Privacy labels 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

Privacy labels for IoT consumer products

Christoffer Ramsvig Thambirajah

© 2019 Christoffer Ramsvig Thambirajah

Privacy labels for IoT consumer products

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

Printed: Reprosentralen, University of Oslo

Abstract

In recent time, personal privacy have come to peoples attention as we are digitally connected to each other more and more. The development of new mobile products connected to the Internet are starting to take a larger spot in people's everyday-lives. All of these products goes by the term *"Internet of Things" (IoT)* and are now starting to concern people when it comes to privacy. There have been introduced regulations from EU like General Data Protection (GDPR), trying to make companies more responsible when processing sensitive data. Still, there are privacy concerns in normal peoples everyday-life. Most of these concerns comes by the fact that people do not have enough insight/knowledge of how their data is being treated within these IoT products. This may be how the data is distributed, stored and used by the company that created the product. There is in other words a need of presenting this technical information in a more understandable and precise manner. Even if people doesn't ask for a solution to this problem, it is shown earlier that a simple and understandable approach for this type of technical information is valuable for people when it comes to choice of product. By presenting information that previously was unavailable to people in a more understandable way puts the consumer in charge of choosing how his/her private data should be treated.

This thesis investigates possible ways to measure privacy in a generic way so that this measurement can be used in presenting the privacy of each product within IoT to the end-customer. It also addresses a possible way of presenting this information to the end customer.

Another important part of the thesis is analyzing a actual product within IoT. Such an analysis delivers valuable information when it comes to mapping all the different technical parameters as well testing out measurement methods.

Furthermore, the thesis proposes a measurement method that is applicable for measuring privacy in a generic way as well as improvements/requirements for using this method on a international scale. Hopefully, the thesis is a contribution for the research within IoT & privacy and how this may be presented in a best possible way for the end-customer.

Acknowledgements

Contents

I Introduction **1**

1 Introduction **3**
1.1 Motivation 3
1.2 Problem Statement 4
1.3 Method of the thesis 5
1.3.1 Possible measurement method for the thesis 7
1.3.2 Choice of measurement method 8
1.4 Related work 9
1.5 Summary 10

2 Background **11**
2.1 Impact of Internet of Things (IoT) in specific domains 11
2.2 Security affecting Privacy 13
2.2.1 Self-awareness 14
2.2.2 Security by Design (SbD) 14
2.2.3 Security standards 16
2.2.4 Privacy by Design (PbD) 16
2.3 Introduction to Privacy Labels 17
2.4 Summary 19

3 Privacy in health-monitoring **21**
3.1 High level functional aspects 21
3.2 Use case: Polar M600 22
3.3 Functional architecture 22
3.3.1 Polar M600 - technical features 23
3.4 Technology details Polar M600 23
3.4.1 Android Wear/Wear OS by Google 25
3.4.2 Android Wear: Security and privacy aspects 26
3.4.3 Polar Flow 26
3.4.4 Polar Flow: Security and privacy aspects 28
3.5 Technological challenges: Polar M600 29
3.5.1 Privacy and measurability of privacy 29
3.5.2 What does privacy numbers mean? 29
3.6 Evaluation of the data 30
3.6.1 Measurability of privacy 30
3.6.2 The four main elements for measuring privacy 32
3.6.3 Controlled collection 33

3.7 Summary 34

4 Assesment methodology for privacy **37**
4.1 Translation from technical parameters 37
4.1.1 Multi-metric approach explained 37
4.1.2 Evaluation of the methodology 38
4.1.3 Variation and limitations 39
4.2 Key points to determine a privacy label 39
4.2.1 Privacy label seen from a user perspective 40
4.2.2 Privacy label seen from a vendor perspective 40
4.3 Two different privacy aspects to evaluate 41
4.3.1 Transparency 41
4.3.2 Configurability 42
4.4 Summary 42

II Use scenario **45**

5 Applying the Multi-Metric method **47**
5.1 Description of the different subsystems 47
5.2 Scenarios 48
5.2.1 Scenario 1 - Extreme privacy awareness 48
5.2.2 Scenario 2 - Medium privacy awareness 48
5.2.3 Scenario 3 - Regular privacy awareness 49
5.2.4 Scenario 4 - No privacy awareness 49
5.3 Device configurations 50
5.4 Metrics for privacy evaluation 51
5.4.1 Bluetooth 51
5.4.2 Wi-Fi 52
5.4.3 Screen lock 52
5.4.4 Automatically synchronization 53
5.4.5 Automatically confirmation of new followers 54
5.4.6 Privacy of profile 55
5.4.7 Privacy of sessions 56
5.4.8 Privacy of activity summaries 57
5.4.9 Groups 58
5.5 Privacy assesment results 60
5.5.1 Result - Scenario 1 60
5.5.2 Result - Scenario 2 61
5.5.3 Result - Scenario 3 61
5.5.4 Result - Scenario 4 62
5.6 Evaluation of results and critical assessment 62
5.6.1 Evaluation - Scenario 1 (according to table 5.10) . . . 62
5.6.2 Evaluation - Scenario 2 (according to table 5.11) . . . 63
5.6.3 Evaluation - Scenario 3 (according to table 5.12) . . . 63
5.6.4 Evaluation - Scenario 4 (according to table 5.13) . . . 64
5.6.5 Evaluation of the measurement method 64
5.6.6 Evaluation of the parameters 65

- Extreme privacy

6. Eval…

which parameters

5.7 Sensitivity of configurations 66
5.8 Sensitivity of weights and parameters 69
5.8.1 Test 1 - Sensitivity of weights 69
5.8.2 Test 2 - Sensitivity of parameters criticality 71
5.8.3 Test 3 - Sensitivity of parameters criticality and weights 73
5.9 Summary 74

III Discussion & conclusion Conclusions **77**

6 Discussion %delete **79**
6.1 Chapter 1 79

7 Conclusion **81**
7.1 Open issues & future work 82

List of Figures

2.1 European Energy Label 18

3.1 Polar M600 22
3.2 Polar M600 Features 24
3.3 Wear OS by Google 25
3.4 Polar Flow 27
3.5 Polar Flow Explore 28
3.6 Polar Flow Privacy Settings 34

4.1 Multi-metric method visualized 38

5.1 Polar Flow before being following 54
5.2 Polar Flow after being following 55
5.3 Configuring privacy for automatically confirming new followers 55
5.4 Configuring privacy of profile 56
5.5 Configuring privacy of sessions 57
5.6 Configuring privacy of activity summaries 57
5.7 Presenting how a public group look like 59
5.8 Privacy settings when creating a group 59
5.9 Polar Flow Privacy Statement after suspending Explore . . . 69
5.10 Function introduced that lets each user update all data (including historical data) to private 69

List of Tables

1.1 Sensitivity values for calculating the Privacy Quotient 7
1.2 Example of table showing users Privacy Quotient after a completed survey [44] 8

3.1 Technical specifications - Polar M600 23

5.1 M1 - Bluetooth metric 52
5.2 M2 - Wi-Fi metric 52
5.3 M3 - Screen lock metric 53
5.4 M4 - Automatically synchronization metric 54
5.5 M5 - Automatically confirm followers metric 55
5.6 M6 - Privacy of profile metric 56
5.7 M7 - Privacy of sessions metric 57
5.8 M8 - Privacy of activity summaries metric 58
5.9 M9 - Groups metric 59
5.10 SPD_{System} for Scenario 1 61
5.11 SPD_{System} for Scenario 2 61
5.12 SPD_{System} for Scenario 3 62
5.13 SPD_{System} for Scenario 4 62
5.14 M6 - Privacy of profile metric with extra parameter (*Followers with automatically accepting new followers*) 67
5.15 M7 - Privacy of sessions metric with extra parameter (*Followers with automatically accepting new followers*) 67
5.16 M8 - Privacy of activity summaries metric with extra parameter (*Followers with automatically accepting new followers*) . . . 67
5.17 Hypothetical SPD_{System} result given an extra parameter . . . 68
5.18 Hypothetical SPD_{System} when increasing each weight by 20%. 70
5.19 Hypothetical M1 - Bluetooth metric (increased by 20%) . . . 71
5.20 Hypothetical M2 - Wi-Fi metric (increased by 20%) 71
5.21 Hypothetical M3 - Screen lock metric (increased by 20%) . . 71
5.22 Hypothetical M4 - Automatically synchronization metric (increased by 20%) 71
5.23 Hypothetical M5 - Automatically confirm followers metric (increased by 20%) 71
5.24 Hypothetical M6 - Privacy of profile metric (increased by 20%) 72
5.25 Hypothetical M7 - Privacy of sessions metric (increased by 20%) 72

5.26 Hypothetical M8 - Privacy of activity summaries metric (increased by 20%) 72
5.27 Hypothetical M9 - Groups metric (increased by 20%) 72
5.28 Hypothetical SPD_{System} when increasing each parameters criticality value by 20%. 73
5.29 Hypothetical SPD_{System} when increasing each parameters criticality value and weights by 20%. 74

Part I

Introduction

Chapter 1

Introduction

1.1 Motivation

I was motivated to write this thesis, because my understanding is that the privacy and security within the IoT community is not taken into consideration when products are released to the consumer marked. Does people actually take their privacy into consideration when they are purchasing a new smartwatch? Or are they just looking at its functionality and what it is capable of doing?

As the world is moving forward and is becoming more digital, it is important to look at how our privacy is on the internet. The consumers are frequently asking for better functionality from the tech market, which then again pushes the companies to come 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 things, why would anyone bother making them?

Because of the exponential growth within the IoT market, my understanding is that the consumer mostly values functionality over privacy. This trend triggers me and makes me wonder how this can be solved in the best way. One way could have been to simply set a rule and classification to each and every IoT product that is being released in the maket. Doing that would definitely have made the companies aware of the privacy and most likely made them implement the security that is needed in order to fulfill the needs. By doing so, one would mostly set limitations for the growth of new products. This may be because IoT products often aims to solve one exact problem. As this would slow down the development of such products, one should rather look at other possibilities in order to solve this issue.

Another way of forcing the privacy into the market and make people aware of how their privacy is to create a privacy label on each product.

Another way of forcing privacy awareness into the market is to put the consumer in the position of choosing how his/her privacy should be treated. As of today, a general does not have the competence of taking such a decision. In order for a consumer of doing so, he/she will need to be presented some kind of information that explains how the sensitive

data is being used by the vendor. When a customer buys for example a smartwatch, it is clearly explained what kind of functionality that is 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 have a much more natural relationship with functionality.

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

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

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

questions difficult to be answered

These are hard questions and may not have one single answer and is exactly one of the things that triggers me to look deeper into it. This thesis aims to answer these questions which may advance the research within this field.

address these questions as high-level guidance for the research, and contribute…

1.2 Problem Statement

The need for ensuring privacy have just become larger and larger with the years gone by. This may be seen in context with the rise of small IoT products which offers more and more closely monitoring of a person. By doing so, we consent for the vendors to treat our data in such a manner that they can offer us their products which hopefully will make our everyday-life even better and more efficient. A common saying is that a *"normal"* person should not be afraid of giving away his/her data given that it is treated in a safe manner. A political person in a highly respected position should rather think about this. An example of this is the case with Angela Merkel and the claims of NSA wiretapping her phone from 2010 until 2013 [5].

This may not be the actual case when looking at cases like the one between Cambridge Analytica and Facebook in the American election back in 2016 [30]. The case is extremely interesting to look into, namely because each *"normal"* or *"regular"* person was affected by this. This was a professional and targeted attack aiming to influence peoples understanding of what they should vote during the election. Each victim was not necessarily capable of understanding what kind of attack they were exposed to. This because the attack was to present targeted ads and in this way influence the political thoughts of a person.

Given such attacks, people have started to be more aware of their own privacy while browsing the Internet. Regulations like GDPR are also starting to take effect on the market and one can expect more to come within the coming time. One of the solutions that may apply to this critical area is Privacy labeling. To do so, we need to address the core elements in order to calculate the privacy of a product. There may be a number of ways of doing it, but there are some key points to evaluate either way. This thesis will focus on determining the following concepts:

- Transparency - How transparent is the product/platform?

In order to have a transparent product/platform, a user should be able to "see through" everything within the system. The vendor should not need to hide anything with respect to the consumer.

- Configurability - How large is the specter for a user in order to configure his/her privacy?

Given a IoT product that regularly talks with large and interactive platform, the user may expose his/her personal data to unknown entities. As this might be desirable for some people, this might not be the case for the rest. Given that the overall system offers good and clear configurability, the user is in the position of controlling how this data shall be treated.

Furthermore, there are *four* main elements that should 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 needs to be taken from a textual and general manner into an actual numeric value that represent the impact of each element and at the end can be used for evaluating a privacy label. As of now, I will not go any deeper into these elements. A more broad introduction of them may be found in section 3.6.2.

1.3 Method of the thesis

Throughout this thesis we follow the *engineering design method*, which is defined in 8 steps. The explanations below are based on references from *"Science Buddies"* [39].

- *Define the problem* - The problem is defined by asking several questions. We need to address *what* the problem is, *who* has the problem & specify *why* it is important to solve exactly this problem.

- *Do background research* - There is no need for re-inventing the wheel. Before going into such a research, we should first do a background research to see if there has been made any similar solutions that might be helpful to use. This may also help avoiding mistakes done in the past.

- *Specify requirements* - This stage presents the different characteristics the solution should have in order to succeed. This can be done by analyzing/mapping concrete examples (products) and gather key information.

- *Brainstorm, evaluate and choose solution* - One should always look at different solutions for solving a problem. There is a great possibility that an earlier project have come up with a solution that might be applicable for this exact task. When all the different solutions have been addressed, the best one for this specific task shall be chosen.

- *Develop and prototype solution* - The development phase can now start. This may be done over a great matter of time, even after it is delivered and presented. There should also be created a prototype of the solution which is a working version of the solution.

- *Test solution* - When testing the solution, we often address new problems which may result in a redesign of the solution. Such tests are done in iterations.

- *Communicate results* - The outcome of the solution should be presented in a understandable way and explain exactly what results the solution accomplished.

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

repeat: main questions

Problem statement has been defined in the previous section, thus we will focus on the following four research questions to further detail the analysis. The questions are defined as follow:

- **Q1. Which 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?**

Which are the … as result from the work in this thesis?

In order to determine a privacy label, we firstly need a method for determining 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 the term "Privacy" to different groups, how is this translatable to actual numbers and values?

How can we be able to look at a single product and its functionality while still take all its dependencies into consideration? There have been done several projects related to measuring privacy in the past years, but mostly with user-focused rather than product-focused.

1.3.1 Possible measurement method for the thesis

intro…. 2-5 references

From my point of view,

The most interesting project that have been conducted is the work of Agrima Srivastava et al. [44]. The project goes under the name of *"Measuring Privacy Leaks in Online Social Networks"* and is a method have been proposed for measuring privacy within Online Social Networks (OSN) like Facebook, Twitter, etc... The main goal for the method is to produce a *"Privacy Quotient"*. The Privacy Quotient represent the overall result produced after the method have 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) people tend to share in OSN (e.g. *contact number, job details, political view*). Further on, they weight these different parameters with respect to the sensitivity. For example, they have listed up a table presenting the different parameters with its sensitivity as follow:

because…

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 is used for giving each person a Privacy Quotient which may be between 0 & 7 where 0 is extreme privacy awareness and 7 is no privacy awareness. 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 [44]

The method can be applicable in order to determine a privacy label, but does not evaluate the actual product. It rather focuses on the user and just how he/she interacts with it. Therefore, I've chosen not to go further with this method.

utmerket!

