacy of activity summaries is set to public. Joins a public group and regularly publishes to the group. Automatically confirms new followers.

5.4 Component metrics for privacy evaluation

Below is presented a metric for each component to be evaluated in the Multi-Metric method. Each metric contains a set of different parameters (e.g. On and Off), which have their own criticality. This shows how critical the parameter is, related to the privacy of this specific metric. Furthermore, each metric contains a weight, representing the impact the whole metric would have on the overall system. An example may be the sharing of personal data with friends. If one chooses to share private data with friends, this may effect a higher criticality value than not sharing one's data. This metric will also have an impact on the overall system, and, the value given should reflect this impact. The values given are always within the range of 0 and 100, where 0 represents an impact as low as possible and 100 represents an impact as high as possible.

5.4.1 Bluetooth

When turningcHth 916183 Bluetooth on (on the Polar M600), the watch will be able to short range connect to Polar Flow on a smartphone. It will constantly broadcast within its range. This metric offers two different parameters, On and Off. Assuming that Bluetooth is turned on, our privacy will automatically be more exposed, as the device will broadcast and let anyone know its presence within a short distance. Still, it should not be given any higher criticality value than *40*, as the connection will need an authorization from the device, and the distance range is also quite small. With Bluetooth turned off, we may assume that privacy can only be exposed through a physical attack. This is because the Multi-Metric method only focuses on one component at a time and does not consider other components (such as Wi-Fi). Still, it should be assigned a criticality value as the data are stored locally and may be accessible if a physical attack is conducted. Therefore, it receives a criticality value of *5*. The weight is set to *10* and may be explained with the fact that Bluetooth only offers connectivity within a close range on closed transmission channels, and, also a need for authorization upon connecting.

Bluetooth	$\mathbf{C_p}$
On	40
Off	5
Weight	10

Table 5.1: M1 - Bluetooth component metric.

5.4.2 Wi-Fi

When activating Wi-Fi on the Polar M600, the watch will be able to distribute data directly to the Polar Flow app on a smartphone at a larger range than via Bluetooth. When using a Wi-Fi connection the watch constantly broadcasts across the network. This metric also offers two parameters (On and Off). To some extent, this metric is quite close to the Bluetooth metric, but exposes the user's privacy slightly more. This may be supported by the fact that activating Wi-Fi will broadcast in a larger area, and is also why turning it on receives a criticality value of *45*. The criticality alone does not necessarily represent the difference between Wi-Fi and Bluetooth, but when introducing a weight of *25*, we will get a more precise overall result. When turning Wi-Fi off, the same criticality value holds, as it does for Bluetooth. The fact that data are stored locally will offer a potential for a physical attack where the privacy may fall and is, thus, the reason for assigning a criticality value of only *5*.

Wi-Fi	**C_p**
On	45
Off	5
Weight	25

Table 5.2: M2 - Wi-Fi component metric.

5.4.3 Screen lock

By setting a screen lock on the Polar M600, the user lowers the risk for a physical data attack. In order to determine what criticality values the three different screen lock methods should be given, we first need to address the security difference between them. In the report *"Towards Baselines for Shoulder Surfing on Mobile Authentication"*, Aviv et al. address the differences between a screen lock pattern and a PIN code [6]. Based on their research, they have found that *"We find that 6-digit PINs are the most elusive attacking surface where a single observation leads to just 10.8% successful attacks (26.5% with multiple observations). As a comparison, 6-length Android patterns, with one observation, were found to have an attack rate of 64.2% (79.9% with multiple observations). Removing feedback lines for patterns improves security to 35.3% (52.1% with multiple observations)."* A password is considered more secure as the possible combinations increase drastically.

The impact of a physical attack may be critical when considering the privacy. If no screen lock has been set, the risk for leaking sensitive data increases drastically. This is also the reason for assigning a criticality value of *70*. It might be possible to argue that this value should have been even higher but the fact that a *physical* attack needs to be conducted should also be taken into consideration. The risk for such an attack appearing is quite a bit lower than for example a cyber attack. Considering a 6-digit PIN code, we've set a criticality of *20* which sets it in the middle of the three authentication mechanisms. A PIN offers both a quick way for entering the watch, as well as a medium security level related to authentication. A drawing pattern receives a criticality value of *25*. This value underlines the fact that such a solution is considered less reliable than for example a custom password. Setting a password will be assigned a criticality value of *10* which reflects the strengths of this solution. At the end point of this metric, we set the weight to a value of *40*. The reason for this given value is, as before mentioned, that a physical attack would first need to be conducted. Given that the object is a watch, the risk of an attack occurring thus significantly falls.

Screen lock	$\mathbf{C_p}$
Password	10
Pattern	25
PIN	20
No screen lock	70
Weight	40

Table 5.3: M3 - Screen lock component metric.

5.4.4 Automatic synchronization

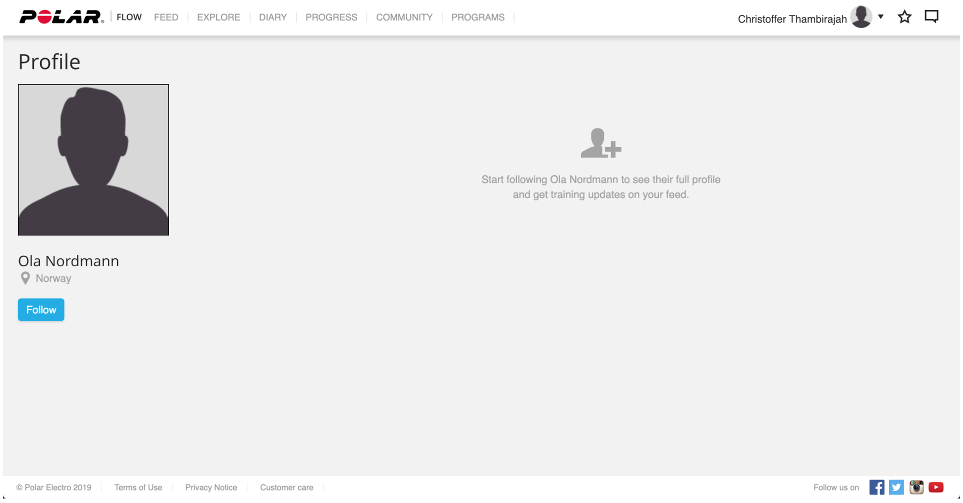
By enabling automatic synchronization to Polar Flow, the watch will automatically synchronize all new training sessions having been recorded. This increases the risk for eavesdropping or data leakage, but one should expect that Polar transfers the data in a secure way. This metric offers two parameters as well, On and Off. By automatically synchronizing training data to the app (the Polar Flow platform), the user will instantly lose control of the data. The user needs to activate this synchronization manually. By giving this metric a weight of *60*, we state that the user has given up a lot of his privacy to Polar. One should assume that Polar will use the data in a safe manner and that the user has the full right to choose how the data shall be processed. When turning on synchronization, we assign a criticality value of *50*, which reflects the fact that data are starting to become available to other entities, other than just to the owner of the watch (e.g. Polar Flow). When turning synchronization off, the user is vulnerable only to physical attacks (assuming that Bluetooth and Wi-Fi, too, are turned off). This will leave us in the same situation as turning Wi-Fi or Bluetooth off and will therefore result in the same value, namely *5*.

Automatic synchronization to app	$\mathbf{C_p}$
On	50
Off	5
Weight	60

Table 5.4: M4 - Automatic synchronization component metric.

5.4.5 Automatic confirmation of new followers

When enabling the function for automatically confirming (all) new followers, privacy falls quite significantly. Given that this function is set, we will basically offer anyone the ability to follow one respective profile. The privacy must be seen in context with the privacy settings having been set for the profile, as well. If a user chooses to automatically confirm new followers, the user will be in a similar situation to setting his privacy settings for the profile to public (as mentioned in Table 6.1). Assuming that this automatic confirmation is activated, the user has no control of who will be able to survey his data (assuming that the user has configured the privacy setting to "Followers"). The privacy is drastically reduced upon activation and this results in a criticality value assigned to *75*. A representation of how this would work out is presented in images 5.1 (before *Follow*) and 5.2 (after *Follow*).

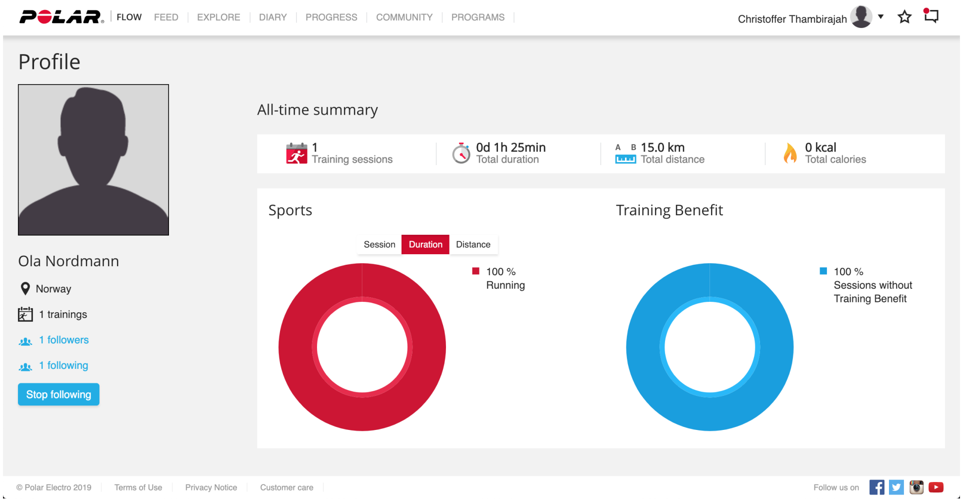


Profile

Ola Nordmann
Norway

Start following Ola Nordmann to see their full profile and get training updates on your feed.

Figure 5.1: Polar Flow: A user's profile before a *Follow* request has been confirmed.



Profile

Ola Nordmann
Norway
1 trainings
1 followers
1 following

All-time summary

1 Training sessions	0d 1h 25min Total duration	15.0 km Total distance	0 kcal Total calories

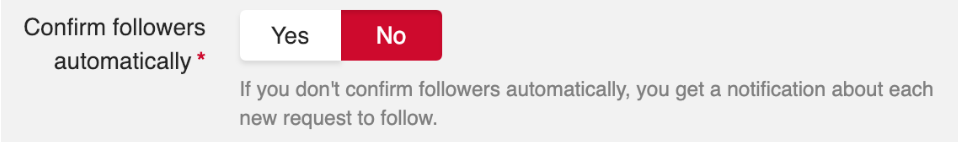
Sports

🟥 100 % Running

Training Benefit

🟦 100 % Sessions without Training Benefit

Figure 5.2: Polar Flow: A user's profile after a *Follow* request has been confirmed.



