CARDIFF UNIVERSITY SCHOOL OF COMPUTER SCIENCE AND INFORMATICS

Uncovering Personal Information in the Internet of Things

Final Report

13th May 2016

***40 Credits*: CM3202 One Semester Project**

***Author*:** Jamie Ide

***Supervisor*:** Dr. Alia Abdelmoty

Moderator: Dr. Padraig Corcoran

Abstract

People willingly provide their health, activity and sleep data for an incentive when participating in corporate well-being programs. Employers benefit from a reduction in insomnia, employee absences and health care costs, whilst also seeing an increase in workplace productivity. Individuals benefit from the ability to use the wearable devices to tailor specific goals, from fitness, to improving sleep quality, in addition to incentives (e.g. money or reduced health care costs). Whilst the data provides benefits for both parties, it can also be used for purposes which can compromise an individual's privacy. This paper therefore presents a study of privacy implications possible from the provision and collection of employee's health, activity and sleep data and the impact knowledge of identified privacy implications has on their behaviour.

The dimensions of the problem are analysed through research and taken trough a modelling process known as Soft Systems Methodology. This is then used to guide an analytical study of some representative data sets, utilising one of the most popular wearable fitness trackers distributed in well-being programs. The results of the research and data analysis provide a demonstration of the potential privacy inferences that can be derived from the health, activity and sleep data. Furthermore, a survey is designed to examine participant's awareness of collectable information, sharing preferences of collectable information and the level of concern and subsequent impact on behaviour regarding possible privacy implications derived from user data. Additionally, interviews are primarily utilised to identify feasibility of proposed requirements, prior to finalising a set. The final section provides a set of recommendations as to how users can protect their data, in the form of requirements, which have also been mapped against two market leaders to identify compliance.

The study indisputably confirms that users are unaware of potential privacy inferences from the provision and collection of their data. Users' behaviour and needs are altered as a result. Future work needs to investigate the development of a system that complies with all recommendations identified in this report.

Acknowledgements

I would like to thank Dr. Alia Abdelmoty for her consistent guidance and support throughout the duration of this project. It would have not been possible without the knowledge and supervision she provided.

I would like to thank all those who participated in the survey and interviews and especially those who provided datasets. All of the datasets fundamentally supported the project. I would also like to thank Layla Khudayir for providing me with a Fitbit device to allow for the collection of a data set.

Finally, I would like to thank my friends and family who have consistently picked me up from the hard times and supported me throughout my studies at Cardiff University.

Contents

Table of Figures

Table of Tables

Requirements:

Supporting Tables:

Introduction

The concept of the "Internet of Things" (IoT) is more prevalent now than ever before and its adoption is showing no signs of slowing down. In fact, the IoT is anticipated to have unprecedented growth through to 2020, with the market expected to surpass $1.7 trillion, amongst over 20.8 billion devices (Eddy, 2015). The concept surprisingly isn't new and by nature is simple; The IoT can be described as a network of physical object's (devices, gadgets or "things") containing embedded technology that are connected through wired and/or wireless connections (and unique addressing schemes), which essentially creates a pervasive environment enabling interactions between physical and digital worlds. Support from stakeholders and market forces alike have enabled the establishment of the concept, consequently the features and design of devices have progressed tremendously in response.

This paper focuses on wearable fitness trackers, in particular Fitbit, whom are a global leader in the industry. Wearable fitness trackers in their own right have advanced from pedometers to fully fledged health, activity, sleep and even location tracking devices. Wearable devices are tapped into the connected self and are a key player in growth of the IoT. The devices are packed with "smart sensors" and make use of Bluetooth technology to wirelessly connect to smartphones. This allows for useful information to be displayed on a supporting application. These "smart sensors" essentially allow the device to connect with you as a person and help tailor specific personal goals (like health and fitness or improving lifestyle). Sales of wearable fitness trackers (sports watches, fitness monitors, wristbands and smart watches) are expected to reach 102 million units in 2016, with the wearable's market in general growing over 18% from 2015 (Gartner, 2016). The increase in functionality and sheer number of connected devices, means an absurd amount of data is being generated. Worryingly, a large proportion of this is personal data, or data derived from people (e.g. activity records), which allows us to distinguish a person from other people in a group and subsequently profile them (Github, 2014).