It turns out that there is no other methods that stands out and seems applicable at this moment. Below, I will shortly present the chosen method for this thesis.

1.3.2 Choice of measurement method

one of the very few scientific work looking into meas. privacy is the .... I've chosen this

As for this thesis, I've chosen to look focus on the method *"Multi-metric approach"* presented by Iñaki Garitano et al. [16]. The reason for choosing this method is the fact that it is able to offer both a bird-eye look as well as a evaluation down to the core of each component.

The way this is done is to first map out the *"Overall System"* which may be a platform where the device uploads its data to. Such a platform may have loads of dependencies and these may taken into consideration when applying the method. Furthermore, one need to map out the different *"Subsystems"*. A subsystem is different parts of the overall system. One subsystem may be the actual device that is to be evaluated while the other may be the platform. Further on, a subsystem contains different *"Components"*. A component may be different core functionalities of the subsystem (e.g. Wi-Fi, Bluetooth, etc...). Each component have the possibility of being configured in different ways (e.g. on & off). These configurations is presented in a metric where each configuration gets a so called *"Criticality"* which represent how critical this specific configuration is with respect to the subsystem. The 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 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). These configurations are at the end evaluated in whats 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 give us a good presentation of what privacy the device & 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 needs to be addressed, but I will not go into such details in this section. This is more precisely presented in section 4.1.1.

1.4 Related work

Within the field of creating a privacy label, there have been some projects going on for some years. One of the first projects mentioning "Privacy" and discussing issues related to this is a work done Frederick Davis under the name *What do we mean by "Right to Privacy"?* back in 1959 [11]. He addresses concerns regarding peoples privacy in a bit different manner that one would address them in 2019, but is still highly relevant. By quoting the Frederick, one of the problems he 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 entering this in 2019, one can still find it representative. Speaking of IoT, what kind of rights does a person have if he/she chooses to share sensitive training data within a community and this data goes astray?

Beyond that, there have been quite a few projects related to the topic Privacy labeling. One of them is a project by the name of *"Designing a Privacy Label: Assisting Consumer Understanding of Online Privacy Practices"*, conducted by Patrick Gage Kelley [23]. This project aims at presenting a label for presenting how the privacy is treated for a specific product. Kelley substantiate parts of the motivation written for this thesis. By 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 presents a easily understandable label which is meant to put the consumer in a better position when deciding what product to buy. He addresses problems related to the current privacy policies and the difficulty of understanding these policies.

This paper was presented in 2009 which then gives a good indication of how valuable such a label is. There have already been 10 years since

this paper was presented, but still there is no such label within the market. Kelley et al. has also presented a paper within the same field where they performed a development process in order to create a presentable privacy label for consumers [24]. Back in 2009, there was estimated 0.9 billion IoT devices on a worldwide scale, while there is predicted to be 20 billion within 2020 [22]. Such a rise of new devices shows the importance of introducing this kind of label.

As of now, there is a collaborative project going on under the name *"SCOTT" (Secure COnnected Trustable Things)*, performed by 57 parties from 12 different countries [40]. 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 a part of this project and may be found under the name of *"BB26.G"* [7]. Measurable privacy is a key factor within the project in order to be able to present such a privacy label.

Building Block BB26.G

1.5 Summary

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

There have also been provided a short statement regarding the problem and why it may be necessary to introduce such a label. It may be possible to achieve the same goal in different ways, but my understanding is that by leaving the choice of privacy awareness in the hands of the consumer will not have that large effect on the development processes within the market, but still offer the focus that is needed within the field.

As this thesis is not the first to talk about the concept of introducing a privacy label, there is rather important to address the uniqueness of the work. This thesis focuses on validate 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 bird-eye look at the overall system whilst it still takes core functionalities of a subsystem into consideration. By merging these two concepts into a single method, we are 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 of this thesis to disclose.

Chapter 2

Background

2.1 Impact of Internet of Things (IoT) in specific domains

As of today, the world is becoming more and more digitalized. This have led to the entry of IoT devices both for the private but also for the professional market. These devices aim to make their users everyday-life easier. Because of their lightness and sensors, these devices often aims to analyze the users everyday-life. According to a study of users interactions with IoT devices, wearable smart devices has its niche by offering accurate health information [25]. This is often made by connecting the device directly to the users's body and then being able to monitor the user. This is clearly expressed by referring to a study done by Masaaki Kurosu: *"In other words, it is to stay connected more closely to users' body unlike smartphone."* [25]. A typical device in this area is a pulse watch, then for example a *smartwatch*. A watch like this is meant to help people improve their lifestyle, give more monitored control of their everyday-life behavior and even push its user further in achieving exercise goals. Typical for a smartwatch on the market today is that it at least have a GPS, pulse tracker and a accelerometer. Also, most of these watches are supported by a mobile application that monitors all these data and which then can present an overview of how each person's everyday-life looks like. A smartwatch like this goes under the term *IoT*.

The term IoT is a quite broad term and covers a whole lot of different devices. One common factor all of these devices contains is that they are often interconnected with a larger and more complex system. For the smart-watch, this would typically be a cloud or server that treats the data's distributed. This have led to the use of such devices in the following domains:

- Agriculture
  - According to the American news and finance website *Business Insider*, the growth of food production will rise with 70% from 2006 - 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 this market. According to Business Insider,

such IoT devices within the agriculture may be sensors placed within the fields in order to get a detailed view over the current temperature, acidity etc... This type of information may be valuable for each farmer, so that they can maximize their food production. A typical example of this may be when a wants to go for a holiday. As of now, a farmer may have a hard time trying to go on a vacation. This because he/she needs to regularly water the fields. By introducing IoT, the farmer may be able to remotely water the field either on a general timing. Looking at it in a more provident way, the farmer may be able to track the condition within the field and based on that information choose whether to water or not.

- Health care
  - Within health care, there are huge possibilities for implementing IoT devices. By introducing IoT into this field, there is a lot of different security and privacy issues that is to be taken into consideration. This may be because of the sensitivity of the data that is to be processed. There are a various of different possibilities in this segment, both in-hospital operations, nursing homes and home devices for long term patients [26]. By referring to the work done by *P. A. Laplante and N. Laplante*, there is proposed different types of usage areas within the heal care, for example people suffering form Alzheimer or bulimia (eating disorder). Solutions may be closely monitoring of the patients when they are at home. If the pulse drastically drops or the patient suddenly is far away from his/her home, technology like this may be able to alert personnel in time.
- Retail
  - Within the retail industry, there is a heavy growth of IoT. This would typically be sensors that are able to track each persons activity in e.g. a grocery store. These sensors may be NFC sensors or more specifically iBeacons [28]. The use of such sensors opens for a whole new perspective by profiling each user and their habits, and then do targeted marketing based on these data. According to a study done by *Pawel Nowodzinski*, there is estimated that the IoT will have a possible growth of *"up to 3.7 trillion dollars economic surplus"* within the retail industry [28].
- Transportation
  - The transportation industry is another sector where the IoT have been on the rise for several years. Such technology opens for the possibility of monitoring vehicles and other transportation services from a different geographical location. According to the *IoT Institute*, the use of IoT edge computing are on the arise 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 IoT is on the move.

- Energy
  - The energy business is currently facing a total makeover when it comes to how the end-user delivers its data. The rise of smart meters (AMS) is an ongoing project that is to make a big impact on how the energy companies operate. The AMS delivers a two way communication and offers a variety of different possibilities. One is that the end-user will no longer have the responsibility of sending in the amount of energy usage to the energy supplier, this will go automatically through the smart meter. Another big aspect that arises a big security concern is a feature that allows remote controlling of the smart meter [12]. This opens for both advantages in order of control for the energy supplier company, but also disadvantages if this feature would come in the hands of bad intended people.

- Manufacturing
  - IoT is already well established within the manufacturing sector. According to a report delivered by *ProQuest*, the annual investment in IoT will rise from from US$ 6.17 billion (2016) to US$ 20.59 (2021) [9]. This growth shows that IoT is becoming more and more important in order to make the production more profitable. IoT devices used in this field may be monitor sensors that aims to analyze the efficiency of the daily production. By collecting such data, makes the possibility for a company to better map where the specific needs for more efficiency lays.

In addition to this business view… a large range of products addressing the end-customer directly [REF]

As this technology raises some serious privacy and security concerns. How are the data exchanged between the smart phone and the watch? How is the data stored? How are the data distributed between different cloud services? There are great variety of mitigations that might lead to a more secure handling of this issue, but I won't be addressing all of those. In the next section, I will broadly explain one proposed method that is called *"Privacy Labels"*. This will also be one of the main topics to go deeper into during the rest of this thesis.

Thesis: END-USER empowerment

2.2 Security affecting Privacy

Security impacts privacy. This statement is inevitable as we would need security on top in order to maintain privacy. It would not make sense to let each user choose what information should be public available and not if

there is no security at top of this. Given such a system, a malicious person might be able to conduct *user profiling* (monitoring a user over a longer period and mapping his/her habits). There is a great possibility of such an attack within IoT as these devices continuously deliver sensitive and precise data that can have a large impact on a person. One does not want such information to be in the hand of unauthorized personnel. We therefore need security in order to deliver privacy.

There is a variety of different mitigations for the vulnerabilities within the IoT industry. This thesis will not focus on all of them, but I will be taking a broad look at some of them.

2.2.1 Self-awareness

In general, a normal person does not take privacy into concern when buying a new device. Very often, the focus for the product lies in the functionality and not the privacy. Assuming that the level of privacy within the device is quite low, the user may be more prone than desired. The simplest privacy mitigation may then be *self-awareness*. This can be as easy as changing the default password on 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 own. Currently speaking, each person on the earth, in average owns 3 IoT devices [29]. Looking into what is expected for 2025, there is expected that each person in average will own *9* different IoT devices. Both 3 and 9 devices may not sound like a whole lot. But assuming that most of these IoT devices are located in more wealthy countries, the average rises quite drastically. In 2018, there is approximately 23 billion IoT devices, while this is estimated to become approximately 75 billion within 2025. This gives a perspective of how large this industry has become. Given that each person are in control of and overview over each and every device they own, the privacy vulnerabilities drastically drops.

2.2.2 Security by Design (SbD)

The concept of *Security by Design* is ten different rules set by Open Web Application Security Project *(OWASP)* for designing a secure system [41]. These rules applies both to software development and physical IoT architecture. The principles are as following (taken directly from OWASP official descriptions [41]):

- *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 these different ten rules are 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 industry factory with a whole lot of critical sensors that is connected to the Internet, one would typically need them to operate fast. There is very often a trade-off between

speed and privacy. In order to minimize the vulnerabilities for this type of system, one should implement security in different layers. By setting strict privacy regulations at the very top level of the system, the need for high security may drop the deeper one go into the system. By doing so, one is able to maintain the speed and availability that is needed in order to do a complete job.

2.2.3 Security standards

In order to maintain control of the development for all products on the market, there should be a general standard for creating/deploying products to the market. In a report from NIST, there is a clear statement regarding standardization for the IoT market [19]. It appears that the current state of the art within standards for the IoT market is not sufficient enough in order to maintain stable security for each product. The report states different core values for a secure system, e.g. encryption, digital signatures and so on [21]. These are quite important parts to address in order to find a good cut between security and functionality. To be able to standardize the whole IoT market, there is a whole lot work that needs to be done. This might be the most sufficient way to go, but will take time. This topic is the closest to what this thesis will look deeper into, namely to be able to set a list of criteria for what a "secure" system should look like. Although this thesis focuses on privacy and will *not* focus on security, it is important to address the fact that security have a large impact on privacy.

2.2.4 Privacy by Design (PbD)

PbD is a list of different principles that should be taken into consideration when building a product. The start of the ideas behind principles were introduced by Alan F. Westin back in 1968 [38]. The different principles are presented as follow (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 personnel
- *Reasonable security:* Adequate security safeguards should be put in place, according to the sensitivity of the data collected.

while PbD is focussing on developers…this thesis …

- *Accountability:* Record keepers must be accountable for compliance with the other principles.

Even though the essence of these principles have been within the market since 1968, there is still issues related to the topic. The need for better privacy is growing exponentially as IoT is increasing in peoples everyday life. The concept *Privacy Labels* is therefore a suggested way of presenting the privacy in a more understandable way to the end user [37]. 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 this might be helpful, we firstly need to define the concept *"privacy"*. According to *Cambridge Dictionary*, privacy is defined as following: *"Someone's right to keep their personal matters and relationships secret"* [35]. This tells us that privacy is a concept of having personal data kept private. Or that confidential data is being kept secret and only visible for authorized personnel. This definition will be most of the foundation in order to create such a privacy label.

This is a concept of creating labels from e.g. A++, all the way down to F (where F is failed). The concept is based on much of the same principles as the European energy labels for white goods (as shown in figure 2.1). This label gives a graphical overview over the products classification, so that it is understandable for each and everyone. The introduction of this label have been a great success and is one of the reasons for doing exactly the same with respect to privacy. This label is based on different criteria for white goods and the goal is to create similar measurable criteria for privacy when presenting a Privacy label.

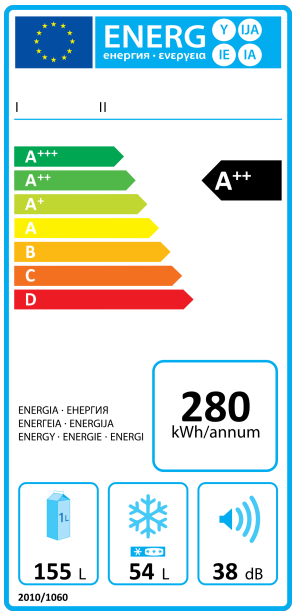


Figure 2.1: European Energy Label

As addressed before, there have been conducted similar work regarding Privacy labeling [24] which substantiate the need for such a label even more.

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

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

Furthermore, there should be taken into account a variety of different aspects, for example the freshness of the data, notion of data sensitivity, etc... This method could be applied to any products within the different sectors described in section 2.1. By looking at for example the health care sector, there are absolutely a need for such labeling. Most of the devices that are used, is used in conjunction with personal data that is to be kept secret/private. Given such a label, it would be easier for the administration to choose which product is the most suited or not. This would also apply to a regular person when buy an IoT device for health monitoring.

Given the home health service, there might be people suffering from different types of diseases (e.g Alzheimer). By suffering from such a disease, the person's memory capacity will slowly fade away [1]. As mentioned in section 2.1, this is an opportunity for the use of IoT, namely that one for example can be able to keep track of the patient at every

time. Simultaneous as this type of technology offers a lot of benefits, it also offers some privacy concerns. One should expect that all sensitive data are transferred on a secure and encrypted connection. One should also expect that no unauthorized personnel will be able to administrate such a system as it can cause serious injuries, even death for the patient. It should be possible for the end-user to have an overview over how this data is being treated.