Confirm followers automatically * Yes [✓ No]

If you don't confirm followers automatically, you get a notification about each new request to follow.

Figure 5.3: Polar Flow: Configuring privacy for automatically confirming new followers.

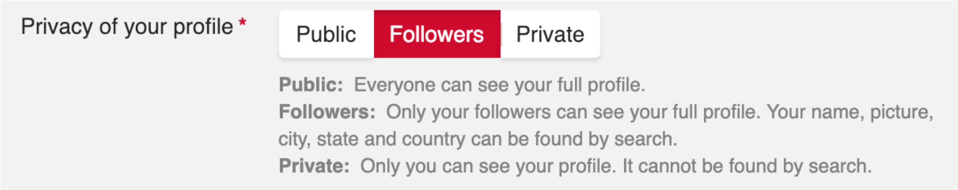
Turning off automatic confirmation of new followers would leave the user in control of who he wants to share data with. Still, there is a risk of an attack if the user thinks he knows the person trying to follow and therefore chooses to accept, while the follower actually turns out to be somebody else. Given this risk, the option receives a criticality value of only *5*. The weighting of this metric is set to *70* and is substantiated by most of the information given when turning the function on.

Confirm followers automatically	C_p
On	75
Off	5
Weight	70

Table 5.5: M5 - Component metric for automatically confirming followers.

5.4.6 The privacy of a profile

By permitting other profiles and insight into one's private profile, one also discloses basic information. Insight does not, however, grant access to synchronized training sessions. The parameters *Public* and *Private* both reflect the same as *On* and *Off* and therefore receive the same criticality values, namely *75* and *5*. The reason for claiming that *Public* holds the same criticality as "On" in this metric (Table 5.5) is because of the actual functionality of automatically accepting new followers (assuming that the privacy of the profile is set to *Followers*). This would leave the user in the same situation as if it was public. When it comes to the parameter *Followers*, it is reasonable to place it between the other two parameters as it limits the user to manually choose who he wants to share data with. The weighting of this metric should be in the same area as the metric in Table 5.5 simply because it offers most of the same functionality.



Privacy of your profile *

Public [✓ Followers] Private

Public: Everyone can see your full profile.
Followers: Only your followers can see your full profile. Your name, picture, city, state and country can be found by search.
Private: Only you can see your profile. It cannot be found by search.

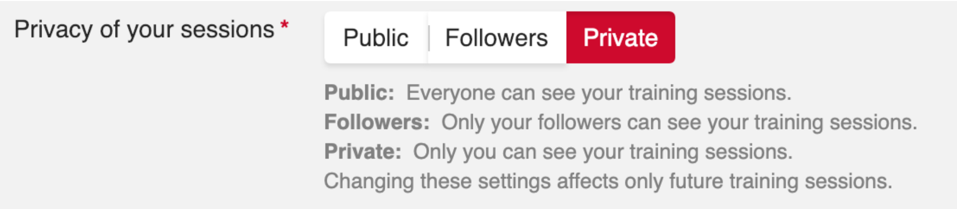
Figure 5.4: Polar Flow: Configuring the privacy of a profile.

Privacy of profile	C_p
Public	75
Followers	40
Private	5
Weight	70

Table 5.6: M6 - Privacy of a profile component metric.

5.4.7 Privacy of sessions

It is possible to choose which privacy setting one would like to have on all training sessions being synchronized with Polar Flow. Given that a user chooses to set this to *Public*, the user fully discloses all training sessions being synchronized. This also applies for the setting *Followers*, but it is restricted to followers accepted by the user. *Private* means that no one, except the user himself, have access to the data. As stated before, this function offers many of the same features as *Privacy of profile*, but the main difference is which training data are being presented. When configuring a profile to *Public*, one chooses to disclose all basic information. When configuring privacy of sessions to *Public*, one chooses to fully disclose all training data. That is the reason why we should increase the criticality value by 5 compared to the metric presented in Table 6.1. The same applies for the parameter *Followers*. The results then become *80* and *45*. Regarding the parameters *Private* and *Weight*, it is sufficient to use *5* and *70*, since the critical parameters are increased (*Public* and *Followers*), and they will therefore have sufficient impact on the overall result.



Privacy of your sessions *

Public: Everyone can see your training sessions.
Followers: Only your followers can see your training sessions.
Private: Only you can see your training sessions.
Changing these settings affects only future training sessions.

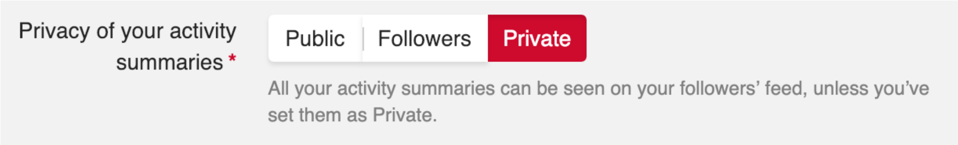
Figure 5.5: Polar Flow: Configuring the privacy of the sessions.

Privacy of sessions	C_p
Public	80
Followers	45
Private	5
Weight	70

Table 5.7: M7 - Privacy of the sessions component metric.

5.4.8 Privacy of activity summaries

THe system offers a possibility for disclosing activity summaries. This means that a user may disclose his activity summaries for either a specific crowd (*"Followers"*) or to everyone (*"Public"*). Such an activity summary may be seen in each user's *"Feed"*. For this metric, we need to address the fact that disclosing information publicly will give anyone full insight into each training summary, which may include quite sensitive information (e.g. pulse, route, etc.). Given that this is precise information, one should increase the criticality value, as well as increasing the weighting. Both the parameters *Public* and *Followers* are then assigned criticality values of *85* and *50*. As pointed out for the metric M7 in Table 5.7, it was sufficient to just increase the criticality while letting the weighting stay the same as in metric M6. For this metric, we should increase the weighting, as these parameters would have a larger impact on the overall privacy. The weight is therefore assigned a value of *80*. The option for leaving the privacy to *Private* will relate to the same condition as metrics M7, M6, M5 and M4.



Privacy of your activity summaries *

Public | Followers | Private

All your activity summaries can be seen on your followers' feed, unless you've set them as Private.

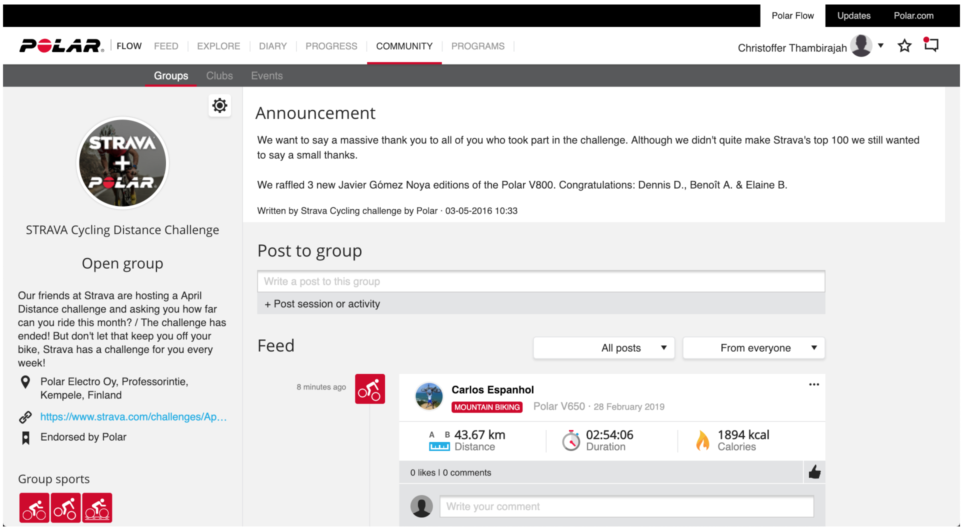
Figure 5.6: Polar Flow: Configuring privacy of activity summaries.

Privacy of activity summaries	$\mathbf{C_p}$
Public	85
Followers	50
Private	5
Weight	80

Table 5.8: M8 - Privacy of activity summaries component metric.

5.4.9 Groups

By joining a group, a user will be able to post both training sessions and monitor other member's training sessions. When posting a session to a group, one fully discloses the information to everyone in the group, independently of the privacy setting of one's own profile. The reason for assigning a criticality of *80* when regularly publishing sessions is that the user does not necessarily know the other members of the group. There is a slight risk for further disclosure of a profile that regularly publishes in a group, and it might go viral, ending up in the hands of people with whom the user not necessarily wishes to contact directly. Some of this applies to the second parameter as well (joining, never publishing sessions). The user is now possibly exposed to distribution, or marketing, efforts. The criticality value assigned is *40*, which is only half as high as if he had published sessions regularly. The reasoning behind this is, as mentioned, the power of marketing efforts. If a user exists within a group but never publishes any sessions, he still reveals his presence by being a spectator and, therefore, increases the risk of any unwanted entity trying to make contact or monitor his profile. What information such an entity will be able to collect would be relative, based on the other metrics, such as M8, M7 and M6. Not joining a group receives the same criticality value as the other metrics, M1, M2, M4, M5, M6, M7, and M8 (all except for M3, *Screen lock*), as it does not expose any information. The weight is set to such a high value as *65* because by joining a group, a user will by definition in any case give away valuable information. This may be because he chooses to publish data, or it can be just being by monitored in the group. By just being monitored by the group, the user discloses his basic information to the crowd in the group.



STRAVA Cycling Distance Challenge

Open group

Our friends at Strava are hosting a April Distance challenge and asking you how far can you ride this month? / The challenge has ended! But don't let that keep you off your bike, Strava has a challenge for you every week!

Polar Electro Oy, Professorintie, Kempele, Finland

https://www.strava.com/challenges/Ap…

Endorsed by Polar

Group sports

Announcement

We want to say a massive thank you to all of you who took part in the challenge. Although we didn't quite make Strava's top 100 we still wanted to say a small thanks.

We raffled 3 new Javier Gómez Noya editions of the Polar V800. Congratulations: Dennis D., Benoît A. & Elaine B.