In addition, further worry is justified when noting that one of the major catalysts for wearable's growth has been the corporate wellness market. Corporate wellness is the process by which employers seek to improve the overall wellbeing of their staff. Employers ultimately reap the rewards in doing so. Increasingly in order to achieve this, employers have relied upon distributing subsidised fitness trackers. The result of this can be incredible amounts of personal information such as health, activity and sleep data being visible to an employer. This market is also expected to see continued exceptional growth. A study by ABIResearch (2013) identified the opportunity for more than 13 million wearable devices to be incorporated into corporate wellness plans established by businesses, by 2018. Therefore, corporate wellness, in relation to fitness tracking device distribution, has the promising prospect to transform how employers interact with their employees. Employees willingly provide their data whilst attempting to meet tailored goals (both individual and employer set, with employer goals often being incentivised) and this ultimately benefits both parties. However, it also provides the need to investigate potential drawbacks from the data collected, as a result of the interactions between these devices and humans, in regards to compromising user's privacy. Hence the motivation for this project.

This paper therefore presents a study of privacy implications of the provision and collection of employee data from wearable devices, in relation to user awareness and behaviour. Put simply, before employee's consent to wearing a device, they should have the ability to know what data it collects, how to see the data it collects and ultimately what privacy vulnerabilities are associated with the data collected by the device. This paper aims to identify if this is the current position. Firstly, through modelling the dimensions of the problem. Secondly, through data analysis to identify privacy implications implicit in user data (using a real-world dataset). Finally, through the carrying out of quantitative analysis to extract user's awareness, behaviour and opinions. If proven not to be the case, this project will provide recommendations for protecting employee's personal privacy when using wearable devices as part of a well-being program. The paper also explores the benefits of the provision and collection throughout.

Previous research has investigated the trade-off between privacy and utility in relation to consumer behaviour, the impact of wearable technology on consumers, organisations and user's privacy concerns and finally users' willingness to participate in sharing data with an employer (including what incentive encourages them the most to partake). However, consumer concern and awareness in relation to existing and potential privacy threats resulting from the interaction between these devices and humans over time, in contrast to the instantaneous snapshots a user sees, has not been fully examined. Assessing and bridging this gap would play a significant role in providing employees participating in corporate wellness programs with sufficient and effective means to obtain privacy, something which has not yet been achieved.

Related Work

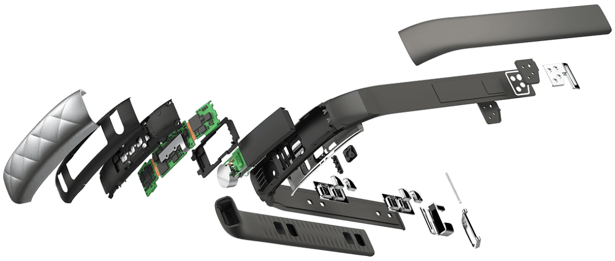
In this section, two pertinent questions to the hypothesis studied are reviewed, these are: what kind of privacy implications can be identified from data collected by wearable fitness trackers and to what degree are privacy related inferences a concern amongst wearable fitness tracker users.

Current Attitude towards Privacy Concerns Relating to Wearable Fitness Trackers

The Evolution of Privacy, Wearable Devices and Wearable Markets

Privacy concerns have been around for centuries and thus are not new. They are also present in multiple fields and are not limited to the technological field. Technology can, however, be acknowledged for reforming the way the public thinks about privacy and for allowing it to take on a new significance (see Appendix A for more information on modern day privacy). With ease of sharing information, comes the motivation for others to breach one's privacy. Additionally, the explosion of the Internet of Things (IoT) has led to dramatic enhancements in the functionality the devices provide. People willingly allow wearable fitness trackers to continuously collect various types of data, from a variety of complex sensors. Originally only pedometers which measured steps, minute and inherently inconspicuous sensors embedded in the devices (shown in Figure 1) have evolved to collect incredible amounts of information (shown in Figure 2). A study by LICBS & Zeno (2014) identified that 72% of consumers are aware that information is collected, however, the rapid development in functionality and minimalistic design, means users may not be fully aware of what is being collected and there is motivation to identify if this is the case.

Figure 1 - Anatomy of a Fitness Tracker (Jawbone, 2016)



Through collaboration with an operating system on the device, and filtered through an algorithm specific to manufacturers, the “smart sensors” provide users with an instantaneous snapshot (on a supporting application, web interface or device interface) of their activity, sleep, health and even workout routes visualised on a map.

Figure 2 - "Smart Sensors" Embedded in Wearable Fitness Trackers (Adapted from Microsoft, (2016))

Sensor	**How and what does it collect?**
Accelerometers/Gyrometer	Accelerometer (or gyrometer) essentially measure motion (movement, direction and speed), this enables the tracking of steps for instance. This information can be partnered with heart rate data and weight/BMI information, that a user manually enters to identify the number of calories burnt.
GPS	GPS fundamentally receive high-frequency, low-power radio signals from satellites to determine location. This enables the monitoring of routes, and can allow for more accurate speed and distance data.
Optical Heart Rate Monitor	Typically uses light sensors to continually monitor the level of blood flow through a user’s skin. Heart rate fluctuations help identify calories burned and sleep quality.
Ambient Light Sensor	This is used to identify the required level of brightness the device requires so it can automatically adjust.
Galvanic Skin Response (GSR)	Measures the electrical connectivity of the skin. This can enable the identification of when a user is sweating, so better monitoring can be carried out.
UV Sensor	Measures the ultra-violate levels in a given location. This can be used to identify when you require sun cream.
Barometer	The barometer detects changes in atmospheric pressure to determine the vertical distance you travel.
Thermometer	Measure temperature. If temperature rises but activity level doesn’t it can be due to illness, this can be obtained, as well as used to identify when physical activity is taking place to better monitor.