By offering such a label it will be easier for the end-user to choose which service to use. This label might also push the producers of the product to go even further in securing the data that is being collected. When introducing such a label like this is to 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 retrieve for people when buying products like these.

2.4 Summary

In this chapter, we have taken a bird-eye look at the term IoT and what areas it covers. The most common factor for a IoT device, independent of area, is the purpose of the device and how the overall system is designed. Most of the times the purpose of a IoT device is to gather data, which it forwards to a endpoint for data processing. The reason for forwarding the data rather than evaluate them locally on the device is the capability of the device. As discussed in chapter 2.1, we can see that IoT is taking its place within *agriculture*, *health care*, *retail*, *transportation*, *energy* and *manufacturing*. All of these different industries are using IoT in order to be more independent from daily tasks. Such daily tasks might just be monitoring of the condition inside the barn.

Furthermore, we have taken a broad look at security mitigations both from a user perspective, but also from a manufacturer point of view. As pointed out, the easiest way of ensuring security for a user is self-awareness. Very often this is about being critical when using such a device. Just because there is a common brand name on the product does not necessarily mean that its security is taking perfectly care of. Even if the security is taken care of, the user might be exposed to attacks if the product is used improperly. For a manufacturer point of view, we have been looking at the 10 different concepts given in *Security by Design*. These are ten different concepts that should be taken into consideration when designing a system.

The concept of *Privacy Labels* was introduced. In order to be able to set such a label, we need to have a look at the system as a whole. This may be all the way from data collection done by a sensor all the way till it have been processed by a endpoint. Later in the thesis I will go deeper into which methods that might be usable in order to give such a label. I will also give a careful explanation of what criteria each level within such a label should have.

This chapter is a contribution to Q1 (*Which challenges relate to privacy using IoT devices?*) by explaining the current state of the art within the IoT

community. The chapter have addressed the following:

- It is fair to say that IoT will be dominant in the coming years. The need for a standardization when it comes to privacy is raising. There is mentioned the possibility of forcing a privacy standardization for the vendors into the market, but falls short by the overhead. Implementing such a standardization will take time as well as slow down the innovation. A proposed way of doing this is by introducing Privacy labeling.
- Another aspect is the fact that such IoT devices collect sensitive data very often on a large scale (big data). As machine learning is growing, the possibility of user profiling may rise if the privacy is not maintained.
- As IoT grows larger and becomes more available, the more it becomes relevant for different domains. This introduces a threat for each persons privacy as they become more dependent on these devices within the different domains.

Anbefale Privacy Label?

Chapter 3

Privacy in health-monitoring

In the previous chapter we have addressed the different domains where IoT is represented as well as the need for a privacy standardization. Outcome of the chapter is the suggestion of using Privacy labeling. This chapter will present the use case for testing out the proposed Multi-metric method in order to determine such a Privacy label.

3.1 High level functional aspects

As of today, most of the IoT devices are either physically or wirelessly connected to a platform that monitors its data. This gives the product the possibility of being more complementary, but it raises privacy concerns. There are a lot of different IoT devices on the international market. Vendors for these kinds of products may be for example *Fitbit* or *Polar*. These companies delivers a variety of different products that may be placed under the subject of IoT. Some of these vendors wants to make a central platform for all their products and then link them up to the same user. By doing so, they may be able to offer a more complete range of products which talks with each other and may use the other devices data in order to deliver a more precise analyze. If a user is happy with one of the products from the vendor, it raises the possibility for the customer to buy yet another product from the same vendor on the same platform. This is obviously meant as an advantage for the customer. Simultaneously as the vendors is able to offer more products on the same platform, they end up in a position where they need to treat all the data in a safe manner. Given a data breach into such a platform may lead to *single point failure* which can be quite dramatic if the data is considered sensitive.

A possible flow of data within a typical IoT environment can be as follows. Data is collected via a *pulse belt* that is attached to the users chest under a training session. As soon as the session is finished, the pulse belt transmits all the collected data directly to a *smartphone* via e.g. Bluetooth. As soon as the data have been received by the smartphone, the user might have the possibility to further synchronize this to a *cloud*. Once the data have been transmitted to a cloud, the user might be able to access the training results from whichever device. Such a system requires that privacy

is ensured in each step. By introducing a new transmission, the possibility of for example eavesdropping gets higher. Below, I will look at one product and carefully explain the different possibility that is within the system.

possibilities that are

3.2 Use case: Polar M600

Intro.... healthcare - smartwatch - Polar - M600

A smartwatch that was introduced into the market in 2016 is the *Polar M600* (hereafter called *the M600*). Even though this was released in 2016, it is still highly relevant for the consumer market today. According to Statistica, the number of sold smartwatches have raised from 5 millions units to 141 million (end of 2018) on a worldwide scale [43]. This shows that these products are starting to become a part of each persons everyday-life more and more.

The M600 can either use the Android Wear app or the Polar Flow app. Such a watch aims at making its user more efficient as well as healthier. This may be done by constantly monitoring the user and present the data in an understandable way so that the user can make decisions based on this. Simultaneously as the market for these *IoT* devices are expected to grow exponentially, the privacy is not necessarily taken into consideration. This may be done both from the manufacturer point of view, but also from the users 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 have a whole lot of different specifications [45]. As we can see from table 3.3 on page 23, the watch is quite representative for most of the smartwatches on the todays market. One thing to keep in mind is that this watch supports both *Android Wear* and *Polar Flow*. Android Wear is a generic platform that supports a variety of different wearable devices, e.g. *Smartwatches* [27]. Given that this is a platform that supports different types of devices, it seeks to offer more general functions. This can be both an advantage and disadvantage as the system does not specialize in a single

product. On the other hand it can be an advantage as the user only needs to focus on familiarization with one platform, regardless of what product (e.g. smartwatch) he/she has got.

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. According to the user manual for the M600, both these functions are mentioned, but also a whole lot more (figure 3.2 on page 24) [15]. Here we can see that the watch for example supports a direct Wi-Fi connection which allows the watch to talk directly with the Android Wear app or Polar Flow app regardless of the distance between the smartphone and the watch rather than via Bluetooth. Another interesting element that is supported by the watch, is the GPS features. The watch may log *altitude, distance* and *speed*. All this information is delivered in real-time to the app on the smartphone while the user is doing a workout. According to the user manual, the data is automatically synced with the Polar Flow app after each training session. The watch gives an "inactivity alert" or the user reaches his daily goal. These data are then again synced from the smartphone onto Polar's web-services. Another feature that is not mentioned in figure 3.2, is the support for sleeping monitoring. The M600 supports monitoring of the users 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 monitor the sleeping. The watch will automatically detect that the user is asleep and then start to monitor how the rhythm is. This data is synced in the same way as the workout monitoring, namely to both the Polar Flow app and Polar Flow web service. This naturally raises privacy concerns to how this data is being treated.

3.4 Technology details Polar M600

The M600 have two possible monitor systems. One is *Android Wear* and the other one is *Polar Flow*. Android Wear is a generic platform which have a general support for all watches that runs the Android OS. The clear advantage of this, is that the user only needs to relate to one specific platform, regardless of the watch. It obviously comes with limitations, which are presented below. The other platform is Polar Flow. This is a custom-made platform for all Polar's smartwatches. It comes with a whole

	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: Polar M600 Features

lot of different features and is tailor-made to fit Polar's watches. Android Wear delivers an app for monitoring the data, while Polar Flow delivers both an app and a web service. These services deliver a user-friendly overview of the data that is described in section 3.3.

3.4.1 Android Wear/Wear OS by Google

Android Wear *(now under the name "Wear OS by Google")* is a more generic platform for smartwatches (a version of Google's Android Operating System). It was released by Google in March 2014. The Android Wear supports a whole lot of different smartwatches, including the M600. The current version of the platform is "Wear OS By Google - Smartwatch v3" [3]. This is a platform that aims to support both the Android and iPhone smartphones even though it is based on the Android OS. According to their official web page, the Android wear is: *"Small, powerful devices, worn on the body. Useful information when you need it most. Intelligent answers to spoken questions. Tools to help reach fitness goals. Your key to a multiscreen world."* Because of their wears capability to monitor a person, the device is able to deliver a lot of helpful information to the user.

As of today, almost 2,5 billion people have their own smartphone [42]. This device is far more capable of processing data than a smartwatch (e.g. Polar M600), which is one of the reasons Android Wear have been made. It is also possible to make an application run perfectly good on a wearable without any interception with the smartphone.

Android Wear aims for third party developers to create both applications and devices on their platform. This have led to a whole lot of different companies making their way into this market. According to Android Wears official web page, companies like *Nixon, Hugo Boss Watches, Fossil, Polar, etc...* have created watches running Android Wear OS [4]. As these large worldwide companies makes their way into this market, it will naturally follow that people are going to buy these devices. This also creates a security responsibility to the companies as they are to handle very sensitive personal data.

Figure 3.3: Wear OS by Google

3.4.2 Android Wear: Security and privacy aspects

As the smart watches are running Android, this comes with both advantages and disadvantages. The advantages are that the Android system already have been created and have a lot of different security mechanisms [13]. This may for example be that each application the device is running is being sandboxed (each application has its own private environment). The disadvantage is that the system also inherits most of the security flaws that is already within Android.

Some other security concerns are how the data is being treated. In order to locate the security concerns, we can distinguish between data that is stored locally and data that is being transmitted from the device (most likely to a smartphone). If we consider that the data is being stored locally, we can remove a lot of attack surfaces. Since the applications running on the watch is being sandboxed, this implicates that the application and no others can access its internal storage. Other users/applications can only access the storage under specific circumstances [2]. This may be that the one that wants to access the storage have root access. According to Android's official web page, all internal storage will be removed when the application is being uninstalled. In other words, data that is considered to be sensitive (should not be accessible/visible to others), should be stored here. An application is also able to save data in an *external storage*. This is, according to Android's official web page, a public environment which is world-accessible for all applications. This storage may be on for example an SD-card. This may be handy for applications that e.g. saves images. An user may want to re-use these images after an uninstallation of the application. The security aspects of this 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 within the internal storage, one can to some extent say that it is the developer needs to ensure the privacy.

then

Given that the data is being transmitted to a smartphone, which then transmits the data to a server, we suddenly have a lot bigger attack surface. This opens both for a larger use area for the application, but it also expects more security regarding the handling of the data. We will discuss how some of the watches handles this later in the thesis.

3.4.3 Polar Flow

The other application that is possible to use, is Polars own app, *Polar Flow*. As seen in figure 3.2, the app supports a variety of different possibilities for the end user. According to the official website of Polar Flow, 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"* [31]. By looking further deeper into the user manual, we are met with the following summary of the app: *"In thePolar 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 in the manual, we

are told that the training data automatically will appear in the Polar Flow application. This is possible to share within the *"Flow Feed"* with specific people. The app shows not only the training data, but the users daily activity in details (including sleeping rhythm).

wrapping within text

Figure 3.4: Polar Flow

In order to use the Polar Flow app, the user has to create an Polar account with basic information *(e-mail, first name, surname)*. It has the possibility for adding more specific data like *sex, birthdate, height, weight, maximal heart rate, minimal hear rate, aerobic threshold and anaerobic threshold*. Based on these data, Polar Flow will calculate the users BMI. Within the app, it is possible to make changes to some of these data, but not all of them. The rest has to be done via Polar Flow's web service. The web service also provides a variety of different services. According to the user manual, there is user is allowed to both plan and analyze the training details. It is also the possibility to connect with other people within the Polar network. Here the users can both share their training data with each other and create a public training program for their group.

Regarding the Polar Feed, the users have the possibility, as mentioned earlier, to see how their friend's workout sessions have been lately. Here it is also possible to share the best achievement for a user. There is also another interesting feature within the Polar Flow app that is called *Explore*. This feature lets each user share their favorite route. Their routing information can be published public for all Polar users to see specific information regarding their training session. It is then made visible in the Polar web service. Here it is possible to see where the route was, how long time it took, heart rate (both highest, lowest and average) and how many calories that was burnt by the session. As shown in figure 3.5 on page 28, the user is also delivered a graphical overview over a variety of data from the workout session.

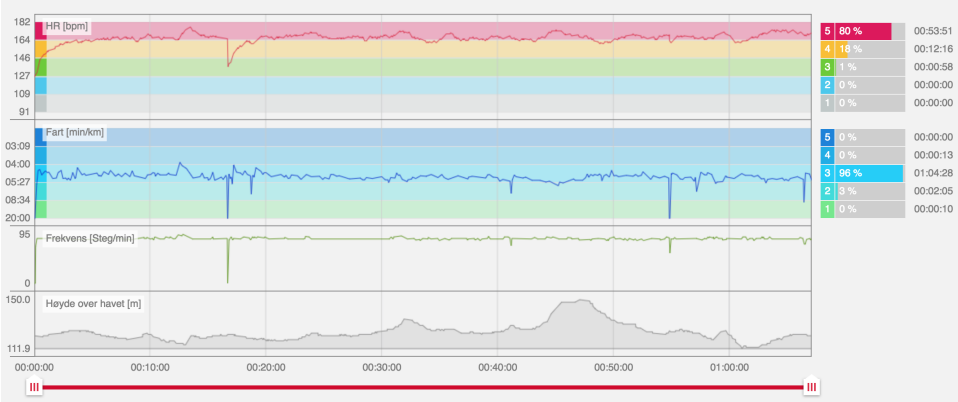


Figure 3.5: Polar Flow Explore

Not only does Explore deliver graphs explaining how training session was, Polar also delivers a feature that is called *"Relive"*. This feature lets each user relive the session by showing a video. This video contains a scale of how heavy the session was, geographical location, duration, current distance ran, current heart rate and also the current speed. It is also deliveres a *Google street view* in order to show the surroundings for the user. The highest heart rate picked up during the session is also delivered in the video. Furthermore, the web service also delivers the feature *Diary*. This is a calendar which logs all activity for each day and gives the possibilities to review all the past sessions.

3.4.4 Polar Flow: Security and privacy aspects

Almost all the information that is gathered is to be considered as sensitive data and should not under any circumstances be available for unauthorized users. Leaving the Explore functionality open for any user to use raises a security concern to each user regarding how this feature is being used in their everyday life. By referring to the official user manual, the Explore feature is to provide 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."* These two sentences give no direct information about who is able to see these data, it may then be understood as public data. Assuming these data is to be understood as public, then one can say that the responsibility lies with the user.

As Polar offers the *Relive* function, any person registered in Polar Flow can suddenly map each person's behavior very precise by looking at the different data that is provided (GPS, pulse, speed, etc...). By mapping these data, it would be possible to create a visualization of how each person's everyday life may be. Assuming these data would be in the hand of unauthorized people, it would for example be possible for a criminal to see a training pattern for a specific person. Based on this pattern, it may be easier to conduct a burglary in the victims home, just by assuming that the person is not at home based on these data.

Table: WearOS vs Polar Flow (?)