Written by Strava Cycling challenge by Polar · 03-05-2016 10:33

Post to group

Write a post to this group

+ Post session or activity

Feed

All posts ▾ From everyone ▾

8 minutes ago

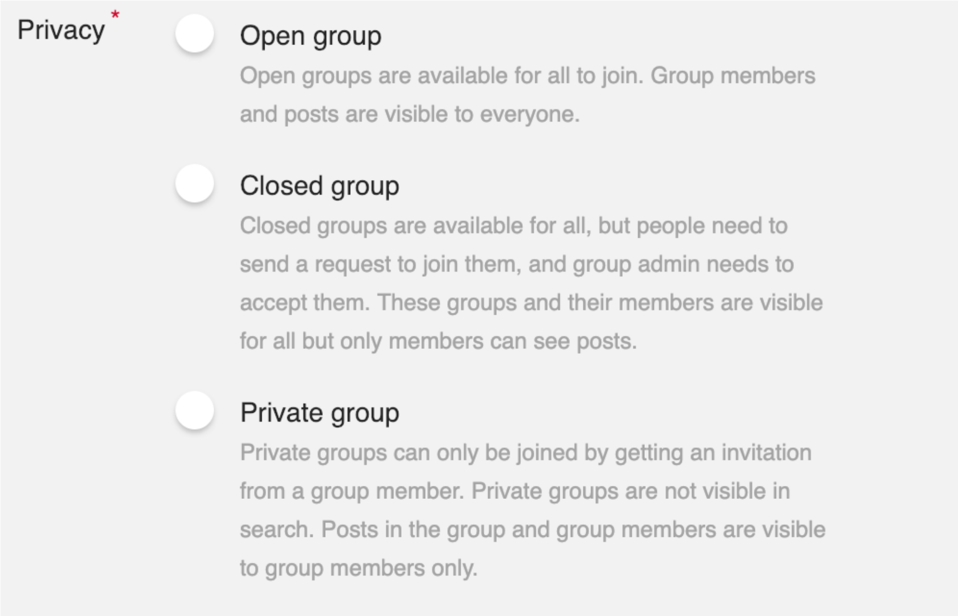
Carlos Espanhol
MOUNTAIN BIKING Polar V650 · 28 February 2019

43.67 km Distance
02:54:06 Duration
1894 kcal Calories

0 likes | 0 comments

Write your comment

Figure 5.7: Polar Flow: Presentation of what a public group looks like.



Privacy *

○ Open group
Open groups are available for all to join. Group members and posts are visible to everyone.

○ Closed group
Closed groups are available for all, but people need to send a request to join them, and group admin needs to accept them. These groups and their members are visible for all but only members can see posts.

○ Private group
Private groups can only be joined by getting an invitation from a group member. Private groups are not visible in search. Posts in the group and group members are visible to group members only.

Figure 5.8: Polar Flow: Privacy settings for group creation.

Groups	$\mathbf{C_p}$
Joining (regularly publishes sessions)	80
Joining (never publishes sessions)	40
Not joining	5
Weight	65

Table 5.9: M9 - Groups component metric.

Different metrics for each component with criticality values and weights expressing their impact on the *overall system* have been provided. All the values of each metric are meant to reflect the impact of this specific component and, therefore, does not take the impact of other metrics into consideration (even if they rely on them). The way the criticality values and weights are measured are to some extent seen in accordance with other metrics. To clarify this, the weights of *Privacy of sessions* and *Privacy of profile* are both set to *70*, as the impact of both metrics are the same.

All these values are subjectively assigned and may vary from one measurement to another.

5.5 Privacy assessment results

When finalizing the metrics, a need to present the metrics and configurations in a table presents itself. The metrics may be represented as *"M1, M2, M3..."* and the criticality as *"C1, C2, C3..."* (this thesis only considers privacy in the Multi-Metric method which is the reason for expressing only the *"P"* value, as it represent the Privacy for each metric). The metrics are meant to reflect each component used in the different configurations. This would mean that both configurations A and B will receive values from M1 and C1 (given that M1 and C1 are representative for the configurations A and B). Each configuration will then have a complete set of values for each metric with the criticality represented. For this specific evaluation, the different metrics will be presented as following:

- M1 - Bluetooth component metric
- M2 - Wi-Fi component metric
- M3 - Screen lock component metric
- M4 - Automatic synchronization component metric
- M5 - Automatic confirm new followers component metric
- M6 - Privacy of profile component metric
- M7 - Privacy of sessions component metric
- M8 - Privacy of activity summaries component metric
- M9 - Groups component metric

Once these values are placed into the table, the equation for the Multi-Metric method *RMSWD* (Root Mean Square Weighted Data) may be applied (the function as explained in Equation 4.1). This function will return a result for each configuration in what we call *"Actual Criticality"*. In order to receive a final result, we need to subtract the Actual Criticality from 100 (to present the result in the correct way). The result provided may subsequently be set up against the original scenario goal established before applying the method. A final result of 100 will then be considered *"perfect privacy"*, while a result of 0 will be considered *"no privacy"*. The configurations used when applying this method may be found in section 5.3.

The table below shows each *configuration* and its components (*C* metrics (*M*). The calculated *criticality* for each configuration is also presented. This is an overall table presenting all the results provided after applying the RMSWD function on the different configurations (as explained in Equation 4.1). In the subsections below, a more specific table for each scenario seen in accordance with the SPD_{Goal} of the given scenario is presented.

Criticality										$\textbf{SPD}_{\textbf{System}}$	
	C1	C2	C3	C4	C5	C6	C7	C8	C9		
Metric	M1	M2	M3	M4	M5	M6	M7	M8	M9	Criticality	$\text{SPD}_{\text{System}}$
	P	P	P	P	P	P	P	P	P		
Conf. A	5	5	25	-	-	-	-	-	-	19	81
Conf. B	5	5	20	-	-	-	-	-	-	15	85
Conf. C	40	45	20	50	5	5	5	5	5	22	78
Conf. D	40	45	10	50	5	5	5	5	40	26	74
Conf. E	40	45	70	50	5	40	45	50	40	45	55
Conf. F	40	45	20	50	75	40	45	50	80	55	45
Conf. G	40	45	20	50	75	75	80	85	40	66	34
Conf. H	40	45	70	50	75	75	80	85	80	73	27

Table 5.10: $\text{SPD}_{\text{System}}$ for the overall system Polar.

5.5.1 Results: Scenario 1 (Extreme privacy awareness)

Below, we were able to see the final results of scenario 1 after applying the Multi-Metric method. As presented in section 5.2.1, scenario 1 is about extreme privacy awareness. We would expect that the system safeguards the privacy as "John" chooses not to synchronize the watch with any third party, and also sets a screenlock.

SPD$_{\text{System}}$	**Scenario 1**		
Metric	**Criticality**	**SPD$_{\text{Goal}}$**	**SPD$_{\text{System}}$**
Conf. A	19	90	🟩 81
Conf. B	15	90	🟩 85
Conf. C	22	90	🟨 78
Conf. D	26	90	🟨 74
Conf. E	45	90	🟥 55
Conf. F	55	90	🟥 45
Conf. G	66	90	🟥 34
Conf. H	73	90	🟥 27

Table 5.11: SPD$_{\text{System}}$ for Scenario 1.

The results show that both of the intended configurations for this scenario (configurations *A* and *B*) *pass*. Furthermore, we notice that configurations *C* and *D* ends up as a *medium* result. The configurations *E* to *H* *fail*. This shows that the overall system meets our expectations for extreme privacy awareness.

5.5.2 Results: Scenario 2 (Medium privacy awareness)

This scenario aims to be "medium" privacy aware, exemplified by "Kate" who chooses to synchronize her data with Polar Flow, but still wants her privacy to be safeguarded. She therefore sets her privacy settings to *private*. Below, we were able to see exactly how the overall system reacted to this attitude towards privacy.

SPD$_{\text{System}}$	**Scenario 2**		
Metric	**Criticality**	**SPD$_{\text{Goal}}$**	**SPD$_{\text{System}}$**
Conf. A	19	80	🟩 81
Conf. B	15	80	🟩 85
Conf. C	22	80	🟩 78
Conf. D	26	80	🟩 74
Conf. E	45	80	🟥 55
Conf. F	55	80	🟥 45
Conf. G	66	80	🟥 34
Conf. H	73	80	🟥 27

Table 5.12: SPD$_{\text{System}}$ for Scenario 2.

The table for scenario 2 shows that configurations *A*, *B*, *C* and *D* all *pass*. This result very much adds up to the findings in the result table provided for scenario 1, as we notice that the overall system meets our requirements for both extreme privacy awareness and medium privacy awareness. Another noticeable element is the SPD_{Goal} that was set for this scenario (80). This goal tends to be slightly more precise and correct compared to the SPD_{Goal} set for scenario 1 (90). The rest of the configurations (*E* to *H*) *fail*.

5.5.3 Results: Scenario 3 (Regular privacy awareness)

In this scenario, "Nancy" aims to be a so called "regular" person. She synchronizes all data from her watch to Polar Flow. She furthermore wants to share her data with friends. The results below present how the overall system reacts to this approach with respect to the SPD_{Goal}.

$\text{SPD}_{\text{System}}$	**Scenario 3**		
Metric	**Criticality**	**SPD_{Goal}**	**$\text{SPD}_{\text{System}}$**
Conf. A	19	60	81
Conf. B	15	60	85
Conf. C	22	60	78
Conf. D	26	60	74
Conf. E	45	60	55
Conf. F	55	60	45
Conf. G	66	60	34
Conf. H	73	60	27

Table 5.13: $\text{SPD}_{\text{System}}$ for Scenario 3.

The results of scenario 3 *pass* one of its intended configurations (*E*) and receive a *medium* result for its second intended configuration (*F*). The scenario receives a *medium* result for configuration *D* as well. These results tells us that the overall system is able to deliver *Regular privacy* to some extent, but not necessarily as precisely as we aimed for. The rest of the configurations (*A* to *C* and *G* & *H*) *fail*.

5.5.4 Results: Scenario 4 (No privacy awareness)

For scenario 4, "Alice" chooses to be as transparent as possible. She chooses to synchronize all data captured by the watch directly to Polar Flow and leave them all public for anyone to monitor. The results below present how the system reacts.

SPD$_{\text{System}}$	**Scenario 4**		
Metric	**Criticality**	**SPD$_{\text{Goal}}$**	**SPD$_{\text{System}}$**
Conf. A	19	30	81
Conf. B	15	30	85
Conf. C	22	30	78
Conf. D	26	30	74
Conf. E	45	30	55
Conf. F	55	30	45
Conf. G	66	30	34
Conf. H	73	30	27

Table 5.14: SPD$_{\text{System}}$ for Scenario 4.

The last scenario receives a *pass* on both intended configurations (*G* and *H*). Configuration *F* receives a *medium* score with regard to the SPD$_{\text{Goal}}$. Notable from this result is the fact that we are fully able to configure *No privacy*. The rest of the configurations (*A* to *E*) fails.

5.6 Summary

This chapter has applied the Multi-Metric method for the overall system, Polar, and focused on the subsystems Polar Flow and Polar M600. We provided a short description of the two different subsystems with focus on functionality. Furthermore, we introduced four different scenarios. These four scenarios were meant to reflect the different ways it was possible to use the overall system with the given specifications for each subsystem.