With clear and apparent benefits, it is easy to see why consumers feel so willing to allow the collection of their data. Whilst consumers may seemingly feel comfortable and are aware that information is collected, they may not comprehend that data could potentially be shared amongst third parties, or exploited for purposes which differ from the instantaneous snapshot they are accustomed to. Consumers might be worried if informed that a recent FTC study identified that a total of 12 different health and fitness apps sent data to a staggering 76 different third parties (Kaye, 2014). This information becomes even more compelling when noting that LICBS & Zeno (2014) also discovered that 59% of users are unaware that information can be shared with third parties, and a further 55% do not want their information shared with third parties.

In addition to privacy and device functionality evolving, the markets underpinning wearable devices have also advanced. For example, corporate wellness, which has established itself as one of the fastest growing areas of business for market leaders such as Fitbit. Estimates stipulate Fitbit will have revenue of $180 million dollars from corporate wellness in 2016 (Oslon, 2015). Fitbit CEO, James Park, also shared with Oslon (2015) that he expected the corporate wellness business to be worth an astounding $11 billion by 2019, showing there is no indication of market growth decelerating. Fitbit have capitalised on this fresh market and proudly boast a whole array of large companies who are on board, including the likes of Adobe, BP, Coinstar and Boston College. Oslon (2015) recognised that Fitbit have also sold to 70 big American employers, including Target and Barclays, who both subsided the cost of 330,000 and 75,000 Fitbit devices for employees respectively. Amy McDonough, who runs Fitbit's wellness business, shared with Oslon (2015) that businesses on board are enthusiastically running competitions in an attempt to reduce staff insomnia and absences. One example provided was oil giant BP, who are currently individually tracking staffs steps over the course of a day to determine eligibility for a lower health care premium in the succeeding year (the more steps they take, the lower the health care costs). In addition to BP, Cloud-computer provider Appirio saw a 6% ($280,000) reduction in their 2014 insurance premiums, this was after sharing activity data from 400 subsidised workers Fitbit's with their insurer (Oslon, 2016). Therefore, there is a clear motivation for employers, manufacturers and employees alike to partake in such programs and a need to investigate the privacy implications in doing so, which have not yet been fully explored.

In regards to worker's opinion of this growing market, PWC (2015) conducted a study of 2,000 working adults to better understand. PWC identified that 40% would be willing to use wearable technology from their employer. This figure rose to over half (56%) if people know the data will be used to improve their wellbeing at work. The incentives found most popular in making participants willing to share their data for were, flexible working hours, free health screening and health and fitness incentives. There were respondents who were not willing at all to take an incentive to part with their data, of those 41% said they don't trust their employer not to use the data against them in some form. A similar amount (40%) didn't feel they could trust their employer to use the supplied data for their benefit. Perhaps most intriguing, the study by PWC (2015) identified that respondents were more open to the idea of parting with their data to employees if the data is anonymised and shared in aggregate form, rather than their individual data. This shows that not only can employers expect big benefits from exploiting their employee's data, but that a large proportion of people are willing to participate and thus, a large proportion could be susceptible to privacy implications. This provides motivation to explore if any privacy implications pose a threat to participants.

Attitudes and behaviour towards Private Information

The increase in number of connected devices in conjunction with the ease of exchanging the information collected, through social media and other platforms, has led to a reform in public and expert attitude towards such information.

- Over half (54%) of UK consumers never share or are extremely careful in the sharing of personal data because they were not always or not at all confident their data is sufficiently protected (Accenture, 2015)
- Significantly over half of people (70%) are concerned about their information being used for different purposes than it was collected for (Jourová, 2015)
- Over half (55%) of 2,511 technology industry professionals and experts polled do not agree that there will be a system in place giving people the decision to decide how they want to share their information, whilst also letting companies profit (PWC, 2014)