3.5 Technological challenges: Polar M600

With all the different types of information that is stored/distributed with the M600, it arises some technological challenges regarding the security. Most of the information that is being treated is personal and should not under any circumstance become available for unauthorized personnel. Another aspect is the software that follows along with the watch, namely *Polar Flow*. This service offers, as mentioned, a lot of different functionalities. They are mostly for the benefit of the customer, if used correctly. Regardless of the benefits of the service, there is a social privacy issue. This will be discussed in the subsections below.

3.5.1 Privacy and measurability of privacy

The M600 supports a variety of different ways to track the users behavior. By referring to the figure 3.2, one can see that there is a possibility of collecting a variety of different information from the user, e.g. voice and pulse. This data is either stored locally on the watch or distributed to the cloud, either via a smartphone or directly via Wi-Fi.

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

3.5.2 What does privacy numbers mean?

There have proposed 8 different levels of privacy labels [37]. These levels goes all the way from A++ down to F, where F is failed. Below, I will explain the requirements for each levels. In order to make accomplish a specific privacy level, different parameters are taken into consideration (e.g. configurability). This means that to a certain extent the system can be evaluated to both a level B and D (given the configuration done by the end-user). The result will be based on how the given system present the possibility of configuring it's own privacy and also the configuration options.

- *Level A++:* One should expect that no data is 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 is being treated. There is no restriction for what unauthorized people can see/edit. The solution is not GDPR compliant.

beskrivelse …. draft som kommer ut av diskusjoner med fagpersoner
These labels need further discussion and a harmonisation…
Given the technical background of my work, I rather focus on …

3.6 Evaluation of the data

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

3.6.1 Measurability of privacy

are

When we look at privacy, there is a lot of different parameters that needs 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 this thesis, I will go deeper into this approach, both by describing it and applying it on the different use cases. The approach evaluates each level of the system and will lay the foundation 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*".

By looking at the use case, Polar Flow, there are a whole lot of different data that is being stored. Below, I will describe these data with respect to the "*Controlled collection*":

Framework for bruk av disse or? [16]

- General information:
  - Basic information (**full name, town, country, e-mail, sex & birthdate**). Each of these data elements alone may not be sensitive, but by combining them, they are to be considered sensitive. In order to determine the privacy of the user, one should expect that this data is being kept secret and unreachable for unauthorized entities. *Mandatory information.*
  - **Height & Weight**: This information alone is not to be considered sensitive by itself, but may have impact in association with all the other data that is being stored. *Mandatory information.*
  - **Training background**: This information is not to be considered sensitive by itself, but may be sensitive in association with the other data that is being stored. One should therefore expect this to be kept in a safe environment, unavailable for unauthorized entities. *Mandatory information.*
  - There are a lot of other data that is 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**: By using the M600, Polar Flow receives the heart rate of the user from each training session.
  - **GPS**: The M600 continuously stores 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 while doing a training session. Based on this, Polar Flow presents both the length 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 between age, workout duration, heart rate and length. This information, in association with the basic information, may be sensitive.

why? what's next?

3.6.2 The four main elements for measuring privacy

intro

- **Controlled collection (Data)**
  - The first element to consider is how the collection of the data is controlled. As described above, Polar stores a lot of different data that may be considered sensitive in context with each other. Both the way they are treated and how the client is offered to modify the usage of this data will have an impact on the privacy of the user.
- **Controlled processing (Purpose)**
  - As stated by Polar in their privacy statement, their purpose for using the data is 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"* [32]. In order to ensure the privacy of the user, 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 what the user have given 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 criteria for the privacy of the user. This information can be used by a third party to for example make a narrow profiling of the user. As it turns out in Polar's case, they tend to be strict in how the data is being distributed. By referring to Polar's privacy statement: *"You are responsible for managing the information you share or transfer out of the system"*. This puts the user in responsibility of the data on the outside of Polar's services.
- **Invasion prevention (Security)**
  - In order to ensure privacy, we will naturally rely on security. If there is no security on top, one can't ensure that the privacy of the user is intact. There is a lot of research around this topic, but this will not be the focus for this thesis. In this thesis, we assume that security is ensured by default.

To give a complete overview of how the privacy of the user is ensured, all these four different criteria should be set up against each other. Below, I will go deeper into the first criteria, namely *Controlled collection*.

3.6.3 Controlled collection

To evaluate the data, we need to evaluate them in context with each other. As discussed above, a lot of the data is not to be considered sensitive alone by itself, rather in context with other data.

When looking at the training data that is being synced with the watch and *Polar Flow*, it is offered a quite clear *transparency*. By looking at figure 3.6 on page 34, we can see that privacy is ensured by design. The profile privacy is default set to private. There are three different options, namely *Public, Followers* and *Private*. The public function gives everyone access to view all information on the user's profile. All this *configurability* will result in a more positive evaluation of the system. While the user is offered the chance to configure his privacy settings, he is automatically made more aware of how the data is being treated. The user is able to set a specific 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 is offered to update all the session history to being private.

Based on the configurability options, it seems like Polar Flow offers good privacy options for their users. But is this actually the case? As discussed in section 3.4, Polar Flow offers the function *Explore*. This function very much adds up to the configurations that is being set in the privacy settings. Given the configurability the user is offered, it is possible to argue that this function fully approved, both by the users and Polar itself. As it turns out, this function has become very popular. In my opinion this may not be because people actually want to use the function, but simply because they are not aware of what kind of data they are distributing. As a result of this, Polar have temporarily taken the function down [33]. As it turns out in the statement, Polar clearly states that there has not been any leakage of any data. But it raises concerns to how the public data may be used. As the function Explore offers very detailed information of the user, there may be a potential threat the user. This may be for example profiling each user based on the different data. It would not necessarily be that hard for a malicious person to form a clear view of when a person is out for training on a regular basis. People tend to have regularly training habits. Just by evaluating this, a malicious person would be able to, most likely find out *where the person lives*, *when he/she is at home*, *the health condition of the person* and so on. This is one of the reasons why Polar chose to temporarily take the service down.

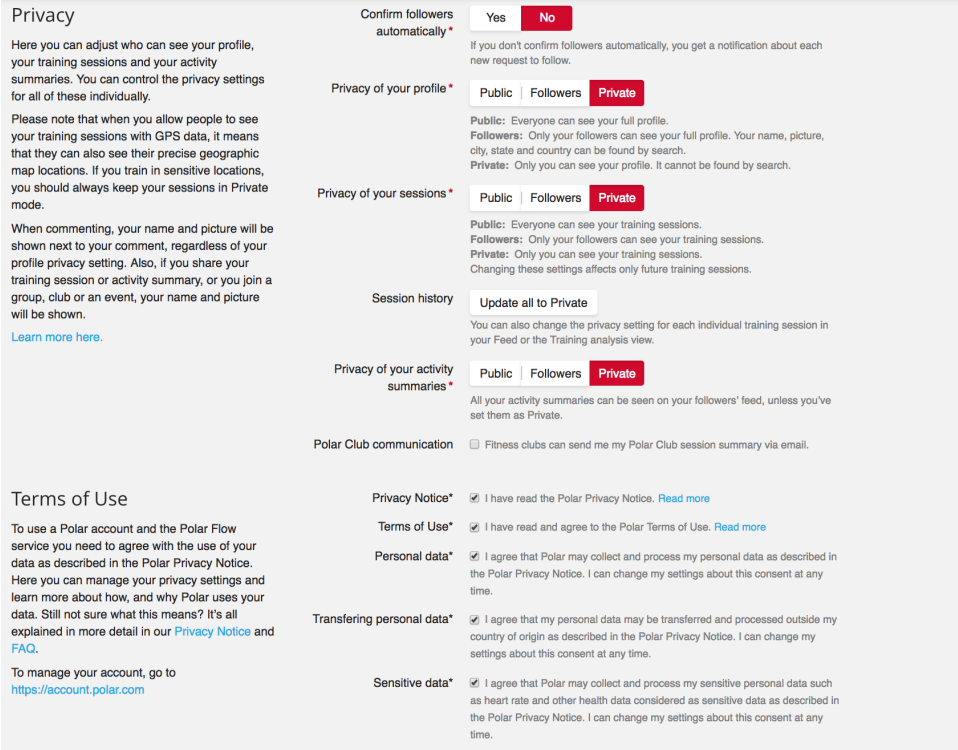


Figure 3.6: Polar Flow Privacy Settings

3.7 Summary

In this chapter we have been taking a deeper look into the smartwatch Polar M600 and its endpoints (Polar Flow/Android Wear) as well as looking at the general regulations for measuring privacy. This watch is to be considered as representative for the smartwatch market and I have therefore elaborated its functionality and architecture. A possible data flow for such a system have been presented and we can see that by introducing such a flow comes responsibilities associated with privacy.

Both the endpoints Polar Flow and Android Wear have been explained quite specific with focus on security and privacy. Furthermore the concept of privacy labels was introduced and given a broad introduction.

The Privacy labeling have been presented on a scale from A++ (top score) all the way down to F (failed). In order to be able to give a precise determination of a label, we have also introduced four main elements that needs to be considered as well, 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've discovered the different data that needs to be measurable 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, otherwise we can risk that the measurement becomes inefficient because of the size.

- 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 large scale as there would most likely be large variations between experts. My recommendation is therefore to introduce some centralized database where privacy values are presented so that an expert can use these within the metrics.

Chapter 4

Assesment methodology for privacy

4.1 Translation from technical parameters

As discussed in section 3.6.1, we have to have to find a way of measuring the privacy. As we look further, we will need a way of translating these measurements from technical parameters into actual privacy values. This translation is done mostly by applying the Multi-metric approach. I will later in chapter five apply this method on the Polar M600.

4.1.1 Multi-metric approach explained

The multi-metric approach is a methodology for measuring the *Security*, *Privacy* and *Dependability* (SPD) for a system. The methodology takes both a bird-eye look at the system from a general perspective and combines this with the core functionalities of the system. By combining all these different values together, we will end up with a result between 100 and 0, which will be the SPD_{System} and in this case will only be focusing on privacy. At the very beginning of the methodology, we will set a SPD_{Goal} for the privacy. This value will be what we expect as outcome.

The function gives a much more precise overview of which privacy issues the system may have and exactly where the issues is located. In order to give such a precise overview, we will need to split 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 of these scenarios will have their own SPD_{Goal}. Furthermore, we will make a variety of different *configurations* which may apply to all the different scenarios. Finally, different metrics need to be made for each component (e.g. Wi-Fi connectivity). Assuming we are describing the component encryption, there are two possibilities for how this component can be used, namely *on* or *off*. We will also be adding a *weight* to each component, based on how big impact the component will have (in this case privacy). Both these outcomes will have a criticality value both for security, privacy and dependability (in

this case just privacy). Each component's criticality value is joined together in order to create the criticality value of the subsystem. By combining all the results from the different subsystems, we will at the end get the total SPD_{System}.

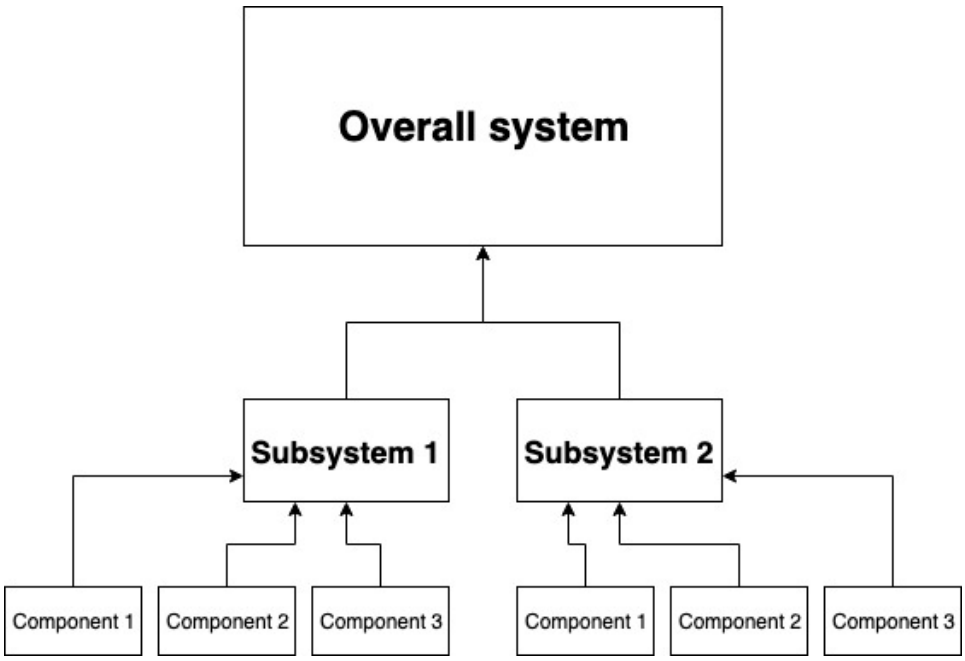


Figure 4.1: Multi-metric method visualized

4.1.2 Evaluation of the methodology

When applying the Multi-metric methodology, we will at the end get a result based on the actual functionality of the device, set up against the assumptions before applying the function. The overall goal is to come as close as possible to the original SPD_{Goal}, but this can vary.

In order to give the product a privacy label, we will use the outcome of this function as some of the foundation for setting the specific label. The outcome of the multi-metric for each scenario (SPD_{System}) will be, as mentioned, a value between *100 - 0*. We will get a result for each configuration with respect to each scenario. This may be displayed in a matrix in order to give a good overview. After getting the 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) & red(failed). The criteria are as follows (set up against the SPD_{Goal}):

- Green: Within the range of ± *10*
- Orange: Within the range of ± *20*
- Red: Everything else

This function, Root Mean Square Weighted Data, presents how the criticality C is calculated. It is based on the actual criticality x_i and the weight W_i.

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

4.1.3 Variation and limitations

As addressed above, the result may vary from the original goal that was set. There are a lot of different parameters that may influence the actual result. The weight of each metric may not be the correct weight for the metric in the first place. An example may be weighting *GPS tracking* too high with respect to privacy. At first sight, one would maybe think that this is critical for the privacy of the product, but in reality might not be that critical. This assumption will have a great influence on the relation between the goal and the result. One disadvantage of the function might be how exactly these metrics are set. By referring to the paper where the Multi-metric methodology was presented, we can read the following: *"The weight w_i is provided by the expert in the field, and provides the significance level of each (i) metric within a component, (ii) component within a sub-system or (iii) sub-system within the system evaluation"* [16]. As we can see, the weighting is done by "experts in the field". It should be some sort of central reference for each metric. This may be a generic weight & privacy criticality for *GPS tracking*. Given such a reference point, one would be more likely to have a more precise SPD_{Goal}.