The first scenario was being extremely privacy aware, while the other three slowly, but surely, removed the focus on privacy. Scenarios 1 and 4 were both extremes, while a more "regular" person might have related to either scenario 2 or 3. Furthermore, we introduced different configurations, which may be seen with respect to the scenarios. This means that configurations A and B are meant to reflect scenario 1, while configurations C and D are meant to reflect scenario 2, and so on. The first two configurations started off by being extremely privacy aware, while the focus for the rest on privacy slowly dropped (the focus changes from *privacy aware* to *functionality aware*). After defining the configurations, a metric was introduced for each component. Such a metric aims to present the different states a component may be in. In the end, the Multi-Metric method was applied to the overall system based on the values from the scenarios, the configurations, and the metrics. It turned out that the overall system was quite close to what we expected would be the outcome, which again provides a quite configurable system. The results vary all the way from 30 to 85 which emphasizes the configurability (the user seems to be able to configure his own privacy quite well).

Next chapter (*chapter 6*) will evaluate the results provided in this chapter. Chapter 6 will evaluate each scenario, as well as each configuration. Critical questions regarding the sensitivity of the measurement method will also be raised.

Chapter 6

Evaluation

This chapter will evaluate how the four different scenarios were calculated and what may have been done differently. This chapter will also give an evaluation of the measurement method (the Multi-Metric method) and a recommendation of whether it is applicable for determining a Privacy Label, or not. The evaluation of the measurement method will be focusing on the method itself, as well as the measurement parameters provided.

In order to get a measurement result as precise as possible, we both need precise and representative scenarios. By representative we mean that all different scenarios cover both extreme privacy and no privacy, while still covering all scenarios in the middle. These scenarios are not likely to cover *all possibilities*, but should aim at being as generic and relatable as possible. A scenario will reflect the patterns in a group of people when using the products. The term "extreme privacy" is relative from product to product as the configurability may vary which then again for example will lower the possibilities for configuring sufficient privacy for some people. We therefore need to see the scenarios and SPD_{Goal} in accordance with the actual product. Still, we should have a general rule or guidance explaining what the SPD_{Goal} (S, 90, D) expects from the product. This would mean that an extreme privacy awareness for product A may have an SPD_{Goal} of (S, 90, D), while product B may have an extreme privacy awareness, i.e. an SPD_{Goal} of (S, 70, D), as the configurability has dropped drastically.

6.1 Evaluation of results and critical assessment

Below, an evaluation of the four scenarios describing different goals for privacy is presented, focusing on how well they are described, and discussing whether there should have been made any adjustments before applying the Multi-Metric method.

It is noticeable to see that the highest score of any configurations, is configuration B (85). Furthermore, configuration H (27) presents the lowest score. Comparing these two scores, we get a difference of 58. This number indicates that the overall system *Polar* offers considerable *configurability*.

After we applied the RMSWD function have been applied (explained in Equation 4.1), we have compared the results with each of the four different scenarios. By doing so, we have either receive a result tagged *passed*, *medium* or *fail*. These colors show what configuration is most suitable (green), second suitable (orange) and least suitable (red).

6.1.1 Evaluation: Scenario 1 (Extreme privacy awareness)

The SPD_{Goal} for scenario 1 (according to table 5.11) was set to SPD_{Goal}(S, 90, D) which is a quite high goal. "John", in this scenario, primarily aims at passing configuration A and B which are configured to fit this specific scenario. The results shows that it holds for both configurations A (81) and B (85), which pass, while configurations C (78) and D (74) ends up as a medium. The remaining fail.

As of this scenario, we were not able to meet the goal of 90. Our highest result is configuration B of 85. Looking at configuration B, the only way to upper the privacy score would be setting a *custom password* as a screen lock. Assuming that this were to be done, we would have received a result of *92*. This is a result even higher than the goal for "John". Our understanding of this is that it is possible to use the overall system such a way that almost 100% ensures the privacy of the user, but drastically drops the functionality of the system. In order to receive a result of 92, "John" is limited to only use the Polar M600 by itself as well as using the most secure way of locking the watch (by a custom password). This scenario might appeal to people wanting to monitor their training sessions or daily activity but is not in interest of synchronize this data to any devices. This may be because of privacy awareness or simply because it is not of interest.

When concluding the results provided for scenario 1, we may classify it as a *success* as both configurations A and B passed.

6.1.2 Evaluation: Scenario 2 (Medium privacy awareness)

Looking at scenario 2 (according to table 5.12), the goal was set to SPD_{Goal}(S, 80, D). "Kate" aims in this scenario primarily at passing configurations C (78) and D (74) are made to fit this specific scenario. Looking at the results, we can see that configurations A (81), B (85), C (78) and D (74) passes. The rest fail (E-H). This scenario have a SPD_{Goal} (80) quite close to scenario 1 (90), but ends up with twice as many configurations passing (4) compared to scenario 1 (2). This may indicate that scenario 2 is more representative for common people. Both configurations C and D opens for synchronization with Polar Flow, which lets "Kate" monitor her results via second device (smartphone, PC). Still, the privacy is maintained quite close to the SPD_{Goal} where D is the "worst" with its score of 74 (a difference of 6 from the SPD_{Goal}). This option is likely to be applicable to people when buying a smartwatch like Polar M600.

6.1.3 Evaluation: Scenario 3 (Regular privacy awareness)

The third scenario of "Nancy" (according to table 5.13) had an overall goal of SPD_{Goal}(S, 60, D). This scenario primarily aims at passing configurations

E (55) and F (45) are made to fit this specific scenario. After applying the method, we see that configuration E (55) passes, while configurations D (74) and F (45) get a medium result, and the rest fail. The fact that only one configuration passes (E) shows the impact of distributing sensitive data digitally. As for configuration F (which is customized to fit this scenario), "Nancy" regularly publishes activities in a public Polar Flow group. This configuration have a drastically impact on the overall result with its criticality value of 80 as well as a weight of 65. If we were to change this to the parameter "Joining (never publishes sessions)" (criticality value of 40), the configuration would have passed with a result of *51*. A conclusion of this scenario is that one need to be aware of disclosing such sensitive data in a public environment as it may have a considerable impact on the privacy.

6.1.4 Evaluation: Scenario 4 (No privacy awareness)

The results of scenario 4 (according to table 5.14) seem to be as expected, as both configurations G and H pass. "Alice" had an overall goal for this scenario of SPD_{Goal}(S, 30, D). This scenario primarily aims at passing configurations G (34) and H (27) as these they are made to fit this specific scenario. Both configurations G (34) and H (27) passes and may be considered representative to the scenario. These results shows that the overall system is offering a high level of *configurability* as "Alice" is able to configure her privacy all the way down to 27. Configuration F (45) receives a medium score while the remaining fail (A-E). The fact that the rest fail is as expected as scenario 4 fully discloses all sensitive data to the Polar Flow community. Still, we can see that configuration F (45) suffers from the choice of regularly publishing data to a public group and therefore receives a medium score with regard to scenario 4.

6.1.5 General evaluation of the different scenarios and parameters

One may argue that automatically accepting new followers should yield a similar criticality value as configuring "Privacy of activity summaries" to *Public* with "Privacy of profile" set to *Followers*. One way to solve this may be by introducing more parameters for the metrics *"Privacy of sessions"* and *"Privacy of profile"*. It would be interesting to include the parameter for setting a profile to *Followers* while having set the profile to automatically accepting new followers. This value should have fairly the same impact as setting the profile to public.

An argument for not introducing another parameter, however, may be because of the marketing or distribution exposure a profile will get by configuring it to *Public*. If a profile is set to *Public*, it will be made much more available to the Polar Flow community, as compared to a profile set to *Followers* only. We can prove this by looking at the Explore function, which will present the session results from every public profile. In order to locate a profile set to *Followers*, one would specifically need to look it up.

Based on this argument, one might say that such a result, as presented for configuration F with respect to scenario 4, will be sufficient.

6.2 Evaluation of the measurement method

In this thesis we have used the Multi-Metric method for assessing privacy. The Multi-Metric method is very generic and adaptable, which also makes it versatile when applied to any given system. It gives us a good birdseye view look on the overall system while also evaluating the system's core functionalities. Looking at the results produced by the method, it is possible to argue that these would *almost* be sufficient for classifying a Privacy Label. The reason for stating that these values are almost sufficient, is the lack of evaluation of the concepts of *configurability* and *transparency*. This needs to be evaluated, as well.

There have been proposed a way of measuring this (configurability and transparency), by introducing them as parameters for each components' metric. In order to do so, one should evaluate the criticality for the configurability and transparency of each component (between 0 and 100). This should then be done each components' metric where.

This thesis have discussed the possibility of measuring *configurability* based on the variations in the results provided by the RMSWD function (explained in Equation 4.1). Given a system that both have high results as well as low and the average of these is between 40 to 60, we can assume that the system offers high configurability and should thus be weighted in a positive direction when assigning a Privacy Label.

There have not been concluded which solution to work on (average vs configurability and transparency as parameters).

Another important aspect that should be considered when evaluating the method, is the need for creating a centralized database of values for criticality and weights. The method [16] clearly states that these values should be established by an expert within the field. A problematic issue with this method would appear if such a database was not to exist. If a set of ten people were to look at the criticality for, say the metric of for example *Bluetooth*, the likelihood of all the people calculating the same values is close to zero. This means that the results produced by the method would vary from person to person when applying it.

In order to escape this issue, a centralized database should be created by some public authority consisting of specialists in each of any given field (e.g. can a medical *doctor* provide valuable information when measuring cardiac data, and his knowledge may be needed in order to calculate a precise privacy value). This can be done in collaboration with public authorities (as for Norway may be authorities like *"Forbrukerrådet"*, *"Datatilsynet"*, etc.) which may assign key people within specific fields (e.g. a doctor may say that sharing cardiac related data to anyone is assigned a criticality value of 85) for determining criticality values. If such a database is established, the method would be of even more interest for calculating a Privacy Label.

6.2.1 Evaluation of the measurement parameters

When choosing parameters for a metric, the parameters should be as specific as possible in order to yield the best possible results. Upon introducing more parameters, the complexity of the method will grow quite drastically. By this means that when the size of the *metrics grow*, we would also need even more *configurations* in order to use all the different parameters provided. As for the measurement conducted in this thesis, we could have introduced a fourth parameter in the component metric "Groups" saying "Joining a closed group and regularly publishes sessions". By introducing such a parameter, we should have introduced this parameter as a third configuration for some of the scenarios. Given that we add such parameters, this will impact the complexity of the whole Multi-Metric method as we need even more configurations. The configurations provided for the measurement of the overall system *Polar* represent a sufficient amount of metrics and parameters as it covers the main functionalities as well as the most critical aspects of Polar Flow and Polar M600. The minimum parameters required for a metric is 2 (e.g. a component with the parameters On and Off). A sufficient measurement should not have fewer metrics than 4 as this is likely to cover most of the core functionalities of a system (e.g. Bluetooth, Synchronization settings, Screen lock, privacy settings for data that is synchronized). A satisfying measurement should include even more metrics than 4 as that would leave it more precise by covering more of the overall system.