This is very disturbing and shows that not only are consumers more hesitant than ever while sharing data and thus place privacy at a higher priority, but also that that the supporting systems are not evolving as quickly as the amount of personal information being collected to allow explicit control when sharing data, whilst also benefiting both parties (particularly relevant with corporate wellness systems). Furthermore, consumers are becoming worried about the exploitation of their information for purposes above and beyond the reasoning for collection (which will be explored in the data analysis section). In addition to making privacy a priority, it would also appear that the general public are becoming knowledgeable to organisations exploiting their data in return for very little benefit. The result of this is greater precaution from consumers in relation to who is collecting their data, who is using their data and what benefit they can expect in return for parting with their data. The study by LICBS & Zeno (2014) reinforces this view. They found that 51% of consumers want to know how their information will be used and 26% take personal data privacy into account when purchasing a device. Perhaps contradictory, self-confidence is also the latest tendency amongst consumers, in relation to negotiating the value of their data, with 52% viewing their personal information as an asset which can be used to get better deals (Acxiom & DMA, 2015). Furthermore, LICBS & Zeno (2014) identfied that 50% of consumers are prepared to share their personal information, as long as they receive rewards. Hence, whilst consumers may be concerned about the protection of their data, consumers are now more than ever more prepared to part with personal information, as long as they have established a benefit in doing so. This is especially true for those who buy wearable devices to be part of a community and follow trends, with LICBS & Zeno (2014) identifying that this group of people are far more willing to trade-off privacy in return for more personalised offers. Corporate wellness seemingly provides benefits to employees through incentives and health benefits. However, these statistics show that the value consumers place over private information can be significantly decreased through incentives, regardless if there are privacy implications in doing so. This provides motivation to identify if incentives can inherently make user susceptible to privacy violations.

Wearable Attractions and Apprehensions

The attraction and growth of wearable device popularity cannot be attributed to one prominent factor, but rather several connected factors. One factor is personalisation. If an object is to be worn on a user's body 24 hours a day, then it inherently becomes incredibly personal. This is a trend that entrepreneurs and large organisations like Apple alike have capitalised on, both in their marketing campaigns and hardware design. Interchangeable bands, sharing heart beats with loved ones and jewellery which enhances the appearance of wearable devices are all being deployed to shape this trend. Data from Slice analysed interchangeable bands made and sold by Apple. The data showed 17% of 20,000 Apple Watch customers purchased an additional band to the bundled one (Love, 2015). Another factor is the functional benefits wearable devices provide. A survey carried out on 20,000 Apple Watch owners acknowledged that 83% reported "some" (59%) to "a lot" (24%) of health improvements since utilising the watches functionality. A further 72% stated they actively engaged with the watch by tailoring goals on a regular basis (Desarnauts, 2015). Another major factor in the wearable market which keeps users actively engaging with their device is the social engagement devices can provide. Users can share their progress on social media, in addition to tracking their friend's progress with popular devices like Fitbit. This has proved incredibly trendy despite early blunders with the feature (Fitbit used to share user's sexual activity data by default until it led to hundreds of people's being monitored and shared online (Hill, 2011)).

Despite many attractions, consumers inevitably have apprehensions with wearable technology. A study by PWC (2014) acknowledged that 82% of respondents were worried that wearable technology would invade their privacy. In addition, 86% expressed concern that wearable devices would make them more vulnerable to security breaches. This concern is reinforced in the 2015 Clearswift Insider Threat Index (CITI). Clearswift (2015) states that within the next year 40% of firms expect an insider data breach (see Appendix B). This particular statistic can be attributed to employee behaviour, alongside three quarters of employees stating that their company doesn't apply enough resources to raise awareness of potential cyber-threats. In regards to employee behaviour, 58% are none the wiser as to what may form a security threat from inside their job and half admit they ignore data protection policies in order for easier completion of their responsibilities. Further analysis in relation to specific consumer concerns and opinions in relation to privacy, can be found in Appendix C. This provides motivation for identifying if consumer's worries are justified.

Potential Privacy Inferences Obtained from Wearable Fitness Trackers

Explicit Privacy Inferences

One has identified several instances of explicit privacy inferences obtained from a wearable fitness tracker. Three studies identified several of the most popular fitness bands including Fitbit, Basis, Garmin, Mio and Jawbone are putting consumer's privacy at risk (Barcena, et al., 2014; Hilt, et al., 2016; Cyr, et al., n.d.). Unique identifiers were found to be fixed on all devices studied, with the exception of the Apple watch, the repercussion being static identifiers enable third parties (such as shopping centres or even an employer's building) to persistently monitor the location of these wearable's at any given point in time, regardless if Bluetooth was switched on or off. Not only was this alarming discovery made, but the study by Hilt, et al., (2016) also found that numerous devices and their accompanying applications allowed for the falsifying of data by any motivated party (more on this in device security section below). This is made even more troubling given that recently a Canadian Law firm relied on data from a Fitbit, this was to attempt to portray the decline in the amount of activity their client had been able to complete following an accident (Oslon, 2014). One must also take into consideration corporate wellness, in which insurers rely on employee data to offer cheaper health rates or monetary/work incentives. If incentives are handed out in response to goals being met (e.g. certain number of steps per day), and a user can actively falsify this data, it provides opportunity for exploitation. Thus, if data can be manipulated it poses serious implications for wearable devices and the law and those offering incentives.