4.2 Key points to determine a privacy label

In order to set a privacy label, must do this with respect to the result of the outcome from the Multi-metric approach. When performing the Multi-metric methodology, we will get a privacy score between 100-0. There will be a score for each configuration with respect to the given scenario. By combining all the results, we are able to calculate the average privacy score. Given good and realistic configurations, we will have a good overview of how the privacy is maintained. This may be expressed as shown in fraction 4.2. By this, we are able to calculate the average privacy A where p symbols the result for a given configuration i with respect to a scenario, divided by the total privacy results p.

$$A = \frac{p^i + p^{i+1} + p^{i+n}}{\sum p} \tag{4.2}$$

There should be some relation between the average A result 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 A on 100 is what it takes to get a privacy label A, will most likely fail. This would also apply to privacy label F, which should not expect to

get an average A on 0. The result will be somewhere between and so should the label be placed.

4.2.1 Privacy label seen from a user perspective

In order to set such a privacy label, we will need to evaluate not only the functionality of the product, but also take in consideration of how this label is being presented to the user. To do so, we will need to understand how the user will perceive this. By referring to the currently ongoing project SCOTT:BB26.G, we can read 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"* [36]. By reading this, understand what sort of challenge it is to measure privacy. As it points out, privacy measurement may be different from person to person. This is because one person may not consider the specific data to be as private, while other may.

If we look at a highly profiled person, for example a prime minister, he/she may have extremely high demands for how his/her data is being treated. At the other hand, 40 years old "Ben", working as an accountant may not have such high demands. Where the prime minister may not accept that his/her data is being stored for more than 6 months, while "Ben" might want to have his data stored for a longer period so that he can browse his history. In other words, privacy is relative for each person. Therefore, it is difficult to set a privacy label based on the user. The evaluation will rather need to be focused on the functionality of the product and how the data is being treated.

4.2.2 Privacy label seen from a vendor perspective

As of today, there is different regulations for deploying a product on the European market. The newest regulation is GDPR (General Data Protection Regulation) from EU. This regulation took place in the European market May 25th, 2018. Shortly described, the goal of this regulation is to give the users more control over their own data and they can at any point demand to get (electronically) all the information that have ever been stored about them. Furthermore, each user can demand to get all private information deleted on the platform/service. If a company fail to meet these demands, they may face a fine up to 4% of their yearly income 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 which is linked to a EU citizen. This means that a company in the US will also be affected by this regulation, given that they offer a service where sensitive information of a EU citizen is stored.

Another demand that is currently in process within the European Union, is a regulation called *"ePrivacy Regulation"* [14]. I will not go into details regarding this regulation, but I will shortly describe it.

The regulation will replace the current directive *"Privacy and Electronic Communications Directive 2002"*. Its main focus area is to ensure the confidentiality of the user. This may be when transmitting messages on a communication channel. In order to understand this, we first need to understand the meaning of the concept *"confidentiality"*. The concept may be expressed as follows: *"Access must be restricted to those authorized to view the data in question"* [10]. This means that the information must not be made available for any unauthorized entities. This can be ensured in various ways, typically by encryption & access control.

The regulation may apply to communication channels like *Facebook* or a whole new interactive communication platform in the future. As of today, there is no such clear demands for how the confidentiality of each user should be ensured. With this regulation, there will be a set of specific criteria and rules for how the confidentiality should be ensured for the user. If a company/platform fail to fulfill these demands, they may face the same fines as set in GDPR, namely up to 4% of their yearly income or up to €20 million (which one is higher).

Both the GDPR and ePrivacy Regulation is EU directives that each vendor has to fulfill in order to deliver a service for people within the EU. These demands, at least GDPR will be extremely central when a label is set for a given product. Shortly summarized, one would expect the vendor to emphasize the privacy of the user and ensure the confidentiality of the data that is being both transmitted and stored.

4.3 Two different privacy aspects to evaluate

To be able to set a privacy label, we need to take different parameters into consideration. Many of these parameters have been covered, but there are still some important aspects to look into. These criteria may be extremely important seen from a user's perspective. Given a top score on each of the following criteria, one can argue that the product should be awarded *Privacy Label A*. Whilst the product may be given label A, there may still be a possibility of configuring the product that suits label C. What *configurability* is there? How is the *transparency* within the system? I will describe this deeper in the following subsections below.

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 Cambridge Dictionary, *"transparency"* is defined as: *"the characteristic of being easy to see through"* [46]. This means that we want the system to be as easy as possible to look through. We can to some extent say that the privacy may drop if the transparency is lowered. In order to maintain the privacy, the user should be able to "see right through" the system. One can compare transparency of a program/system to open-source programming. The vendor should not feel that the system need to "hide" anything, rather show

it directly to the end-user. Transparency substantiates the second element for measuring privacy, namely controlled processing. It is desirable that the vendor clearly describes the purpose of both each function and data that is collected.

4.3.2 Configurability

Another aspect to evaluate is how the *"configurability"* of the system. As mentioned earlier, a system can both be classified to privacy label A & C if we just focus on how the data is being treated. The aspect of configurability totally changes this way of classifying each label. In order to be classified to label A, one will expect that the user is able to configure the product/system in a way that makes the product/system fulfill all the different criteria for label A. 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 each person, maybe based on their role in the society.

4.4 Summary

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

As discussed, the actual value of privacy for each person can vary and needs to be seen as *subjective*. We therefore concluded that the privacy measurement can't be based on how a certain *persona* 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. This findings substantiate the choice (*Multi-metric vs Privacy Quotient*) of the method even more.

The vendors are by this privacy label regulation being held more responsible for how the privacy of each user is ensured. As mentioned, the vendors are already imposed to follow the demands mentioned in GDPR. This regulation very much substantiates the concept of *controlled collection*, as it focuses on how the data is being stored. It also substantiates the concept of *controlled processing*, as it demands the vendor to clearly specify which data is being stored as well as how the data is being treated. It was also mentioned the new and upcoming *ePrivacy* regulation. This regulation focuses on the confidentiality of the data that is being processed on the vendors platform. The Privacy labeling should also cover this area from the vendor's perspective, as confidentiality breach may affect the privacy of the user. This may apply to both element one and three (*controlled collection* & *controlled dissemination*).

To summarize the chapter, we have covered which method that will be

used in order to translate the technical parameters to actual values. We have also found out that the labeling must be done with respect to the functionality of the product, set up against the four different elements for measuring privacy.

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

- This chapter substantiated one of the challenges pointed out in chapter 3, namely the need of a centralized database of privacy values. This will make the method more consistent as we will exclude large variations is privacy values from expert to expert.

- The chapter also points out that both *transparency* and *configurability* should be taken into consideration when measuring privacy of a product. This would mean that good configurability should be weighted in a positive way. This holds for transparency as well. Looking at a system that processes sensitive data and presents high configurability for the end-user, we can expect the outcome result of the Multi-metric method to vary on quite a large scale. This would because the end-user is able to configure his/her profile to either full privacy, no privacy or somewhere between. Assuming that all configurations are set to private by default, this system should be evaluated in a positive way. The outcome results from the Multi-metric will then vary quite a bit. This would mean that if the average of all scores are somewhere in the middle (40/50/60), this system should be presented a "top score". As of now, there is no clear guidelines regarding this aspect of the method.

Part II

Use scenario

Chapter 5

Applying the Multi-Metric method

5.1 Description of the different subsystems

In this chapter I will apply the multi-metric function. The goal of doing so, is to use the result from the method to set a privacy label. When applying the method, we firstly need to point out both the overall system and also the different subsystems. In this case, the overall system will be the platform/brand *Polar*. This overall will be a combination of two subsystems. These subsystems will be *Polar Flow* and *Polar M600*.

Polar Flow is, as pointed out earlier, the platform that combines and evaluates different health data. In order to evaluate the privacy of the system, both configurability and transparency will be two important elements. This is because Polar Flow is an online accessible platform which offers a lot of different functionalities, based on the users training data. Given that the privacy configurability of the service is not maintained, this service may have the potential of causing great damage for a specific user (e.g. monitoring by unauthorized personnel).

Polar M600 on the other hand, will work as the collector of these data's as well as transmitting them to Polar Flow. When applying the method for this sub-system, we will need to have a look at the physical dimension of the watch. We will also have to look at the four main elements for measuring privacy, especially *Controlled dissemination* and *Controlled collection*.

One can argue that *Android Wear* should have been chosen as a subsystem as well. This is because it is possible to use the Polar M600 regardless of Polar Flow. I've chosen to not evaluate this, simply because I will go deeper into Polar M600 and Polar Flow. My suggestion is that a stand-alone project looks deeper into the flow between Polar M600 and Android Wear.

5.2 Scenarios

Below, I will present four different scenarios when using the Polar M600/Polar Flow. All the scenarios will have a different view on privacy. I've chosen to create four different scenarios, simply because they describe the different ways to use the system with respect to privacy. Each scenario will have 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 are ignoring these two elements, we are going to leave the fields for *"S"* and *"D"* blank.

5.2.1 Scenario 1 - Extreme privacy awareness

Bob is a privacy aware person which wants to ensure that all his sensitive data is being treated in a safe manner. Although he is extra aware of how his sensitive data is being treated, he still wants to use the functionality of the watch. He therefore chooses to use the watch stand-alone without connecting it to the Polar Flow web service. This choice may lead to limited functionality seen at the system from an overall perspective, but Bob is still able to monitor his training sessions within the watch++. Since Bob chooses not to connect the watch to any external endpoint (e.g. smartphone), he also chooses to deactivate all wireless connection options directly to the watch (e.g. Wi-Fi and Bluetooth). He also chooses to set a screen lock on the watch in order to unlock it as well.
SPD_{Goal} = (S, 90, D)

For this scenario, we aim for a privacy goal at 90. This is a quite high goal, but we would expect that leaving all the data within the watch will ensure our privacy at the highest possible level. The possibility of physical stealing data is the largest drawback, but since the watch offers the possibility of setting a pin code on the watch one can expect privacy will be safeguarded. Since the possibility of connecting the watch via Wi-Fi/Bluetooth is disabled, we assume that no unauthorized personnel are able to connect/eavesdrop data within the watch.

5.2.2 Scenario 2 - Medium privacy awareness

Bob is medium aware of his privacy. This means that he wants to use most of the functionality of the overall system, but at the same time take his privacy into consideration. He therefore chooses to synchronize all his data from the watch directly to Polar Flow on his smartphone via Wi-Fi/Bluetooth. By doing so, he has the possibility of using most of the functionality the overall system offers. As pointed out, Bob is medium aware of his privacy which means that he configures Polar Flow to the highest privacy setting. This means that all of his data is to be private and out of reach for anyone within the Polar Flow community. He also chooses to set a screen lock on the watch in order to unlock it as well.
SPD_{Goal} = (S, 80, D)

The privacy goal of this scenario ends up at 80. The reason for this, is that Bob chooses to synchronize his data with Polar Flow, which extends the attack surface and also the value chain for where the data is 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 the privacy settings are set to private. Another aspect which occur by synchronize the data, is the possibility of eavesdropping the data that is being transmitted. Bob opens for a connection to a third party, which automatically will decrease the privacy. Again, one should expect both Polar M600 and Polar Flow to handle this transmission in a secure way.

5.2.3 Scenario 3 - Regular privacy awareness

Bob is what one can name a *"regular person"*. The statement *regular person* means that he uses most of the functionality that comes with the overall system. In order to do so, he chooses to synchronize all his data that is captured with the watch directly to Polar Flow via his smartphone. This means that all of his data is stored within the overall Polar system. Furthermore, he chooses to open the possibility of sharing his data with his friends. This is a privacy option that is given by Polar Flow which means that people who Bob accepts as his friends, are able to monitor all his training results that is being uploaded to Polar Flow. He also chooses to join a public group within the Polar Community which offers the possibility of sharing training sessions with all the people within the group.
SPD_{Goal} = (S, 60, D)

Bob receives a privacy score of 60 for this scenario. The reason for this score is that he gives insight to all of his private monitored data to his friends (accepted by Bob personally). By doing this comes also an ethical/social question, namely the trust of sharing this information with people he knows. Most likely none of his friends will abuse this information, but there is a possibility for a malicious person to attempt a *social engineering* attack. This may be conducted by pretending to be one of his friends and then receive an accepted follow request. Another element to consider is Bob's choice of joining a public group. By joining such a group, he reveals all data that is being uploaded by himself to the group. This means that anyone who joins the group is able to stay there as spectator and monitors all the activity. Such a spectator is then able to even *"relive"* the training session. He also leaves the possibility of eavesdropping by transmitting his data between the watch and the smartphone.

5.2.4 Scenario 4 - No privacy awareness

In this scenario, Bob chooses to fully disclose all his data on a public level. He sets all his privacy settings to public, which means that basically everyone is able to have a look into all his training data that is being synced with Polar Flow. In other words, people registered within the Polar Community does not need an acceptance from Bob in order to monitor his data. They can directly look into them via his profile. Furthermore, he

chooses to join a public group and regularly posts new training sessions to the group. This means that he is able to fully use the functionality of the overall Polar platform.
SPD_{Goal} = (S, 30, D)

Bob receives a score of 30 for this approach. This scenario aims to utilize the functionality of Polar Flow and the Polar M600 as much as possible. With that said, the privacy will automatically drop. This is because Bob chooses to fully disclose all his personal data monitored by the watch. By doing so, he opens the possibility of using the overall system at its most, but also leaves himself in a harmful position. This is because anyone that is registered within the Polar Community are able to fully monitor all his data that is being uploaded, even relive them. This may lead to *profiling* of Bob by a malicious person. By regularly watching his training behavior over some time, a malicious person may be able to map and predict where Bob is at a specific time into the future. This information can be used for many different malicious purposes. His privacy score also drops because he joins a public group and regularly posts training data, which broadcasts his public profile to all the people within the group.

5.3 Device configurations

Below, I will present *8* different device configurations. These configurations are made with respect to the four different scenarios. This means that each scenario is assigned two different configurations.

- **Conf. A:** Screen lock is done by a custom drawn pattern on the watch. Bluetooth is turned off. Wi-Fi is turned off.
- **Conf. B:** Screen lock is done by a custom 6 digit PIN code. Bluetooth is turned on. Wi-Fi is turned off.
- **Conf. C:** Screen lock is done by a custom 6 digit PIN code. Bluetooth is turned on. Wi-Fi is turned on. Automatically synchronize data to Polar Flow via app. Privacy of 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.
- **Conf. D:** Screen lock is done by a custom password. Bluetooth is turned on. Wi-Fi is turned on. Automatically synchronize data to Polar Flow via app. Privacy of 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.
- **Conf. E:** No Screen lock. Bluetooth is turned on. Wi-Fi is turned on. Automatically synchronize data to Polar Flow via app. Privacy of profile is set to followers. Privacy of sessions are set to followers. Privacy of activity summaries are set to followers. Joins a public group, but does not publish. Manually confirms new followers.

- **Conf. F:** Screen lock is done by a custom 6 digit PIN code. Bluetooth is turned on. Wi-Fi is turned on. Automatically synchronize data to Polar Flow via app. Privacy of profile is set to followers. Privacy of sessions are set to followers. Privacy of activity summaries are set to followers. Joins a public group and regularly publishes to the group. Automatically confirms new followers.

- **Conf. G:** Screen lock is done by a custom 6 digit PIN code. Bluetooth is turned on. Wi-Fi is turned on. Automatically synchronize data to Polar Flow via app. Privacy of profile is set to public. Privacy of sessions are set to public. Privacy of activity summaries are set to public. Joins a public group, but never publishes. Automatically confirms new followers.