Looking at the parameters that were included in this assessment, the goal was to make an overall evaluation of the systems. Polar Flow is quite a large and complex system that offers a varied functionality. To keep the level of complexity down, one would need to establish some general parameters. This would also be the case if such a method was to be used for measuring the privacy of a product. There would be a need to establish general parameters that apply to any given product within a specific field.

As of this assessment, we introduced 4 different metrics related to the watch itself, while introducing another 5 metrics for the Polar Flow web service and app. The watch metrics may be seen as more generic, as any smartwatch on the market to some extent will "have the same functionality". The functionality of a smartwatch may, of course, vary from one to another, but most of them aim to deliver basically the same functionality; that is, the monitoring of its user and the presentation of the information in a nice way. Many of these watches also offer a connection to a cloud where data can be stored and processed. This means that the user often will have two choices; Should the watch distribute data to the cloud, or, shall it retain data locally on the watch? We therefore included the metrics *Bluetooth* and *Wi-Fi*. Both parameters are generic and they drastically affect the privacy of the device when turned On, as compared to Off. Furthermore, we also included the possibility for setting a *Screen lock*. This is an essential parameter that ought to be included, as this may influence the weight or criticality of the Bluetooth and the Wi-Fi. However, if we assume that setting a screen lock is not possible, the smartwatch automatically becomes more exposed, even if both Wi-Fi and Bluetooth are turned off. As one last metric for the smartwatch, we included the possibility for configuring it to *Automatically syncing to app*. This would mean that the user will actually be able to have both Wi-Fi and Bluetooth turned on, while still manually synchronizing a training session to the app. If the user chooses to automatically synchronize data, we see that it impacts the privacy by *9%* (comparing the results of configuration B (85) and C (78)). We notice a change, but not that big. By leaving all the privacy settings to being private, the user is still in control of his own data. The only difference may be the insight he leaves for Polar to have. One element that deserves to be shortly addressed, is the fact that he has no control of when or where the data are being synchronized, meaning that he could be synchronizing data on the subway just as well as at home in his own kitchen. The risk of a synchronization in public environments will naturally affect the privacy issue more paramount. The thesis will, however, not cover this aspect.

Looking at the metrics provided for Polar Flow, the parameters need to be a little more specific, but are still applicable to other systems. Three of the metrics that were introduced maintain a close relation, namely *Privacy of profile*, *Privacy of sessions* and *Privacy of activity summaries*. All of these have the same three options available (*Public*, *Followers* and *Private*), but criticality and weight may differ slightly. Leaving a profile Public will expose the privacy quite a bit, as the basic information is open for anyone to watch. Given a scenario where the *privacy of a profile* is configured to Public, but the *privacy of sessions* and the *privacy of activity summaries* are configured to Private, a maliciously intended person is not necessarily able to collect that much information, just by the fact that the profile is Public. But this information may be exploited when using other services, too (e.g. Facebook). The thesis will not look beyond Polar Flow and Polar M600, but it is important to underline the value of this basic information alone, and, how it can expose the user. Assuming that all three parameters are configured to *Public*, the user exposes information that may be of great interest to a maliciously intended person. Given such a situation, the privacy of the profile/person may be considered as close to zero, even though the user has already consented. The two other metrics can also be applied to other systems. Looking at the *Confirm followers automatically* metric, we can expect that at least some basic information will be disclosed, in so far as up to sensitive information, such as the *activity summaries*. The last metric, *Groups*, may be a quite critical part if a user chooses to regularly publish his training sessions, as the information may be exposed to unfamiliar users. The reason for setting a *criticality of 50* for just joining a group is the power of distribution. Even upon just joining a group and acting as a spectator, the presence of a user may be exposed.

When looking back to the different criteria set for each privacy level in a Privacy Label (described in 3.5.2), we may classify each different configurations as follows:

- **Configuration A:** Label: A+ (The Polar M600 transmits no data, has a screenlock that makes any people "unavailable" to collect/get access to the data.)

- **Configuration B:** Label: A+ (The Polar M600 transmits no data, has a screenlock that makes any people "unavailable" to collect/get access to the data.)

- **Configuration C:** Label: A (The Polar M600 transmits data to Polar Flow, but these data are being stored securely and private so that the user are in full control of these.)

- **Configuration D:** Label: C (The Polar M600 transmits data to Polar Flow, but some of the users basic data may be abused as he chooses to join a public group as well as automatically confirming new followers.)

- **Configuration E:** Label: C (The Polar M600 transmits data to Polar Flow and give insight to training data by leaving his profile open to followers. By doing so, the user looses control over his data as any of the followers may abuse.)

- **Configuration F:** Label: C (The Polar M600 transmits data to Polar Flow and gives followers insight to his training data. Furthermore, he chooses to automatically confirm new followers which leaves him in a situation where "everyone" is able to collect and abuse his data. He also joins a group group which he regularly publishes data to, which exposes him even more.)

- **Configuration G:** Label: C (The Polar M600 transmits data to Polar Flow and gives everyone insight to his training data. He has no control of who may abuse his data as his profile is public. The fact that he joins a public group exposes his identity even more.)

- **Configuration H:** Label: C (The Polar M600 transmits data to Polar Flow and gives everyone insight to his training data. He has no control of who may abuse his data as his profile is public. He also joins a public group which he regularly publishes data to, leaving him even more vulnerable.)

These labels should be seen in relationship with each other as each of them represent slightly different ways of using the overall system (moving from extreme privacy awareness to no privacy awareness). Each result represents how the overall system may be configured and thus leaves the user in control of this. The reason for not assigning a higher level than A+ is the fact that the Polar M600 is able to transmit data, even though it is configured not to do so. Both configurations *A* and *B* are the ones receiving highest score (*A+*) which is because it stores all data locally in a safe manner without any transmission. When comparing this statement with regard to the results provided after applying the

Multi-Metric method, configurations A and B receives scores of 81 and 85. These results very much reflects a Privacy Label worthy an A+. It should be mentioned that these Privacy Labels have been assigned without considering either *Transparency* or *Configurability*. How this may be included in the measurement are presented in the conclusion in chapter 7.

In order to summarize the choices of parameters made, we can say that it is important to address specific, but also generic enough parameters, so that they can be applied to other systems, because we want to be able to use parameters and metrics of a more generic kind.

6.3 Sensitivity of the configurations

As pointed out earlier, the privacy values in the Multi-Metric method and the parameters should be set by an the expert within the field. The criticality for a parameter combined with the weight of the metric is important in order to get the correct result. This would also mean that the result, as such, could be quite sensitive. This sensitivity can vary from one system to another. Given the number of metrics, one single parameter will not necessarily have a large impact on the overall result. Given a system with fewer metrics, each parameter will result in a larger impact.

For this specific system, we can see that changing the criticality for one specific parameter will not necessarily cause a large impact to the result. A way to make the results more sensitive would be to introduce more specific parameters (as discussed in the evaluation of scenario 4). If we assume that a parameter named *"Followers with automatically accepting new followers"* is introduced for the *Privacy of profile* metric, *Privacy of sessions* metric and *Privacy of activity summaries* metric we would have a possibility for a larger impact. By introducing this parameter, we should give it a criticality value quite close to that of *Public*. The metrics can then be presented as follows:

Privacy of profile	$\mathbf{C_p}$
Public	75
Followers with automatically accepting new followers	70
Followers	40
Private	5
Weight	70

Table 6.1: M6 - Privacy of profile metric with extra parameter (*Followers with automatically accepting new followers*).

Privacy of sessions	$\mathbf{C_p}$
Public	80
Followers with automatically accepting new followers	75
Followers	45
Private	5
Weight	70

Table 6.2: M7 - Privacy of sessions metric with extra parameter (*Followers with automatically accepting new followers*).

Privacy of activity summaries	$\mathbf{C_p}$
Public	85
Followers with automatically accepting new followers	80
Followers	40
Private	5
Weight	70

Table 6.3: M8 - Privacy of activity summaries metric with extra parameter (*Followers with automatically accepting new followers*).

Introducing these metrics for scenario 4, we could receive a result as presented below.

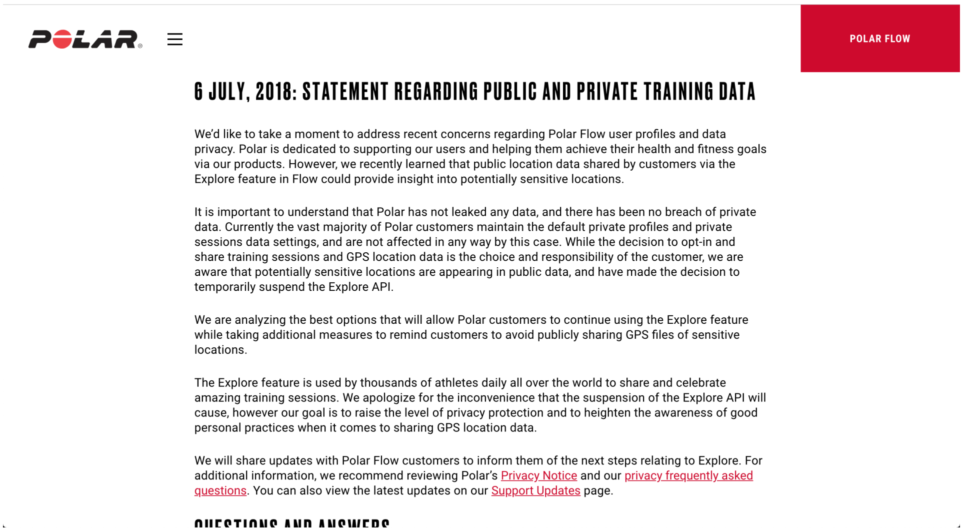
Criticality										$\mathbf{SPD_{System}}$	
	C1	C2	C3	C4	C5	C6	C7	C8	C9		
											Scenario 4
Metric	M1	M2	M3	M4	M5	M6	M7	M8	M9	Criticality	SPD(S, 30, D)
	P	P	P	P	P	P	P	P	P		
Conf. F	40	45	10	40	60	70	75	80	80	66	34

Table 6.4: Hypothetical $\mathrm{SPD_{System}}$ result given an extra parameter

Here, we have updated metrics 6, 7 and 8 with the parameter "Followers with automatically accepting new followers" and given it the criticality of the configuration "Public", minus 5 (which should be sufficient enough, given the lack of marketing or distribution of the profile). We can see that the result changes quite drastically from *45* to *34*. This is an indication of the sensitivity for each result and amplifies the importance of how the metrics are produced.