Implicit Privacy Inferences

Furthermore, there are inferences which are implicit in the data generated by wearable fitness trackers. For example, a man recently took to popular social new networking site Reddit in an attempt to resolve what he felt was an issue with his Fitbit device. The man posed the issue that his wife had logged 10 hours of activity in Fitbit's 'Fat burning zone' without increasing her level of activity, something which had not happened before. Naturally, this resulted in the belief that the sensor was broken. In fact, the man was so certain the sensor wasn't functioning properly, that he asked for advice on recalibrating the device before he raised the issue with Fitbit's customer service. His concerns weren't shared with everybody, another user differed in his explanation for the higher-than-usual heart rate and wasn't so sure it was a broken device, explicitly starting "Has she experienced anything really stressful in the last few days or is it a possibility she is pregnant?". A visit to the doctor later and the wife discovered she was pregnant (Kelly, 2016). Whilst It may have been in the couples plans to start a family, it may not be in the plans of consumers for third-party's (such as employers) to identify this. This poses a real privacy threat and potentially room for extortion. This is in addition to the sexual activity being discovered in Fitbit user's activity data, as touched on previously, which Barcena, Wueest, & Lau (2014) identified also poses an extortion threat to users.

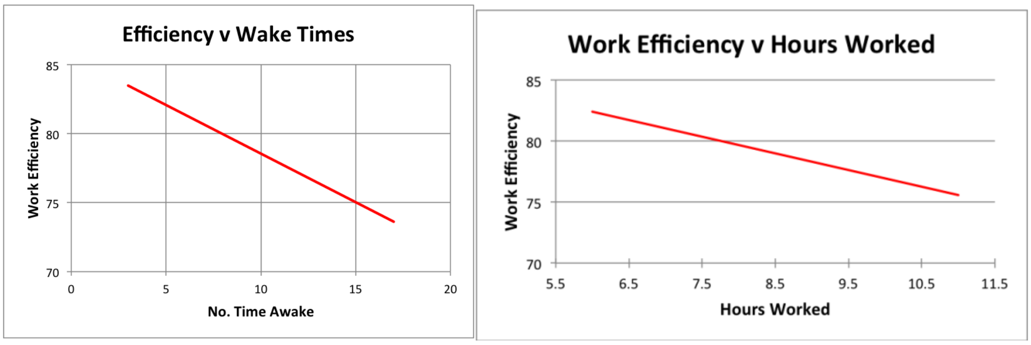
Additionally, a study was conducted by Profusion and reported by O'Connor (2015), in which for 10 days, Profusion's data scientists used Fitbit's and accompanying apps to track 171 personal metrics for 31 staff who volunteered. The data scientist analysed the data and identified that they could group staff into groups, based solely on patterns of behaviour. They were able to apply labels to groups, with one being "busy and coping", whilst another received the more distressing label “irritated and unsettled”. The results, as expected, left volunteers concerned, when discussing a colleague who took part a lady stated it was “the most stressed I’ve ever seen her”, another found it “quite disturbing”. The experiment shows the level of surveillance and possible classification of employees that is possible with data generated from a wearable fitness tracker, both of which are an invasion of privacy.

Moreover, a different more personal study was carried out by Wisbey (2012), managing director of FitSense. His study aimed to identify if there was any relationship between his sleep habits, activity during the course of the day and how productive he was at work. In order to identify if there was, he used a FitBit Ultra to track his sleep and activity. He overcame the notoriously difficult metric to measure productivity by using RescueTime (Ben used the daily efficiency rating in RescueTime as well as looking at both morning and afternoon efficiency independently). He collected the data over a two-month period and analysed it using the statistical package SPSS to determine any statistical relationships. The three main correlations identified were:

1. Inverse correlations between number of awakenings and productivity
2. Inverse correlations between the duration of his sleep and productivity
3. Inverse correlations between the lengths of time spent working and productivity.

This means that poor or little sleep, longer work days or a greater number of awakenings all undesirably affected his productivity at work. Perhaps most fascinating, he identified that his productivity was affected all day opposed to just the morning or afternoon, removing the notion that poor sleep only affects the first few hours of work. Figure 3 highlights the correlations, the graphs show just how big of an impact sleep quality and the number of hours worked can have on work place productivity.

Figure 3 - Productivity Graphs - (Wisbey, 2012)



In summary, a number of potentially useful correlations can be identified from exploring patterns implicit in user data, and this motivates the need to further explore real world data sets to determine the full extent at which it poses a risk to user privacy.