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

5.4 Metrics for privacy evaluation

Below I will present a metric for each component that is to be evaluated in the multi-metric method. Each metric contains a set of different parameters (e.g. On & Off) which have their own criticality. The criticality of a parameter represent how critical this parameter is related to privacy for the specific metric. Furthermore, each metric contains a weight. A weight represent the impact this whole metric would have on the overall system. An example may be sharing personal data with friends. If one choose to share personal with other friends, this may have a higher criticality value rather than not sharing the data. This metric will also have an impact of the overall system and the value that is given should reflect this impact. The values that is given is always within the range of 0 - 100, where 0 represent as low as possible impact and 100 represent as large as possible impact.

5.4.1 Bluetooth

When turning Bluetooth on (on Polar M600), the watch will be able to connect to Polar Flow on a smartphone within a short range. It will constantly broadcast itself within its range. This metric offers two different parameters, namely on and off. Assuming that Bluetooth is turned on, our privacy will automatically be more exposed as the device will broadcast itself and let anyone within a close distance know its presence. Still, it should not be given any higher criticality than *40* as connection needs an authorization from the device as well as the distance range is quite small. When Bluetooth is turned off, we can assume that the privacy can only be exploited via a physical attack. This is because the method only focuses

on one metric at a time and does not consider the other metrics (like Wi-Fi). Still, it should have some criticality as the data is stored locally as 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 substantiated with the fact that Bluetooth only offers connections within a close range, closed transmission channel and the need for authorization when connecting.

Bluetooth	C_p
On	40
Off	5
Weight	10

Table 5.1: M1 - Bluetooth metric

5.4.2 Wi-Fi

By activating Wi-Fi on the Polar M600, the watch is able to talk directly to the Polar Flow app on a smartphone within a larger range than via Bluetooth. When using a Wi-Fi connection, the watch constantly broadcast itself across the network. This metric offers two parameters as well (on and off). To some extent, this metric is quite close to the metric for Bluetooth, but exposes the privacy of the user a bit more. This may be substantiated by the fact that activating Wi-Fi broadcasts within a larger area and is 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 the weight of *25*, we will get a more precise overall result. When turning it off, the same holds as for Bluetooth. The fact that the data is stored locally will offer the potential of a physical attack where the privacy may be dropped and is the reason for the criticality value of *5*.

Wi-Fi	C_p
On	45
Off	5
Weight	25

Table 5.2: M2 - Wi-Fi metric

5.4.3 Screen lock

By setting up a screen lock (on the Polar M600), the user lowers the possibility of 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 PIN code [6]. Based on their research, they have found out 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)." Furthermore, a password is considered more secure as the different possible combinations increase dramatically.

The impact of a physical attack may be critical when considering the privacy of a user. If no screen lock is set, the possibility of leakage of 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 higher, but the fact that a *physical* attack needs to be conducted should be taken into consideration. The possibility of such an attack appearing is quite lower than for example a cyber attack. Looking at a 6-digit PIN code, we've set a criticality of *20* which puts it in the middle three different authentication mechanisms. Such a PIN offers both a quick way of entering the watch as well as a medium security level related to authentication. Furthermore a drawing pattern receives a criticality of *25*. This value states that such a solutions is considered quite more unreliable than for example a custom password. Setting a password gets the criticality value of *10* which reflects the strengths in such a solution. At the end of the metric, we weight this with the value of *40*. The reason for this value is, as mentioned, a physical attack would need to be conducted. Given that the object is a watch, the possibility for such an attack occurring drops quite a bit.

Screen lock	C_p
Password	10
Pattern	25
PIN	20
No screen lock	70
Weight	40

Table 5.3: M3 - Screen lock metric

5.4.4 Automatically synchronization

By enabling automatically syncing to Polar Flow, the watch will automatically sync all new training sessions that have been recorded. This uppers the possibility of eavesdropping/data leakage, but one should expect that Polar transfer these data in a secure way. This metric offer two parameters as well, namely on and off. By automatically synchronizing training data to the app (Polar Flow platform), the user instantly looses control of the data. The user manually need to activate this synchronization. By giving this metric the weight of *60*, it clearly states that the user gives up a lot of his/her privacy to Polar. One should assume that Polar uses these data in a safe manner and that the user have the full right to choose how they shall be processed. When turning this synchronization on, we give it a criticality value of *50* and may be explained in the same way as the weighting of the metric. When turning synchronization off, the user is only vulnerable for a physical attack (assuming that Bluetooth and Wi-Fi is turned off). This

will leave us in the same situation as turning off Wi-Fi/Bluetooth and will therefore give the same result, namely *5*.

Automatically syncing to app	C_p
On	50
Off	5
Weight	60

Table 5.4: M4 - Automatically synchronization metric

5.4.5 Automatically confirmation of new followers

When applying the function of automatically confirming new followers, the privacy drops quite a bit. Given that this function is applied will basically offer anyone to be able to follow the respective profile. The privacy of this must be seen in context with the privacy settings that have been set for the profile as well. If a user chooses to automatically confirming new followers, the user will be in a quite similar situation as setting his/her privacy settings for his/her profile to public (mentioned in table 5.14). Assuming that this is activated, the user have no control of whom is able to look at his/her data (this assumes that the user have configured the privacy of his/her to be "Followers"). Privacy is drastically dropped by activating and result in the criticality value *75*. A representation of how this work is presented in the images 5.1 (before following) and 5.2 (after following).

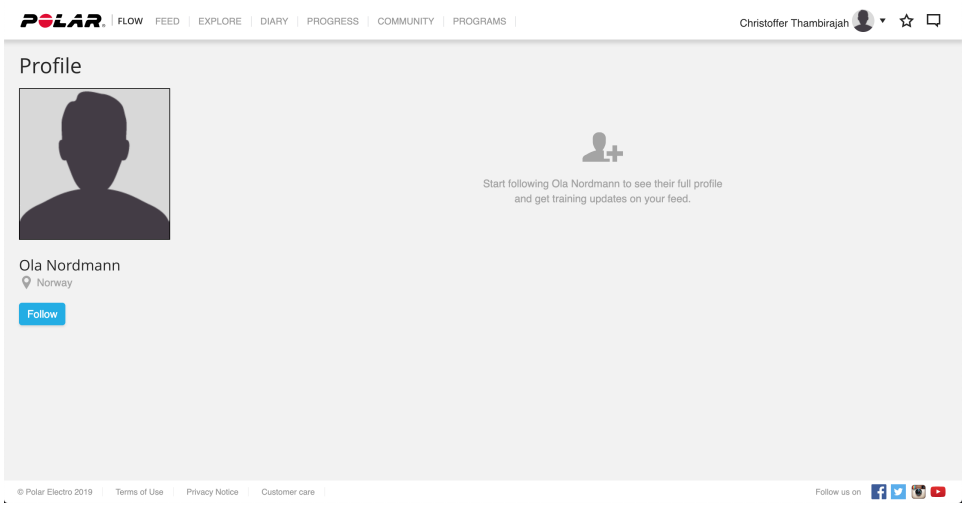


Figure 5.1: Polar Flow before being following

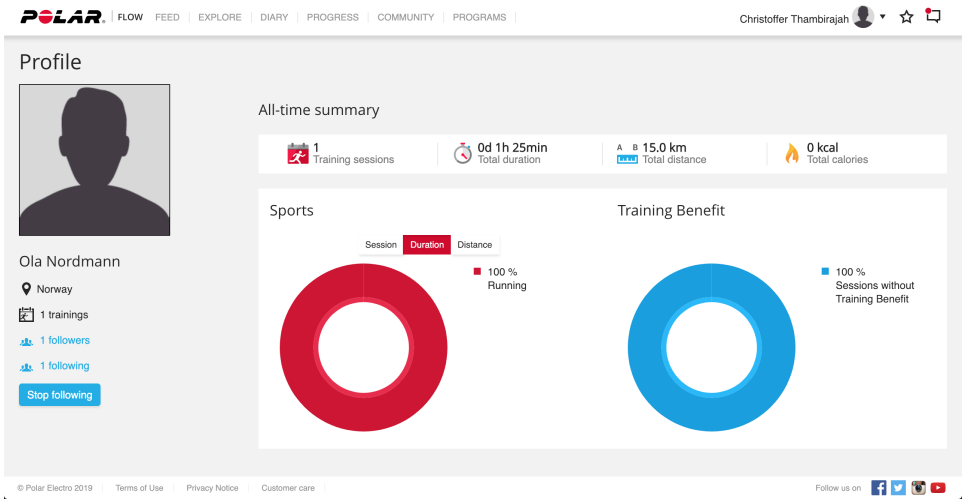


Figure 5.2: Polar Flow after being following

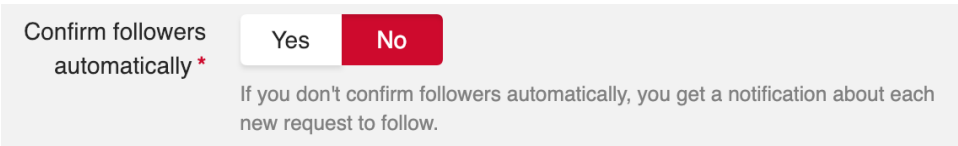


Figure 5.3: Configuring privacy for automatically confirming new followers

Turning this off would leave the user in the control of whom he/she wants to share the data with. Still, there is a possibility of an attack where the user for example think he/she knows who tries to follow him/her and chooses to accept while this actually turns out to be someone else. Given such possibilities, this option receives a criticality value of *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 - Automatically confirm followers metric

5.4.6 Privacy of profile

By giving permission to let other profiles have insight to one's private profile, one disclose basic information. This do not give access to synced training sessions. Both the parameters *public* and *private* reflects the same as *on* and *off* and therefore receives the same values, namely *75* and *5*. The reason for saying that public have the same criticality as "on" in the metric above (table 5.5) is that the actual functionality of automatically accepting

new followers (assuming privacy of profile is set to followers) 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 within the middle as it limits the user to manually choose who he/she 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.

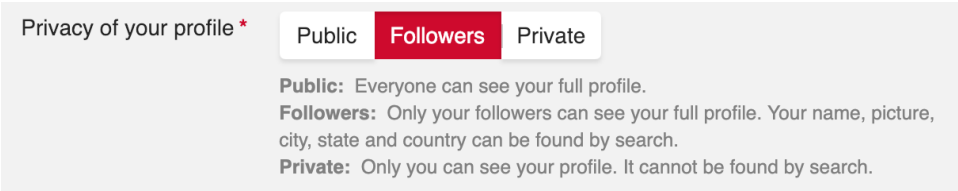


Figure 5.4: Configuring privacy of profile

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

Table 5.6: M6 - Privacy of profile metric

5.4.7 Privacy of sessions

It is possible to choose which privacy setting one would like to have on all training sessions that is being synced with Polar Flow. Given that a user chooses to set this to *"Public"*, the user fully disclose all training sessions that is being synced. This also holds for the setting *"Followers"*, but it is restricted to accepted followers by the user. Private means that no one except the user itself have access to the data. As stated, this function offers many of the same features as *Privacy of profile*, but the main difference is the training data that is being presented. When configuring a profile to be public, one chooses to disclose basic information. When configuring the privacy of sessions to being public, one chooses to fully disclose all training data publicly. That is the reason why we should increase the criticality value by 5 compared to the metric presented in table 5.14. The same holds for the parameter followers. The result then becomes *80* and *45*. Regarding the parameter private and the weight, it is sufficient to use both *5* and *70* since the critical parameters are increased (public and followers) and will therefore have sufficient impact on the overall result.

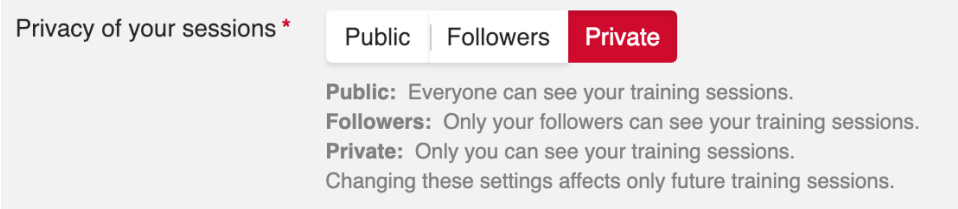


Figure 5.5: Configuring privacy of sessions

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

Table 5.7: M7 - Privacy of sessions metric

5.4.8 Privacy of activity summaries

There is a possibility of disclosing activity summaries. This means that a user is able to disclose activity summaries for either a specific crowd (*"Followers"*) or everyone (*"Public"*). Such an activity summary may be seen in each users *"Feed"*. For this metric, we need to address the fact that disclosing this information publicly gives everyone full insight to each training summary, which may be very sensitive information (e.g. pulse, route++). Given this precise information, one should increase the criticality values as well as increasing the weighting. Both the parameters public and followers are then assigned the values *85* and *50*. As pointed out for metric M7 in table 5.7, it was sufficient to just increase the criticality while letting the weight 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 to *80*. The option for leaving the privacy to private will relate to the same conditions as metric M7, M6, M5 and M4.

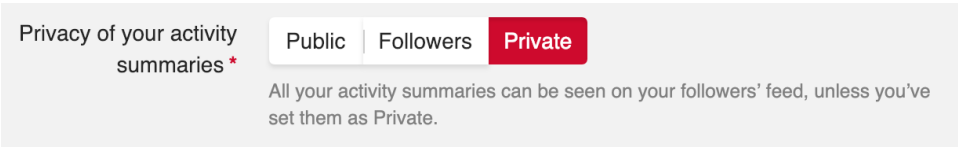


Figure 5.6: Configuring privacy of activity summaries

Privacy of activity summaries	C_p
Public	85
Followers	50
Private	5
Weight	80

Table 5.8: M8 - Privacy of activity summaries metric

5.4.9 Groups

By joining a group, a user is able to both post training sessions and monitor other training sessions by other members. When posting session to a group, one fully disclose this information to everyone within the group, independent of the privacy setting of ones profile. The reason for giving a criticality of *80* when regularly publishing sessions is the fact that the user does not necessarily know who is within the group. There is a slight possibility that distribution of a profile that regularly publishes within a group might go viral and ends up in the hands of people whom the user not necessarily wishes to be in direct contact with. Some of this holds for the second parameter as well (joining, never publishes sessions), namely the power of distribution/marketing. The criticality is assigned to *40*, which is half as high as if he/she would have regularly published sessions. The reasoning behind this is, as mentioned the power of marketing. If a user is within a group, but never publishes any sessions, he/she shows presence by being a spectator and therefore increases the possibility of unwanted entities trying to make contact/monitoring his/her profile. What information such an entity will be able to collect would be relative, based on the other metrics like M8, M7 and M6. Not joining receives the same result as the other metrics (except *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 in any case give away valuable information. This may be because he/she chooses to publish data or it can be just monitoring the group. By just monitoring the group, the user discloses his/her basic information to the crowd within the group.