Another element that needs to be taken into consideration is the concept of *configurability* and *transparency*. Given a system that varies greatly in results, we might find indicated that the possibilities for a good configuration of its own privacy, is present. Given these possibilities, it logically follows that we should weight the overall system in a positive direction, assuming that the system by default configures all settings to private (which is the case for both Polar M600 and Polar Flow, as presented in Figure 3.6).

The concept of transparency also needs to be taken into consideration. Looking at this system, we can, to some extent, say that transparency is also taken into consideration. In the summer of 2018 (6 July, 2018), Polar Flow temporarily suspended the function "Explore" [36]. It was suspended due to the lack of clarity in their terms. As Polar stated: *"It is important to understand that Polar has not leaked any data, and there has been no breach of private data."* Furthermore, their statement told us that: *"While the decision to opt-in and share training sessions and GPS location data is the choice and responsibility of the customer, we are aware that potentially sensitive locations are appearing in public data, and have made the decision to temporarily suspend the Explore API."* Looking at this statement from a transparency point of view, one can argue that transparency is highly valued in Polar's overall system.



6 JULY, 2018: STATEMENT REGARDING PUBLIC AND PRIVATE TRAINING DATA

We'd like to take a moment to address recent concerns regarding Polar Flow user profiles and data privacy. Polar is dedicated to supporting our users and helping them achieve their health and fitness goals via our products. However, we recently learned that public location data shared by customers via the Explore feature in Flow could provide insight into potentially sensitive locations.

It is important to understand that Polar has not leaked any data, and there has been no breach of private data. Currently the vast majority of Polar customers maintain the default private profiles and private sessions data settings, and are not affected in any way by this case. While the decision to opt-in and share training sessions and GPS location data is the choice and responsibility of the customer, we are aware that potentially sensitive locations are appearing in public data, and have made the decision to temporarily suspend the Explore API.

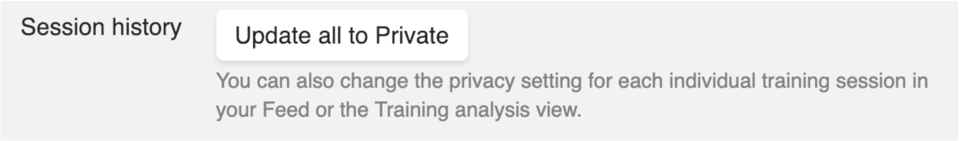
We are analyzing the best options that will allow Polar customers to continue using the Explore feature while taking additional measures to remind customers to avoid publicly sharing GPS files of sensitive locations.

The Explore feature is used by thousands of athletes daily all over the world to share and celebrate amazing training sessions. We apologize for the inconvenience that the suspension of the Explore API will cause, however our goal is to raise the level of privacy protection and to heighten the awareness of good personal practices when it comes to sharing GPS location data.

We will share updates with Polar Flow customers to inform them of the next steps relating to Explore. For additional information, we recommend reviewing Polar's Privacy Notice and our privacy frequently asked questions. You can also view the latest updates on our Support Updates page.

QUESTIONS AND ANSWERS

Figure 6.1: Polar Flow Privacy Statement after suspending Explore.



You can also change the privacy setting for each individual training session in your Feed or the Training analysis view.

Figure 6.2: Polar Flow: Update all data (including historical data) to private.

From our point of view, both of these concepts should be given a specific weight when determining a result.

6.4 Sensitivity of weights and parameters

There are three ways for validating the precision of the Multi-Metric method. One is to introduce even more specific parameters in order to make it as precise as possible, while another validation may be to test the sensitivity of weights and parameters. The third way may be to conduct the change on both criticality and weights. Below, we will present these *three* different tests.

6.4.1 Test 1: Sensitivity of weights

The first test focuses on increasing the weights by 20%. This would mean that the weights for each metric are presented as follow:

- **Bluetooth:** 12
- **Wi-Fi:** 30
- **Screen lock:** 48
- **Automatic sync to app:** 60
- **Confirming followers automatically:** 84
- **Privacy of profile:** 84
- **Privacy of sessions:** 84
- **Privacy of activity summaries:** 84
- **Groups:** 78

When introducing these updated weights, we end up with a result as follows, and as seen from *Scenario 1* (each column marked *blue* represents a change from the original result):

Criticality										**SPD$_{\text{System}}$**	
	C1	C2	C3	C4	C5	C6	C7	C8	C9		
											Scenario 1
Metric	M1	M2	M3	M4	M5	M6	M7	M8	M9	Criticality	SPD(S, 90, D)
	P	P	P	P	P	P	P	P	P		
Conf. A	5	5	25	-	-	-	-	-	-	19	81
Conf. B	5	5	20	-	-	-	-	-	-	15	85
Conf. C	40	45	20	50	5	5	5	5	5	21	79
Conf. D	40	45	10	50	5	5	5	5	40	25	74
Conf. E	40	45	70	50	5	40	45	50	40	44	56
Conf. F	40	45	20	50	75	40	45	50	80	55	45
Conf. G	40	45	20	50	75	75	80	85	40	67	34
Conf. H	40	45	70	50	75	75	80	85	80	74	26

Table 6.5: Hypothetical SPD$_{\text{System}}$ when increasing each weight by 20%. Blue indicates a change from the original result.

Metric	Criticality*	Criticality**	SPD$_{\text{System}}$*	SPD$_{\text{System}}$**
Conf. A	19	19	81	81
Conf. B	15	15	85	85
Conf. C	22	21	78	79
Conf. D	26	25	74	75
Conf. E	45	44	55	56
Conf. F	55	55	45	45
Conf. G	66	67	34	33
Conf. H	73	74	27	26

Table 6.6: Hypothetical SPD$_{\text{System}}$ compared to its original SPD$_{\text{System}}$ after increasing the weights by 20%. Blue indicates a change from the original result. **NOTE 1:** * = Original result. **NOTE 2:** ** = Increased weights by 20%.

As we will see from the result, there is not much of a change in the final result. 5 out of 8 configurations receive a change, but none of a significant change. All the configurations that changed (C, D,E, G and H) are to be considered as the "same" result as before increasing the weights by 20% as all of them changed either +1 or -1. This test shows that such a small change in the weights does not have any noticeable adjustments. However, it would have been interesting to see what impact an increase of 40% and 60% of the weights would have had on the final results. It turns out that by increasing the weights by 40% gives exactly the same result as the original result (no change). It is therefore not included a table for this. Below, there is presented a table after increasing the weights by 60%.

Metric	Criticality*	Criticality**	SPD$_{\text{System}}$*	SPD$_{\text{System}}$**
Conf. A	19	19	81	81
Conf. B	15	15	85	85
Conf. C	22	23	78	77
Conf. D	26	27	74	73
Conf. E	45	45	55	55
Conf. F	55	55	45	45
Conf. G	66	65	34	35
Conf. H	73	73	27	27

Table 6.7: Hypothetical SPD$_{\text{System}}$ compared to its original SPD$_{\text{System}}$ after increasing the weights by 60%. Blue indicates a change from the original result. **NOTE 1:** * = Original result. **NOTE 2:** ** = Increased weights by 60%.

After increasing the weights by 60%, we can almost see no change in the final results presented in table 6.7. It is noticeable to see that the configurations that change (C, D and G), only differs by 1. This result is to be considered as "same" as the original result. The fact that there is such small changes indicates that changing all the weights with a certain value evens out the change so that we in the end receive most of the same result as the original one. Furthermore, it is clear to see that these weights are meant to support the criticality values rather than influence the result by themself.

6.4.2 Test 2: Sensitivity of parameters criticality

The next test focuses only on changing the criticality values for each parameter. In this case, too, the criticality values are increased by 20% and thus look as follows:

Bluetooth	C_p
On	48
Off	6
Weight	10

Table 6.8: Hypothetical M1 - Bluetooth metric (criticality values increased by 20%).

Wi-Fi	C_p
On	54
Off	6
Weight	25

Table 6.9: Hypothetical M2 - Wi-Fi metric (criticality values increased by 20%).

Screen lock	C_p
Password	12
Pattern	30
PIN	24
No screen lock	84
Weight	40

Table 6.10: Hypothetical M3 - Screen lock metric (criticality values increased by 20%).

Automatic synchronization to app	C_p
On	60
Off	6
Weight	60

Table 6.11: Hypothetical M4 - Automatic synchronization metric (criticality values increased by 20%).

Confirm followers automatically	$\mathbf{C_p}$
On	90
Off	6
Weight	70

Table 6.12: Hypothetical M5 - Automatically confirm followers metric (criticality values increased by 20%).

Privacy of profile	$\mathbf{C_p}$
Public	90
Followers	48
Private	6
Weight	70

Table 6.13: Hypothetical M6 - Privacy of profile metric (criticality values increased by 20%).

Privacy of sessions	$\mathbf{C_p}$
Public	96
Followers	54
Private	6
Weight	70

Table 6.14: Hypothetical M7 - Privacy of sessions metric (criticality values increased by 20%).

Privacy of activity summaries	$\mathbf{C_p}$
Public	100
Followers	60
Private	6
Weight	80

Table 6.15: Hypothetical M8 - Privacy of activity summaries metric (criticality values increased by 20%).

Groups	$\mathbf{C_p}$
Public	96
Followers	48
Private	6
Weight	65

Table 6.16: Hypothetical M9 - Groups metric (criticality values increased by 20%).

When applying the Multi-Metric method with these updated criticality values, we get a result as follows:

Criticality										**$\text{SPD}_{\text{System}}$**	
	C1	C2	C3	C4	C5	C6	C7	C8	C9		
											Scenario 1
Metric	M1	M2	M3	M4	M5	M6	M7	M8	M9	Criticality	SPD(S, 90, D)
	P	P	P	P	P	P	P	P	P		
Conf. A	6	6	30	-	-	-	-	-	-	22	78
Conf. B	6	6	24	-	-	-	-	-	-	18	82
Conf. C	48	54	24	60	6	6	6	6	6	27	73
Conf. D	48	54	12	60	6	6	6	6	48	31	69
Conf. E	48	54	84	60	6	48	54	60	48	53	47
Conf. F	48	54	24	60	90	48	54	60	96	66	34
Conf. G	48	54	24	60	90	90	96	100	48	79	21
Conf. H	48	54	84	60	90	90	96	100	96	88	12

Table 6.17: Hypothetical $\text{SPD}_{\text{System}}$ when increasing each parameter's criticality value by 20%. Blue indicates a change from the original result.