Dimensions of the Privacy Problem with Wearable Fitness Trackers

This section analyses five aspects related to wearable fitness tracker data privacy that need to be recognised to fully model the dimensions of the problem. These are:

1. The regulations/laws governing user's data
2. The security provided to user's
3. The accessibility and visibility of user's data
4. The quantity and quality of user's data
5. Possible utilisation of user's data

This study takes into consideration any privacy-related issues which are related to the above aspects, in addition to identifying the confidence one can have in derived information. This gives one the ability to determine how much each aspect is to be expected to impact a user. For the purpose of this study, Fitbit is considered.

Regulations and the Right to be Forgotten

In December 2015, after three years of negotiations, the informal agreement of the final draft of the EU General Data Protection Regulation (GDPR) was reached. In a press conference, Parliament, European (2015) stated the intended aim when it comes into force in 2018:

> *The new rules will replace the EU's current data protection laws which date from 1995, when the internet was still in its infancy, and give citizens more control over their own private information in a digitised world of smart phones, social media, internet banking and global transfers. At the same time they aim to ensure clarity and legal certainty for businesses, so as to boost innovation and the further development of the digital single market.*

Therefore, the GDPR essentially gives users greater control over their data (access, storage, right to be forgotten) and imposes strict rules on the accountability of third party providers, in relation to their compliance with privacy rules. Ruiz, (2016) argues that the GDPR also brings a tougher provision for consent to the processing of data, seeing a shift from "implicit consent" to “freely given, informed and unambiguous”, which is positive, although to a certain extent short of the originally drafted “explicit consent”. The agreement has been reached to fine companies up $20 million or 4% of annual turnover if they breach the regulations, thus it will likely prompt businesses to protect user’s private data. The agreement has also seen a shift towards a one-stop model, basically this provides the opportunity for a “lead supervisory authority” to tackle instances where processing activity affects data in one or more member states (Willan, 2015). The GDPR also solidifies an already common approach users are taking with Google since a recent court ruling, the right to be forgotten. Since the launch of its official request process, Google has received 386,038 requests and removed 42.5% of all the 1,357,986 evaluated URLs (Google, 2016). This signifies the transition in consumers becoming empowered as users, opposed to being dismissed.

In regards to Fitbit, they offer a somewhat half-hearted approach in allowing users to be forgotten. In their privacy policy[1], Fitbit state that whilst users can remove any data that identifies them (e.g. name, email) by contacting customer support and waiting (this process is done via an automated schedule resulting in data remaining in archive for a brief period), they will continue to use users de-identified data. This commitment is clearly unenthusiastic, user’s data (despite being de-identified) is still utilised by Fitbit after request for deletion. Fitbit have recently moved to become HIPAA compliant in corporate wellness offerings[2], U.S. Health Insurance Portability and Accountability Act (HIPAA), essentially this is a law which protects personal health information utilised by health insurers and others. Both the European regulation and HIPAA are a move in the right direction for consumer protection, although adherence and ensuring no loop holes will prove vital for effectiveness.

Security

Security can be defined as the precautions taken by the device, the application and the networks both connect to in order to protect user’s data against vulnerabilities and threats.
Wearable devices pose a new dimension to the security problem, they not only require device protection, but also protection of user’s data stored in the ‘cloud’ or on servers. This is in addition to the security of the supporting applications, which present user data in a human

[1] https://www.fitbit.com/uk/privacy – Accessed 8th Feb 2016

[2] https://investor.fitbit.com/press/press-releases/press-release-details/2015/Fitbit-Extends-Corporate-Wellness-Offering-with-HIPAA-Compliant-Capabilities/default.aspx - Accessed 6th April 2016

friendly format. The increase in functionality, availability and affordability of wearable fitness trackers has meant the market has become incredibly competitive as manufactures seek to get a portion of the enormous market. This brings security risks within the dimensions that need to be secure, as outlined above. Fitbit's SEC filings show some of the risks that manufacturers face, as identified by Maddox (2015). In the company's S-1 filing with the SEC on May 7, Fitbit outlined the need to deliver the best products, whether it be refining existing or developing new ones. This often requires juggling multiple projects in order to be first to the market. In order to achieve this consideration needs to be applied to multiple factors. One factor is anticipating and effectively addressing consumer preferences and demand. Another factor is ensuring timely and successful research and development. The problem this poses to consumers is that the devices can be rushed in order to achieve this, this ultimately leads to devices which do not provide the security mechanisms that ultimately safeguard user's data. Fitbit state in their privacy policy[3] that they "use a combination of technical and administration controls to maintain the security of data", but do little to explain actually what they are. Likewise, Fitbit also states in their privacy policy that they comply with the U.S. - EU Safe Harbor Framework and the U.S. - Swiss Safe Harbor Framework, but again give no explanation or examples on situations that these laws apply to.