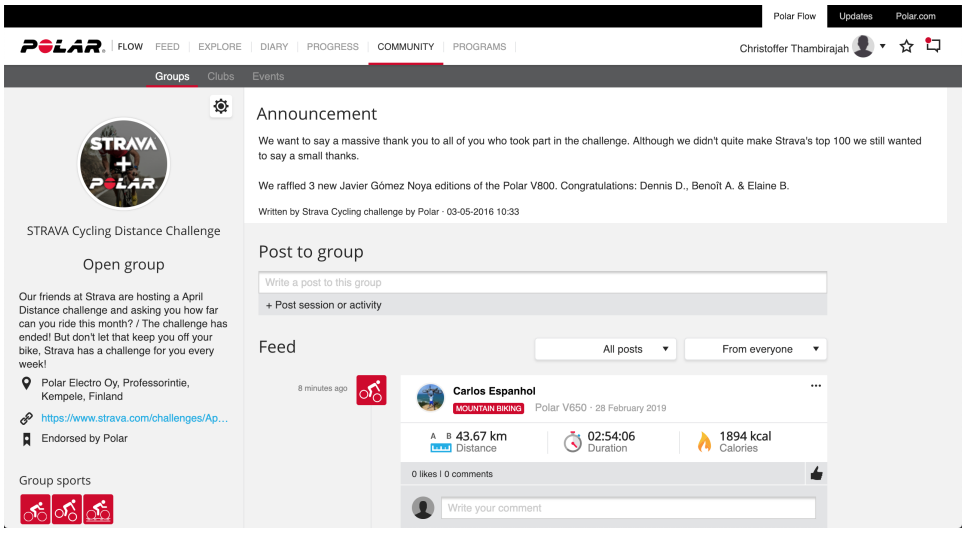


Figure 5.7: Presenting how a public group look like

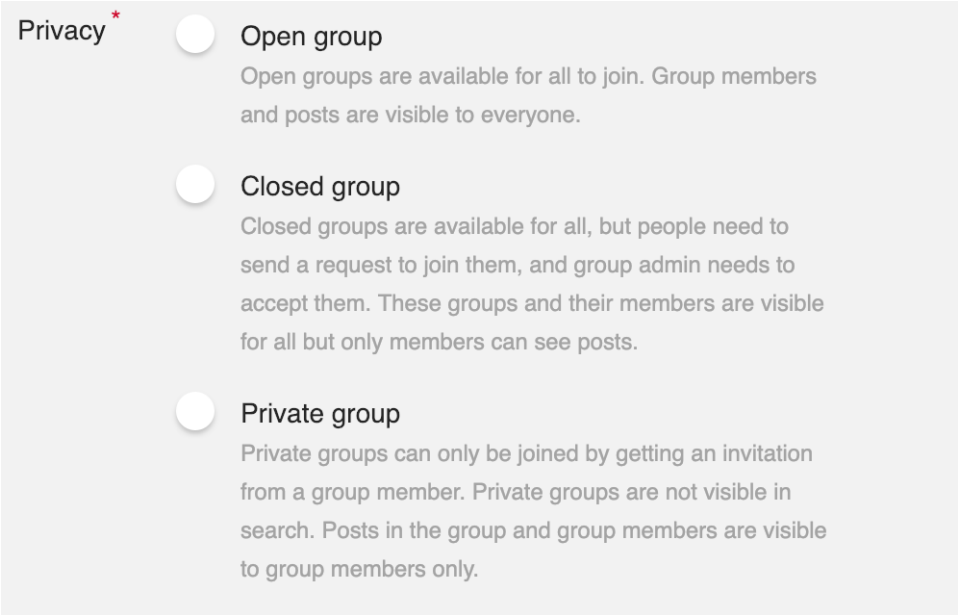


Figure 5.8: Privacy settings when creating a group

Groups	C_p
Joining (regularly publishes sessions)	80
Joining (never publishes sessions)	40
Not joining	5
Weight	65

Table 5.9: M9 - Groups metric

5.5 Privacy assesment results

When finalizing the metrics, there need to made a table with respect to the metrics and configurations. Each metrics may be represented as *"M1, M2, M3..."* as well as the criticality *"C1, C2, C3..."* (this thesis considers only privacy which is the reason for only expressing *"P"* which stands for Privacy for each metric and criticality). These values are presented with respect to each configuration and its respective numbers. This would mean that both configuration A and B will receive values from both M1 and C1 (given that M1 and C1 is representative for configuration A and B). Each configurations will then have a complete set of values for each metric with the criticality represented. For this specific evaluation, the different metrics are presented as following:

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

Once these values are placed into the table, the function (Root Mean Square Weighted Data) may be applied (function explained in equation 4.1). This function will return a result for each configuration. The result in what's called *"Actually Criticality"*. In order to receive the final result, we need to subtract the Actual Criticality from 100 (to represent it in the correct way). The result that is provided may then be set up against the original goal for the scenario that was set before applying the method. A final result of 100 will then be considered as *"perfect privacy"* whilst a result of 0 is considered *"no privacy"*. The configurations that is used when applying the method may be found in section 5.3.

5.5.1 Result - Scenario 1

Below, we're 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 expect that the system safeguards the privacy as Bob chooses to not synchronize the watch with any third parties and also sets a screenlock.

Criticality										**SPD(P)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	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: SPD_{System} for Scenario 1

5.5.2 Result - Scenario 2

This scenario aimed to be "medium" privacy aware. This would be that Bob chooses to synchronize his data with Polar Flow, but wants his privacy to be safeguarded. He therefore sets his privacy settings to *private*. Below, we're able to see exactly how the overall system reacts to such a privacy attitude.

Criticality										**SPD(P)system**	
	C1	C2	C3	C4	C5	C6	C7	C8	C9		
											Scenario 2
Metric	M1	M2	M3	M4	M5	M6	M7	M8	M9	Criticality	SPD(S, 80, 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	22	77
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 5.11: SPD_{System} for Scenario 2

5.5.3 Result - Scenario 3

As of this scenario, Bob aims to be a so called "regular person". This would be synchronization of all data from the watch unto Polar Flow. He furthermore wants to share these data with his friends. The results below presents how the overall system reacts to such an approach with respect to the SPD_{Goal}.

Criticality										**SPD(P)system**	
	C1	C2	C3	C4	C5	C6	C7	C8	C9		
											Scenario 3
Metric	M1	M2	M3	M4	M5	M6	M7	M8	M9	Criticality	SPD(S, 60, 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	22	77
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 5.12: SPD_{System} for Scenario 3

5.5.4 Result - Scenario 4

For scenario 4, Bob chooses to be as transparent as possible. He chooses synchronize all captured data by the watch directly unto Polar Flow and leave them all public for anyone to monitor. The results below presents how the system reacts to this.

Criticality										**SPD(P)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. 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	77
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 5.13: SPD_{System} for Scenario 4

5.6 Evaluation of results and critical assessment

5.6.1 Evaluation - Scenario 1 (according to table 5.10)

The SPD_{Goal} for scenario 1 was set to SPD(S, 90, D) which is quite a high goal. This scenario primarily aims at passing configuration A and B are made to fit this specific scenario. The results shows us that it holds for both configuration A, B and C which passes, configuration D end up as a

medium while the rest fails. This can be justified by the fact that the two first configurations aims to substantiate scenario 1. In other words; we would expect them to pass. Furthermore, the explanation for configuration C passing and configuration D gets a medium may be justified by the fact that they tempt to reflect scenario 2 which is somehow quite close to scenario 1. Both these two configurations and the rest are in a way not to be seen in accordance with scenario 1 as all of them synchronize captured data with either just a smartphone or Polar Flow as well. The fact that configuration E and all the way down to H fails may not be surprising as they all disclose data to external personnel. On the other hand, it is uplifting to see that configuration C and D are within such a close range from the goal, even if they synchronize data. If we look at all the results, we get an average score of 60. By putting this result directly up against our goal, this scenario would fail. When taken into consideration the concept *configurability*, one should not only look at this result as Bob chooses to configure the Polar M600 not to synchronize any captured data. Then it would be more correct to just look at the results of configuration A and B which would give us an average of 83, which states *passed* for the scenario.

As a short evaluation for scenario 1, we can see that the method shows almost what we expected as an outcome and may be classified as *passed*.

5.6.2 Evaluation - Scenario 2 (according to table 5.11)

Looking at scenario 2, we sat a goal of SPD(S, 80, D). This scenario primarily aims at passing configuration C and D are made to fit this specific scenario. Looking at the results, we can see that 3 configurations passes, while one of them ends up as a medium and the rest fails. Both this and scenario 1 have exactly the same amount of passed/medium/failed, which may tell us that an overall evaluation of the system may lay somewhere around these goals. Both configuration C and D passes, which is as expected since they very closely represent the scenario. It is also uplifting to see that the results for configuration A and B ends up in quite a close range from the expected goal for scenario 2. This tells us that the privacy of the user is maintained even though Bob chooses to synchronize his data, as long as he chooses to keep them private.

Looking at the result with a bird-eye look, we see that the average is a score of 60. By setting this up against the overall goal, we end up with a difference of 20 which results in *medium* according to the method.

5.6.3 Evaluation - Scenario 3 (according to table 5.12)

This scenario had an overall goal of SPD(S, 60, D). This scenario primarily aims at passing configuration E and F are made to fit this specific scenario. After applying the method, we see that one of the configurations passes (configuration E), while two of the others gets medium and the rest fails. This shows that configurability of the system is quite good as this scenario not necessarily focuses on privacy. Configuration E and F are meant to apply to this scenario, but they seem to be a bit out of range. This may

be explained by the criticality of metric 9 (publishing within groups). Assuming that a person regularly publishes training sessions into a group with unknown people will automatically leave them more vulnerable.

When comparing the overall goal of the scenario with the average score (60), we can see that the scenario clearly passes.

5.6.4 Evaluation - Scenario 4 (according to table 5.13)

The results of scenario 4 seems to be as expected as both configuration G and H passes. The overall goal for this scenario was set to SPD(S, 30, D). This scenario primarily aims at passing configuration G and H as these configurations are made to fit this specific scenario. Both the configurations are quite on point and we can therefore consider them to be quite representative for the scenario. At the same time, this shows that the overall system has a large variation of privacy configurability.

The rest of the configurations fails except configuration F. We should expect them to fail as scenario 4 aims to have *"no privacy awareness"*. Even though configuration F is presented as a medium result and it is quite interesting to see that it falls within a range of *15* from the original goal. This is because the configuration is set to only allow followers to view the training data. It may be justified by the choice of automatically accept new followers.

In some way, one can argue that the choice of automatically accept new followers should have the same result as configuring a profile to be public if the privacy of the profile is set to followers. One way to solve this may be by introducing more parameters within the metric *"Privacy of sessions"* and *"Privacy of profile"*. One interesting parameter that could have been introduced is the criticality of setting a profile to followers while having set the profile to automatically accept new followers. This value should somehow have fairly the same impact as setting the profile to public.

An argument for not introducing another parameter may be because of the marketing/distribution a profile gets by configuring it to be public. If a profile is set to be public, it is much more available for the Polar Flow community rather than a profile that is set to followers. This may be proven by looking at the function Explore which will present the session results from each public profile. In order to locate a profile that is set to followers, one would specifically need to look it up. Based on this argument, one can say that such a result that is presented for configuration F with respect to scenario 4 is sufficient.

5.6.5 Evaluation of the measurement method

The multi-metric method is very generic and adaptable which makes it very handy to apply to any system. It gives a good bird-eye look at the overall system whilst it also evaluates the core functionalities of the system. Looking at the results that is produced from the method, it might be possible to some extent to use it in order to classify a privacy label. The

reason for not using this alone as a foundation for classifying the label is the concepts of configurability and transparency, as discussed.

Another important aspect to consider when evaluating the method, is the need for a centralized database of criticality and weight values. The method clearly states that these values should be pointed out by an expert within the field which tends to be quite correct. The issue with this method appears when this kind of database is non-existing. If a set of ten people was to look at the criticality for the metric of for example *Bluetooth*, the probability of getting more than one common answer is quite likely. This means that the results produced by the method would vary from person to person after applying it.

In order to escape this issue, there should be created a centralized database by some public authority with specialist in each given field. E.g. should the criticality of setting a profile public within a community like Polar Flow have a specific value based on all the information that is stored within the system. If a database like this is provided, the method would from my point of view be of interest when calculating a privacy label. Evaluation of the method will be further discussed in chapter 6.

5.6.6 Evaluation of the parameters

When choosing parameters for a metric, one should choose as specific parameters as possible in order to get the best possible result. When introducing more parameters, the complexity of the method grows linearly. 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 loads of functionality. To keep the complexity down, one would need to make some general parameters. This should also be the case if such a method is being used for measuring the privacy of a product. There would have been a need to make general parameters that applies to a given product within a specific field.

As of this assessment, I chose to introduce 4 different metrics related to the watch itself, while introducing 5 metrics for Polar Flow. The metrics for the watch may be seen as more generic metrics as any smartwatch on the market will to some extent "have the same functionality". The functionality of a smartwatch may of course differ from one to another, but most of them aim to deliver much of the same functionality, namely monitoring of its user and present this information in a nice way. Many of these watches offers a connection to a cloud where the data is being treated. This means that the user often have two choices; shall the watch distribute the data to the cloud? Or shall it keep it locally on the watch? Based on this assumption, I chose to include the metrics *Bluetooth* and *Wi-Fi*. These are very generic parameters and drastically changes privacy of the device when turned on vs off. Furthermore, I chose to include the possibility of setting a *Screen lock*. This is an essential parameter to include as this may influence the weight/criticality of Bluetooth and Wi-Fi. Assuming that there is no possibility of setting a screen lock, the smartwatch automatically becomes more exposed even if both Wi-Fi and Bluetooth is turned off. As a

last metric for the smartwatch, I included the possibility of configuring it to *Automatically syncing to app*. This would mean that the user is actually able to have Wi-Fi/Bluetooth turned on, but manually synchronizes a training session to the app. If the user chooses to automatically synchronize data, this would leave him more exposed. This can be explained in many ways, but some of them are that he firstly uploads everything (which exposes more data than he might "need" to expose). Secondly, he has no control of when/where this data is being synchronized meaning that he can be synchronizing data on the subway as well as home in his kitchen. Doing such a synchronization on a public place will naturally expose the privacy more.

Looking at the metrics for Polar Flow, the parameters need to be a bit more specific, but still applicable for other systems. Three of the metrics that were introduced have a close relation, namely *Privacy of profile*, *Privacy of sessions* and *Privacy of activity summaries*. All of these have the three same options (public, followers and private), but the criticality and weight may differ a bit. Leaving a profile public exposes 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 both privacy of sessions and privacy of activity summaries are configured to private, a malicious person does not necessarily get that much information from this alone. But this information may be exploited when using other services (e.g. Facebook). This thesis will not look beyond Polar Flow and Polar M600, but it is important to underline the value of just this basic information and what it is able to expose. Assuming that all these three parameters are configured to public, the user exposes information that may be of great interest for a malicious person. Assuming this, the privacy of the profile/person may be seen close to zero even though the user have consented. The value of such health data can very well be generally calculated when using this method for various products. The other two metrics are also possible to make quite applicable for other systems. Looking at the metric *Confirm followers automatically*, we can expect that at least basic information is being disclosed, all the way up to sensitive information like activity summaries. The last metric *Groups* may be quite critical if a user chooses to regularly publish training sessions as this may be exposed to unknown users. The reason for setting a criticality of 50 for just joining a group is the power of distribution. When just joining a group and acting as spectator, the presence of the user is being exposed.