Metric	**Criticality***	**Criticality****	**$\text{SPD}_{\text{System}}$***	**$\text{SPD}_{\text{System}}$****
Conf. A	19	22	81	78
Conf. B	15	18	85	82
Conf. C	22	27	78	73
Conf. D	26	31	74	69
Conf. E	45	53	55	47
Conf. F	55	66	45	34
Conf. G	66	79	34	21
Conf. H	73	88	27	12

Table 6.18: Hypothetical $\text{SPD}_{\text{System}}$ compared to its original $\text{SPD}_{\text{System}}$. Blue indicates a change from the original result. **NOTE 1:** * = Original result. **NOTE 2:** ** = Increased criticality values by 20%.

When increasing each parameter's criticality value by 20%, we see a clear change. Each and every configuration increases its criticality, which clearly states that the Multi-Metric method is quite sensitive to the criticality value. Based on the information given by these two tests, we can say that each metric is more dependent on a precise criticality value than on a precise weight.

Looking at the configurations, we notably observe that the ones with lowest criticality (configurations A (19) and B (15)) have the same order of magnitude, 3. As for the rest of the rest, it slowly but surely grow towards a final increase of 20% (configuration H with its criticality of 88). The more critical configurations change even more as the criticality is increased. This is, tome some extent, to be expected.

6.4.3 Test 3: The sensitivity of the parameters criticality and weights

As a third and final test, we have joined tests 1 and 2 in order to see what impact there is when both criticality and weights are increased by 20%. The results are as follows:

Criticality										**SPD$_{\text{System}}$**	
	C1	C2	C3	C4	C5	C6	C7	C8	C9		
											Scenario 1
Metric	M1	M2	M3	M4	M5	M6	M7	M8	M9	Criticality	SPD(S, 90, D)
	P	P	P	P	P	P	P	P	P		
Conf. A	6	6	30	-	-	-	-	-	-	21	79
Conf. B	6	6	24	-	-	-	-	-	-	18	82
Conf. C	48	54	24	60	6	6	6	6	6	25	75
Conf. D	48	54	12	60	6	6	6	6	48	30	70
Conf. E	48	54	84	60	6	48	54	60	48	53	47
Conf. F	48	54	24	60	90	48	54	60	96	66	34
Conf. G	48	54	24	60	90	90	96	100	48	79	21
Conf. H	48	54	84	60	90	90	96	100	96	88	12

Table 6.19: Hypothetical SPD$_{\text{System}}$ when increasing each parameter's criticality value and weights by 20%. Blue indicates a change from the original result.

Metric	**Criticality$_{*}$**	**Criticality$_{**}$**	**SPD$_{\text{System*}}$**	**SPD$_{\text{System**}}$**
Conf. A	19	21	81	79
Conf. B	15	18	85	82
Conf. C	22	25	78	75
Conf. D	26	30	74	70
Conf. E	45	53	55	47
Conf. F	55	66	45	34
Conf. G	66	79	34	21
Conf. H	73	88	27	12

Table 6.20: Hypothetical SPD$_{\text{System}}$ compared to its original SPD$_{\text{System}}$. Blue indicates a change from the original result. **NOTE 1:** * = Original result. **NOTE 2:** ** = Increased criticality values **and** weights by 20%.

When combining tests 1 and 2, we see that the criticality and SPD$_{\text{System}}$ values are quite stable as in accordance with test 2. This adds up to the fact that weights have a relatively small impact on the overall score compared to the criticality values. Still, one can argue that the function is more stable when applying growth to both criticality and weights.

6.5 Summary

This chapter has evaluated the measurement results from chapter 5. These results are an outcome of the Multi-Metric method after having applied it on the overall system, Polar, with its subsystems Polar Flow and Polar M600.

There was carried out an evaluation of each scenario. This evaluation showed that at least one each scenarios belonging configuration passed. This taught us that the overall system is as stable and robust as we would expected it to be before we conducted the measurements.

This chapter is a contribution to Q4 (*"Recommendations for measurable privacy?"*) and pointed out the following:

- The outcome of this chapter is the importance of good and precise criticality values. Section 6.3 shows the sensitivity of both weights and criticality, and it clearly states that the method favours criticality values. This section also shows that changing the weights with a common value "evens out" the change and for most of the configurations ends up with no change. There have been conducted three tests where the weights have been increased (20%, 40% and 60%). When increasing the criticality values by 20%, we notice that there is slightly more of a change. For the configurations with low criticality (like configurations A (19) and B (15)), we notice a change in the criticality only increases by 3. Furthermore, we notably observe that the criticality increases slowly but steady, ending up at a 20% change (configuration H, was 73, now 88).

  It is recommended that there should be created general, but specific enough, privacy values so that they are sufficient for any system to use. One challenge may be finding the correct relation for the privacy values. It may be hard to create them specific enough, and yet, still generic enough for our purposes.

Next chapter (*chapter 7*) is the final chapter of the thesis and constitutes the last section, as well (*Conclusions*). Chapter 7 will present what each chapter has contributed with regard to the research questions stated at the beginning of the thesis (section 1.3). A conclusion for whether the Multi-Metric method is applicable for determining a Privacy Label will also be delivered. As a wrap up, any remaining open issues, as well as future work that will be presented.

Part III

Conclusions

Chapter 7

Conclusion

This thesis has covered the field of privacy issues related to IoT, and addressed problems regarding measurable privacy. The overall goal was to validate or invalidate a measurement method for determining a Privacy Label [43] so that it is possible to use the method on general terms for IoT products. We presented different possible methods that might apply to this project, but this thesis focused on the Multi-Metric method [16] with respect to Privacy Labeling.

The thesis has followed the *engineering design method* [42] and is based on the following 4 research questions:

- **Q1. What challenges relate to privacy using IoT devices?**
- **Q2. What methods can be used to assess privacy?**
- **Q3. What are the challenges when applying measurable privacy?**
- **Q4. Recommendations for measurable privacy?**

Chapter 2 answered the research question Q1 by pointing out the worldwide rise of IoT, and what challenges with respect to privacy (e.g. user profiling) this may have introduced. The fact that IoT is introduced into ever more domains makes each persons privacy increasingly more challenged, as more people will share even more sensitive data. This may include health related data which before IoT were quite hard for maliciously intended people to access. As for now, such information is getting more threatened, as it is available in the digital world where it previously was accessible only inside a locked cupboard in the doctor's office.

Chapter 3 answered research question Q2 by pointing out that the desired method for measuring privacy would need to address general terms when coming to the specification of parameters to evaluate. The reason for this is the fact that each system can have quite specific parameters (the data that are collected), but these data need to be translated into a more general term. The chosen method for this thesis is the Multi-Metric method that seems to satisfy all the different requirements.

Chapter 4 answered the research question Q3 by pointing out the need for a centralized database for privacy values. The reason for doing so is to exclude the large variations that may appear between "experts" when calculating these privacy values. Furthermore, the chapter addressed the necessity of considering both *transparency* and *configurability* when assessing each system. It is therefore proposed that an average result somewhere between 40 to 60 and should be weighted in a positive way. There is also mentioned an issue related to this. The issue occurs when a system is incapable of presenting sufficient configurability and transparency. Given such a system, we would expect all the results to be quite close to each other as the user is unable to configure the privacy himself. This may be a system that is either extreme privacy aware and doesn't open for sharing data for example. One should then expect to mostly get high results. As for this kind of system, the lack of configurability should be weighted in a negative way. The chapter also addresses an issue that may occur when a system only receives results close to each other in the middle of the scale (e.g. 50, 54, 49, 52, etc.). This would indicate lack of configurability and transparency as well. How this is handled needs to be clarified before moving forward with the Multi-Metric method in order to measure privacy.

Chapter 5 answered research question Q4 by pointing out the importance of good and precise privacy values. The reason for stating this is the sensitivity of each privacy value, especially the criticality values. This chapter completed the evaluation of the overall system *Polar* and its subsystems *Polar M600* and *Polar Flow* by applying the Multi-Metric method. It turns out that the method is quite stable when looking at weight and criticality together (assuming that the relationship between the two is reasonable). Just looking at the criticality, we saw that the result was affected in a larger manner, relative to adjusting the weight by the same amount.

In order to give a product a Privacy Label, we will want to look closely at each layer, as well as at the overall system. As an outcome of applying the Multi-Metric method on the overall system *Polar* with its subsystems *Polar M600* and *Polar Flow*, we see that it receives an average score of *60*. With an average score of 60, the product obtains a *medium plus* score. Assuming that this average score reflects scores peaking both high and low (for example results varying from 30 to 90), we may sense that the system offers high configurability and transparency. If that's the case, this tells us that the user is both able to configure his profile to be highly privacy aware, as well as to being suitable to the a user with no privacy awareness. The conclusion will then be that an average score somewhere in the middle between 40 to 60 with large variations in the results (from high to low), should rather be awarded a top score, assuming that the product is highly configurable.

Another way of solving the issue related to configurability and transparency has been presented by introducing them as parameters for each components metric. This may be done in exactly the same way as for weighting each metric. By doing so, we are able to calculate a criticality value from 0 to 100, specifying how transparent or configurable the current component may be. If this is done, calculating the average score would most likely reflect the level of configurability and transparency even more.

There was provided an overview of suggested Privacy Labels for each configuration provided for the Use-Case scenario (presented in section 6.2.1). These configurations receives labels from *A++* to *E*. As for label A++, this is given to both configurations *A* and *B* as they does not transmit any data as well as securing the watch itself by a PIN code, leaving it protected against a physical attack. Looking at configuration *H*, it receives the label *E*. The reason for this, is the fact that data is transmitted to Polar Flow and disclosed for everyone to see in the Polar Flow community. As of this, he is unable to keep track of who may look into his data and potentially abuse them.

These Privacy Labels for each configurations should be evaluated together in order to give an overview of how the *overall system* may process a users data. If we were to presented a label for the measured system (*Polar* with the subsystems *Polar Flow* and *Polar M600*), we may assign a label of *A+* as it is able to offer a high level of privacy (if configured with privacy in mind). Another argument for such a high label is the *configurability* and *transparency* in the system. As we are given the opportunity to configure the system to either being A++ or C compliant, this should be taken into consideration when assign the label. The presence of configurability is also reproduced after applying the Multi-Metric method as we have seen the scores varying from *81* and *27*. The reason for not giving a higher label than A+ is the fact that a user may transmit data if desired. By referring back to the proposed regulation for label A+, we read the following (in section 3.5.2: *"Data is stored securely. May allow for transmission, but in a way that makes it close to 100% safe."* This statement very much adds up to what we maximum are able to configure the overall system to. This is also the default configuration when configuring the system for the first time.