In regards to device and application security, the study by Hilt, et al., (2016) found that Fitbit takes steps to prevent generated fitness data tampering. This is by encrypting its generated fitness data on the wearable itself, then routing that encrypted data through the company's mobile application to Fitbit's servers. The assumption is that the servers then decrypt this into a readable structured format, then stores it, from which the mobile application can download the data from the server and present it to the user. This essentially removes trust from the application and instead provides the server and device with authority over the integrity of the data. This is significantly better than the applications discussed earlier, which share information with numerous third parties and take little precaution in encrypting user's data. The reliance on servers however means that it is almost impossible to safeguard user's data. In addition, the study by Hilt, et al., (2016) discovered Fitbit use HTTPS encryption across their system, the significance of this is that encryption is used to prevent eavesdroppers from collecting and tampering with user's data. However, Fitbit were discovered not to use SSL pinning, which is a further recommended layer of security. Studies Barcena, et al., 2014; Hilt,

[3] https://www.fitbit.com/uk/privacy - Accessed 8th Feb 2016

et al., 2016 acknowledged that Fitbit do not include LE privacy (this prevents persistent monitoring of devices through static MAC Addresses) in their devices. Fitbit stated that the fragmented state of the Android system prevented them from doing so (not the capability of their devices). Fitbit added they had wished they could implement such mechanisms. Whilst there is still room for improvement in regards to LE privacy and SSL pinning, the device security has actually significantly advanced. A study by Rahman, et al. (2013) developed a suite which exploited Fitbit's design and successfully launched several attacks. The study identified any device within 15ft would have its data vulnerable to capture and modification (which includes information which can identify individuals e.g. user name, city, weight), the device would also be vulnerable to battery depletion attacks (persistent queries sent to the device in order to deplete battery at an increased rate). The implications for poor security within the health tracking field are an increasing worry and whilst it's promising to see advancements, it is clear the functionality and popularity these devices have obtained has been at a much faster rate than the security they provide. Earlier concerns are seemingly therefore justified. Since one will be using a Fitbit in the data analysis section of this report, one can have confidence the data has not been tampered with, as they now take steps to prevent this.

Quality and Quantity of Data

Wearable Fitness trackers are placed around the wrist of a user and basically measure motion and altitude to determine useful health, activity and sleep information. The motion is typically measured with two sensors; a 3-axis accelerometer which tracks direction and a gyroscope to track orientation and rotations. Altitude is determined via a barometer, which tracks changes in atmospheric pressure to determine vertical distance travelled. Heart Rate sensors typically use light technology to measure blood flow through a user's skin. This data is then converted into basic activity data (steps, distance travelled), then this is applied to an algorithm (unique to manufacturers and typically kept secret) in conjunction with a user's height, age, weight and heart rate, this determines information such as calories burned and sleep quality. Finally, the data is presented in a human-friendly format on mobile or desktop applications, on which users can also manually enter and track their Weight, BMI and their food consumption (manual entering is utilised when a sensor cannot determine the statistic). GPS sensors are used to receive high-frequency, low-power radio signals from satellites to determine location, this is used to map out workout routes and more accurate distance information. Additional sensors are detailed in Figure 2. The key thing is that the devices automatically and continuously track data, thus these devices generate large volumes of data. Whether access is available to continuous data (for example, minute by minute) will impact the volume of data collected and its accuracy, hence also the degree of confidence in inferences made from the data.

The accuracy of fitness tracker has come under increasing scrutiny as the functionality has developed. A common tendency amongst market leaders has been to shy away from responsibility of the accuracy of their devices. Fitbit follow this tendency and state although their goal is to provide helpful and accurate information, they accept it is not intended to match the accuracy of real medical equipment, they further add in their terms of service[4]:

> *We are not responsible for the accuracy, reliability, effectiveness, or correct use of information you receive through the Fitbit Service.*

This clearly shows there is no responsibility from Fitbit to provide accurate data or information. Fitbit was recently met with a lawsuit challenging the accuracy of the heart-rate monitor in its Charge HR and Surge products. The lawsuit claimed they knowingly advertised the technology as accurate, when it actually misread heart rates by “a very significant margin, particularly during exercise.” The lawsuit claimed that readings were off by an average of 24.34 beats per minute (bpm), and a staggering 75 bpm in extreme cases. Austin (2016) tested the devices under speculation and whilst in some cases during high intensity exercises it was around 6bpm off a Polar H7 ECG monitor (although this didn’t happen when the device was worn as advertised: “A finger width apart up the wrist”), in general the devices were deemed to be very accurate, thus one can expect the derived information to be so too. Although one will use multiple types of data in the analysis section, this still provides some confidence in its accuracy, regardless if Fitbit do not take responsibility.