In order to summarize the choice of the different parameters, we can say that it is important to locate specific, but also generic enough so that they are applicable to other systems. This is because we want to be able to use parameters/metrics of a more generic kind.

5.7 Sensitivity of configurations

As mentioned in section 4.1.3, the parameters should be set by experts within the field. The criticality for a parameter combined with a weight

is critical in order to get the correct result. This would also mean that the result may be quite sensitive. The sensitivity of a result can vary from one system to another. Given a lot 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 have a larger impact.

For this specific system, we can see that changing criticality for one specific parameter will not necessarily have a large impact on 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 metrics Privacy of profile, Privacy of sessions and Privacy of activity summaries we would have a chance of a larger impact. By introducing this, we should give it a criticality quite close to being public. The metrics could then have been presented like this:

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

Table 5.14: 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 5.15: 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 5.16: M8 - Privacy of activity summaries metric with extra parameter (*Followers with automatically accepting new followers*)

Introducing this for scenario 4, we could have received a result as presented below.

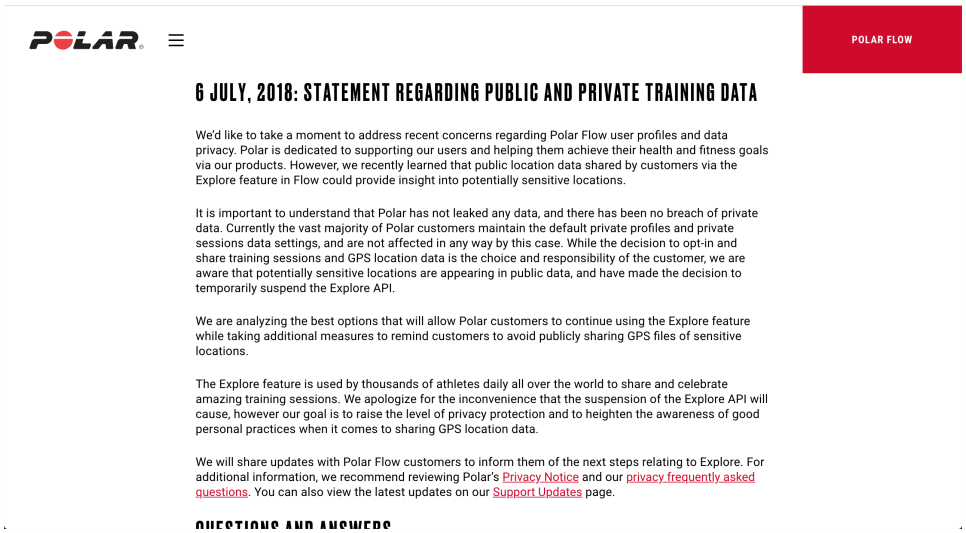
Criticality										**SPD(P)system**	
	C1	C2	C3	C4	C5	C6	C7	C8	C9		
											Scenario 4
Metric	M1	M2	M3	M4	M5	M6	M7	M8	M9	Criticality	SPD(S, 30, D)
	P	P	P	P	P	P	P	P	P		
Conf. F	40	45	10	40	60	70	75	80	80	66	34

Table 5.17: Hypothetical SPD_{System} result given an extra parameter

Here, we have updated metric 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/distribution of profile). We can see that the result changes quite drastically from *45* to *34*. This an indication of the sensitivity for each result and amplifies the importance of how the metrics are produced.

Another aspect that needs to be taken into consideration is the concepts of *configurability* and *transparency*. Given a system that varies greatly in results might indicate that the possibilities of configuring its own privacy quite good is present. The overall system Polar will fall under this as the results varies from 85 all the way down to 30 (a difference of 55). Given these possibilities, it would be logic to weight the overall system in a positive direction assuming privacy is set by default (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 taken into consideration. In the summer 2018 (6 July, 2018), Polar Flow temporarily suspended the function "Explore" [34]. This function was suspended due to the lack of firmness of their terms. As Polar states: *"It is important to understand that Polar has not leaked any data, and there has been no breach of private data."* Furthermore, their statement tells us: *"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 within Polar's overall system.



POLAR FLOW

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.

Figure 5.9: Polar Flow Privacy Statement after suspending Explore

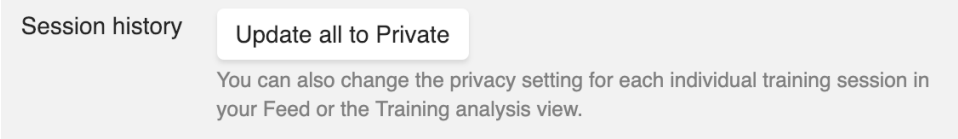


Figure 5.10: Function introduced that lets each user update all data (including historical data) to private

From my point of view, both of these concepts should be given a specific weight when determining a result. Such a weight should obviously be given by an expert within the field.

5.8 Sensitivity of weights and parameters

There are two ways to validate the precision of the multi-metric method. One is to introduce even more specific parameters in order to make it as precise as possible whilst the other validation may be to test the sensitivity of weights and parameters. Below, I will present 3 different test.

5.8.1 Test 1 - Sensitivity of weights

The first test focuses on increasing the weights by 20%. This would mean that the weights for the different metrics is presented as follow:

- **Bluetooth:** 12
- **Wi-Fi:** 30
- **Screen lock:** 48
- **Automatically sync to app:** 60

- **Confirm followers automatically:** 84
- **Privacy of profile:** 84
- **Privacy of sessions:** 84
- **Privacy of activity summaries:** 84
- **Groups:** 78

By doing so, we end up with a result as follow seen from *Scenario 1* (each column marked *blue* represents a change from the original result):

Criticality										**SPD(P)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 5.18: Hypothetical SPD_{System} when increasing each weight by 20%.

As we can see from the result, there are not that much of a change in the final result. 5 of 8 configurations receives a change. Looking at those who change, we can see that the criticality of *configurations C* drops from 22 to 21. This gives a positive SPD_{System} result at 79 (was 78). Next one is *configuration D* where the criticality drops to 25 (was 26) and then receives a positive SPD_{System} result of 75 (was 74). The criticality of *configuration E* drops to 44 (was 45) and ends up with a SPD_{System} result at 56 (was 55). All these three configurations receives a positive change.

When it comes to the three last configurations, we see that there is a negative trend. *Configuration G* increases its criticality to 67 (was 66) and the final SPD_{System} result ends up at 33 (was 34). Furthermore, the last configuration *configuration H* increases its criticality as well to 74 (was 73). This gives a negative SPD_{System} result of 26 (was 27).

The fact that configuration C, D & E receives a positive response in the final result may be explained by the increasing weights of metric 6, 7 & 8 (privacy of profile, privacy of sessions & privacy of activity summaries). These configurations have either configured these metrics to *private* or *followers* which is not considered that critical unlike *public*.

Looking at the two last configurations (G & H), we can see a negative trend. This is explained in the same way as for configuration C, D & E. Namely the fact that they configures their settings to be *public*.

5.8.2 Test 2 - Sensitivity of parameters criticality

The next test focuses only on changing the criticality values of each parameter. In this case as well, the values are increased by 20% and looks as follow:

Bluetooth	C_p
On	48
Off	6
Weight	10

Table 5.19: Hypothetical M1 - Bluetooth metric (increased by 20%)

Wi-Fi	C_p
On	54
Off	6
Weight	25

Table 5.20: Hypothetical M2 - Wi-Fi metric (increased by 20%)

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

Table 5.21: Hypothetical M3 - Screen lock metric (increased by 20%)

Automatically syncing to app	C_p
On	60
Off	6
Weight	60

Table 5.22: Hypothetical M4 - Automatically synchronization metric (increased by 20%)

Confirm followers automatically	C_p
On	90
Off	6
Weight	70

Table 5.23: Hypothetical M5 - Automatically confirm followers metric (increased by 20%)

Privacy of profile	C_p
Public	90
Followers	48
Private	6
Weight	70

Table 5.24: Hypothetical M6 - Privacy of profile metric (increased by 20%)

Privacy of sessions	C_p
Public	96
Followers	54
Private	6
Weight	70

Table 5.25: Hypothetical M7 - Privacy of sessions metric (increased by 20%)

Privacy of activity summaries	C_p
Public	100
Followers	60
Private	6
Weight	80

Table 5.26: Hypothetical M8 - Privacy of activity summaries metric (increased by 20%)

Groups	C_p
Public	96
Followers	48
Private	6
Weight	65

Table 5.27: Hypothetical M9 - Groups metric (increased by 20%)

When applying the multi-metric method with these updated criticality values, we get a result as follow:

Criticality										**SPD(P)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 5.28: Hypothetical SPD_{System} when increasing each parameters criticality value by 20%.

By increasing each parameters criticality value by 20%, we can see a clearly 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 rather than a precise weight.

Looking at all the configurations, it is notable to see that the difference between the original result and this hypothetical result increases almost linearly from configuration A (difference of 3) to H (difference of 15). Naturally, we will get a more negative result as the criticality is increased and is to some extent as expected.

5.8.3 Test 3 - Sensitivity of parameters criticality and weights

As a third and last test, we've put both test 1 and 2 together to see what impact there is when both the criticality and weights are increased by 20%. The results are as follow:

Criticality										**SPD(P)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 5.29: Hypothetical SPD_{System} when increasing each parameters criticality value and weights by 20%.

When combining test 1 and 2 together, we see that the criticality and SPD_{System} values are quite stable in accordance to test 2. This substantiate the fact that weights have quite a small impact on the overall score compared to criticality values. Still, one can argue that the function is more stable when applying growth on both the criticality and weights.

5.9 Summary

In this chapter, we have evaluated the overall system Polar with focus on the subsystems Polar Flow and Polar M600. There have been provided a short description of the two different subsystems with focus on their functionality. Furthermore, there was introduced four different scenarios. These four scenarios are meant to reflect the different ways it is possible to use the overall system with given specifications for each subsystem.

The first scenario starts off by being extremely privacy aware while the three other slowly but surely drops the focus on privacy. Scenario 1 and 4 is both extremes while a more "regular" person may relate to either scenario 2 or 3. Furthermore, there was introduced different configurations which may be seen with respect to the scenarios. The goal of the configurations was meant to reflect one scenario. This means that configuration A & B is meant to reflect scenario 1 while configuration C & D is meant to reflect scenario 2 and so on... The two first configurations starts off by being extreme privacy aware while the rests focus on privacy slowly drops (the focus changes from privacy aware to functionality aware). After defining the different 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 on the overall system based on the values from the scenarios, configurations and metrics. It turned out that the overall system was quite close to what we expected as an outcome which makes it a quite configurable system. The results vary all the way

from 30 - 85 which emphasizes this.

This chapter is a contribution to Q4 (*"Recommendations for measurable privacy?"*). The findings in the chapter are the following:

- Outcome of this chapter is the importance of good and precise privacy and criticality values. Section 5.8 shows the sensitivity of both weights and criticality and it clearly states that the method favors the criticality. My recommendation will therefore be to create general but specific enough privacy values so that they are sufficient for any system to use. A challenge may be the relation between specific enough values while still being generic.

Part III

Discussion & conclusion

Chapter 6

Discussion

6.1 Chapter 1

Chapter 7

Conclusion

The thesis have followed the *engineering design method* and is based on the following 4 research questions:

- **Q1. Which 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 rise of IoT on a world-wide size and which challenges that may introduce with respect to privacy (e.g. user profiling). The fact that IoT is introduced into more and more domains makes each persons privacy more and more challenged as they will share more and more sensitive data. This may be health related data which before IoT were quite hard for a malicious person to access. As of now, such information are more threatened as it is available in the digital world where it earlier only was available within a locked cupboard in the doctors office.

Chapter 3 answered the research question Q2 by pointing out that the desired method for measuring privacy would need to address general terms when it comes to specifying parameters to evaluate. The reason for this is the fact that each system can have quite specific parameters (data that is collected), but these needs to be translated to 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 of a centralized database for privacy values. The reason for doing so is to exclude the large variations that may appear between expert and expert. Furthermore, the chapter addresses that both transparency and configurability should be taken into consideration when evaluating each system. It is therefore proposed that an average result somewhere between the middle (40/50/60) should be considered a top score.

Chapter 5 answered the 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 Polar M600 by applying the Multi-metric method. It turns out that the method is quite stable when looking at both the weight and criticality together (assuming that the relation between these two are reasonable). Just kooking at the criticality, we saw that the result were affected in a larger manner relative to adjusting the weight by the same amount.

This thesis have covered the field of privacy issues related to IoT and addressed problems related to measurable privacy. The overall goal was to find and validate a measurement method for determining a Privacy label [40] so that it is possible to use this method on general terms for IoT products. There is presented different possible methods that might be applicable for this project, but this thesis focused on validate/disprove the Multi-metric method with respect to Privacy labeling.

In order to give a product a Privacy label, we want to look closely at each layer as well as the overall system. As an outcome of applying the Multi-metric method on Polar M600, we see that it receives the average score of *60*. With a score of 60, the product ends up with a medium plus score. Assuming that this average score reflects both high and low scores, we can assume that the system offers high configurability. This tells us that the user is both able to configure his/her profile to be highly privacy aware as well as no privacy aware. A conclusion of this will then be that an average score somewhere in the middle (40/50/60) with large variations in the results (from high to low) should be awarded with a top score.

The outcome of the thesis was to determine how a Privacy label could be measured on general terms and therefore tried to validate a measurement method for determining this. The Multi-method offers a great evaluation, both from a bird-eye perspective as well as for a single component point of view. The method have showed that it is robust and reliable on a large and commercialized scale, but may be unreliable on a smaller scale. This may be because of the privacy values chosen. The thesis suggests that there should be created a centralized database where such privacy values are stored. These values should be set by experts within each domain/field.

7.1 Open issues & future work

This thesis has carried out a careful examination of the Multi-metric method to see whether it is functional for determining a Privacy label. This work alone can not lay the foundation for determining which measurement method that is to be used for calculating a Privacy label. This method should be further tested on other products as well in order to have an even better foundation 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. [44] on creating a *"Privacy Quotient"* which may be used 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 the product it

self. 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.

Assuming that the 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 of privacy values. Such a work should be done in conjunction with public authorities as well as experts from each relevant field for the specific task (e.g. heart rate data might require a doctor).

As further testing and fine-tuning of a privacy measurement method continues, the definition of each level within a Privacy label should also be clarified as well as how many levels there should be. Current proposals for the different layers have been presented in section 3.5.2, but this range might be too big in my opinion.

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

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

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

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

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] *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/.

[30] 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.

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

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

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

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

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

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

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

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

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

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

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

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

[43] *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/.

[44] 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.

[45] *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.

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