The outcome of the thesis was to determine how a Privacy Label could be measured on general terms in order to be applicable for any product on the market. This thesis therefore aimed to validate a measurement method for determining this. The Multi-Metric method offers a clear and precise evaluation of the parameters given to the function, both from a birdseye perspective and for the single component's point of view. The method has shown that it is robust and reliable on a large and commercialized scale, but may be more unreliable on a smaller scale. This may be because of the privacy values chosen. The thesis suggests that a centralized database should be created, where such privacy values are stored. These values should be set by experts within each domain or field.

7.1 Open issues and future work

This thesis has carried out a careful examination of the Multi-Metric method to see whether it is capable for determining a Privacy Label. This work alone can, however, not lay the foundations for determining which measurement method should be used for calculating a Privacy Label. This method should be further tested on other products, as well, in order to have more knowledge when determining what method to choose, or not. It may be interesting to have a closer look on the work provided by Srivastava et al. [47] on creating a *"Privacy Quotient"*, which may also have a potential for determining a Privacy Label. This is a totally different way of looking at the privacy measurement, as it focuses slightly more on the user than on the product itself. Still, the use of such a Privacy Quotient could have been completed in a similar manner, as the average result from the Multi-Metric method shows.

Assuming that future work will focus on further development and tests of the Multi-Metric method, it is important to look deeper into the work of creating a centralized database for storing privacy values. Such a work should be done in conjunction with public authorities (as for Norway may be "Forbrukerrådet", "Datatilsynet", etc.), as well as experts from each relevant field, related to the specific task (e.g. heart rate data might require a medical doctor). There should also be conducted more work related to how *configurability* and *transparency* should be weighted. As of now, we are able to evaluate this by looking at all the results provided from the method together, but this may not be sufficient enough when applying the method on a general basis. The possibility of introducing configurability and transparency as weights should be considered when continuing working on this.

As further testing and fine-tuning of a privacy measurement method goes on, the definition of each level within a Privacy Label may also be clarified even more, as well as how many levels there should be. Current proposals for the different layers have been presented in section 3.5.2, but given todays proposed range from A++ to F, this might be too big.

Bibliography

[1] *Alzheimer description*. Accessed: 2018-03-21. URL: https://www.alz.org/alzheimers_disease_what_is_alzheimers.asp.

[2] *Android Storage*. Accessed: 2018-02-28. URL: https://developer.android.com/guide/topics/data/data-storage.html.

[3] *Android Wear*. Accessed: 2018-02-08. URL: https://developer.android.com/wear/index.html.

[4] *Android Wear General*. Accessed: 2018-04-11. URL: https://wearos.google.com/.

[5] *Angela Merkel - Wiretapping*. Accessed: 2019-04-05. URL: https://www.telegraph.co.uk/news/worldnews/europe/germany/10407282/Barack-Obama-approved-tapping-Angela-Merkels-phone-3-years-ago.html.

[6] Adam J Aviv and John T Davin. "Towards Baselines for Shoulder Surfing on Mobile Authentication". In: (2017). DOI: 10.1145/3134600.3134609. arXiv: arXiv:1709.04959v2.

[7] *BB26.G*. Accessed: 2019-02-28. URL: https://its-wiki.no/wiki/SCOTT:BB26.G.

[8] *Business Indiser - Farmer IoT*. Accessed: 2018-03-16. URL: http://www.businessinsider.com/internet-of-things-smart-agriculture-2016-10?r=US&IR=T&IR=Tcom/.

[9] Beauty Close. "Research and Markets Adds Report : $ 20 . 6 Billion Global IoT in Manufacturing Market". In: (2018), pp. 1–3.

[10] *Confidentiality description*. Accessed: 2018-10-24. URL: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA.

[11] Frederick Davis and Copyright Information. "What do we mean by "Right to Privacy?"" In: 1 (1959).

[12] Soma Shekara Sreenadh Reddy Depuru, Lingfeng Wang, and Vijay Devabhaktuni. "Smart meters for power grid: Challenges, issues, advantages and status". In: *Renewable and Sustainable Energy Reviews* 15.6 (2011), pp. 2736–2742. ISSN: 13640321. DOI: 10.1016/j.rser.2011.02.039. URL: http://dx.doi.org/10.1016/j.rser.2011.02.039.

[13] Quang Do, Ben Martini, and Kim Kwang Raymond Choo. "Is the data on your wearable device secure? An Android Wear smartwatch case study". In: *Software - Practice and Experience* 47.3 (2017), pp. 391–403. ISSN: 1097024X. DOI: 10.1002/spe.2414.

[14] *ePrivacy Regulation*. Accessed: 2018-10-18. URL: https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.

[15] Eyelink. "User Manual". In: June (2006). ISSN: 0028-0836. DOI: 10.1007/SpringerReference_28001. arXiv: arXiv:1011.1669v3.

[16] Iñaki Garitano, Seraj Fayyad, and Josef Noll. "Multi-Metrics Approach for Security, Privacy and Dependability in Embedded Systems". In: *Wireless Personal Communications* 81.4 (2015), pp. 1359–1376. ISSN: 1572834X. DOI: 10.1007/s11277-015-2478-z.

[17] *GDPR EU*. Accessed: 2018-10-18. URL: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

[18] J Hartmanis and J Van Leeuwen. *Lecture Notes in Computer Science*. ISBN: 3540426140.

[19] Mike Hogan, Piccarreta, and Benjamin M. "Draft NISTIR 8200, Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)". In: (2018), p. 187. URL: https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf.

[20] *Honeywell - IoT Institute*. Accessed: 2018-03-20. URL: http://www.ioti.com/transportation-and-logistics/using-edge-computing-honeywell-making-helicopters-safer.

[21] *IoT - Convenience*. Accessed: 2019-04-11. URL: https://csnews.com/iot-becoming-increasingly-important-convenience-fuel-retailers.

[22] *IoT Standardization Review*. Accessed: 2018-08-2. URL: https://gcn.com/articles/2018/02/15/nist-iot-standards.aspx.

[23] *IoT Statistics from 2009 to 2020*. Accessed: 2019-02-28. URL: https://www.statista.com/statistics/764026/number-of-iot-devices-in-use-worldwide/.

[24] *IoTSec Consortium November 2017*. Accessed: 2019-04-11. URL: https://its-wiki.no/wiki/IoTSec:Consortium_Nov.2017.

[25] Patrick Gage Kelley. "Designing a Privacy Label : Assisting Consumer Understanding of Online Privacy Practices". In: (2009), pp. 3347–3352.

[26] Patrick Gage Kelley et al. "A " Nutrition Label " for Privacy". In: 1990 (2009).

[27] Masaaki Kurosu. "Human-computer interaction users and contexts: 17th international conference, HCI international 2015 Los Angeles, CA, USA, August 2-7, 2015 proceedings, Part III". In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9171 (2015), pp. 537–548. ISSN: 16113349. DOI: 10.1007/978-3-319-21006-3.

[28] P. A. Laplante and N. Laplante. "The Internet of Things in Healthcare: Potential Applications and Challenges". In: *IT Professional* 18.3 (May 2016), pp. 2–4. ISSN: 1520-9202. DOI: 10.1109/MITP.2016.42.

[29] Renju Liu and Felix Xiaozhu Lin. "Understanding the Characteristics of Android Wear OS". In: MobiSys '16 (2016), pp. 151–164. DOI: 10.1145/2906388.2906398. URL: http://doi.acm.org/10.1145/2906388.2906398.

[30] Pawel Nowodzinski, Katarzyna Łukasik, and Agnieszka Puto. "Internet Of Things (Iot) In A Retail Environment. The New Strategy For Firm's Development". In: *European Scientific Journal, ESJ* 12.10 (2016), pp. 332–341. ISSN: 1857 - 7431.

[31] *Number of IoT devices per person 2015-2025*. Accessed: 2018-08-2. URL: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

[32] Nathaniel Persily and Nathaniel Persily. "The 2016 U . S . Election : Can Democracy Survive the Internet ? Can Democracy Survive the Internet ?" In: 28.2 (2019), pp. 63–76.

[33] *Polar Flow*. Accessed: 2018-03-13. URL: https://flow.polar.com/.

[34] *Polar Flow Explore Privacy Statement*. Accessed: 2018-09-20. URL: https://www.polar.com/en/legal/privacy-notice.

[35] *Polar Flow Explore Privacy Statement Extraordinary*. Accessed: 2018-08-22. URL: https://www.polar.com/en/legal/faq/public_and_private_training_data_statement.

[36] *Polar Flow Privacy Statement*. Accessed: 2019-01-31. URL: https://www.polar.com/en/legal/faq/public_and_private_training_data_statement.

[37] *Polar M600 user manual*. Accessed: 2018-02-28. URL: https://support.polar.com/e_manuals/M600/wear-os/polar-m600-user-manual-english/manual.pdf.

[38] *Privacy definition*. Accessed: 2018-10-25. URL: https://dictionary.cambridge.org/dictionary/english/privacy.

[39] *Privacy Labeling for the users*. Accessed: 2018-10-17. URL: https://its-wiki.no/wiki/SCOTT:BB26.G#Privacy_Labelling_for_the_Users.

[40] *Privacy Labels Explained*. Accessed: 2018-04-04. URL: https://its-wiki.no/wiki/IoTSec:Privacy_Label_explanation.

[41] Lee Law Review and Alan F Westin. "Privacy And Freedom". In: 25.1 (1968).

[42] *Science method - Engineering method*. Accessed: 2019-03-27. URL: https://www.sciencebuddies.org/science-fair-projects/engineering-design-process/engineering-design-process-steps.

[43] *SCOTT*. Accessed: 2019-03-20. URL: https://its-wiki.no/wiki/SCOTT:SCOTT.

[44] *Security by design*. Accessed: 2018-08-2. URL: https://www.owasp.org/index.php/Security_by_Design_Principles.

[45] *Smartphones Worldwide*. Accessed: 2018-02-28. URL: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

[46] *Smartwatch unit sales worldwide from 2014 to 2018 (in millions)*. Accessed: 2018-02-07. URL: https://www.statista.com/statistics/538237/global-smartwatch-unit-sales/.

[47] Agrima Srivastava. "Measuring Privacy Leaks in Online Social Networks". In: *2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (2013), pp. 2095–2100. DOI: 10.1109/ICACCI.2013.6637504.

[48] *Technical Specification - Polar M600*. Accessed: 2018-02-07. URL: https://support.polar.com/e_manuals/M600/Polar_M600_user_manual_English/Content/technical-specifications.htm.

[49] *The word data: Singular or plural*. Accessed: 2019-04-26. URL: https://www.theguardian.com/news/datablog/2010/jul/16/data-plural-singular.

[50] *Transparency definition*. Accessed: 2018-11-01. URL: https://dictionary.cambridge.org/dictionary/english/transparency.