Information Accessibility and Visibility

Accessibility represents how much of the user’s data are available and visible to others including the user, other users and third parties. It is important to identify the access that users have over the data that is being tracked by their wearable devices, even if they are unaware of the feature and its possibilities. Accessibility underpins users and others ability to identify

[4] www.fitbit.com/terms - Accessed 8th February 2016

inferences, hence importance. Fitbit allow their users to export to either excel or CSV files (with a premium account, which comes at a yearly cost of £39.99). The data which can be exported (at a maximum of a month's data at a time) is outlined on Fitbit's help section on their website[5] and shows the columns automatically populated, as per below:

> **Body**— Includes weight, BMI, and body fat percentage. If users ever manually tracked their blood pressure, glucose, or heart rate, this data is also available. (**Fitbit are still working on making automatic heart rate data available for export**).
> **Foods**— Contains a list of any foods manually logged by a user.
> **Activities**—Includes tracker data such as steps, distance, floors, total calories burned, calories burned from activity, sedentary minutes, and active minutes.
> **Sleep**— Includes sleep data such as time asleep, time awake, and number of times users woke up
> **GPS** - GPS data can be exported to a TCX file which can be used with several applications such as Google Earth.

Fitbit also provide high level analytical tools to users, these analyse weekly or monthly stats and give a brief snapshot of a user's activity stats compared to the Fitbit community. Fitbit also allow users to "benchmark" their stats, this fundamentally allows for comparison and querying of their data against Fitbit's database (e.g. how do I compare to a 50-year-old man?). Fitbit therefore do an excellent job at providing users with access to analytical tools to analyse their data, but hinder consumer's ability to really identify privacy implications implicit in their data for a number of reasons. Firstly, they charge consumers for the privilege of accessing their data, then only provide in 30 day instalments, this then requires further compiling to analyse over further periods of time (time consuming and complex). Finally, they only provide daily statistics and not minutely/hourly data, which could potentially identify different privacy implications than that of daily statistics. A study by Cyr, et al., (n.d.) showed that Fitbit devices collect information to this level of granularity, but does not provide users with the ability to see such data unless they possess the ability to reverse engineer the application. There are several public API's which allow for the exporting of Fitbit data for free (and some to a higher

[5] https://help.fitbit.com/articles/en_US/Help_article/Can-I-export-my-fitness-data-to-my-computer - Accessed 8th February 2016

level of granularity), although one would be trusting a third-party with their data in the process and the general public might not be aware of such API's.

In terms of third party and other user's accessibility and visibility of user's data, Fitbit set users profiles to "Private" by default (although as noted previously, this was previously 'public' until user's sexual activity was being shared publically). In regards to wellness programs, an employer would require an employee to consent before Fitbit will share any data, consent can also be revoked at any time. However, the employer may not need consent to get access and visibility of the data after all, one carried out an experiment as per below:

Approach

Fitbit's website provides the functionality to link a user's Fitbit account to their social media, including Twitter. Fitbit also provide the format in which the tweet will be sent out, like so:

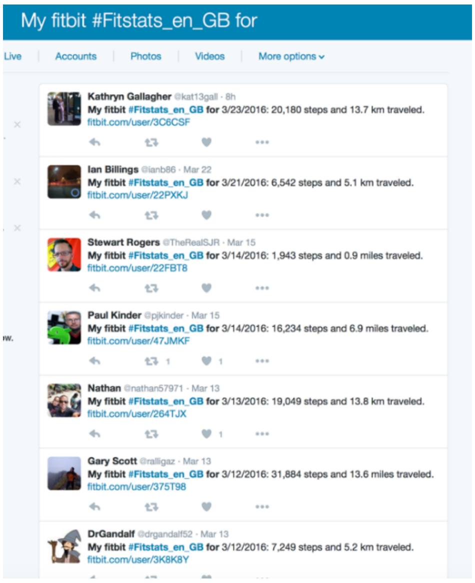
> *My Fitbit #Fitstats_en_GB for 3/24/2016: 0 steps and 0 km traveled.*
> *http://www.fitbit.com/user/…….*

Through utilizing Twitter's search functionality, one copied the initial part of this tweet (assuming everyone's would be the same minus the user name) and searched Twitter.

Results

One's assumption was proved correct, hundreds of results were returned of users who are socially active and share their statistics as shown in Figure 4. Fitbit's website does however give users the option to control who has sight of this data through three selectable options; Public, Friends and Family or Yourself. Therefore, it still requires users to opt into sharing this with the public or an ill-motivated friend or family member to gain access. Fitbit also provides a "preview" mechanism enabling users to view their page from the perspective of each of the three options, this allows users to see exactly what is on show and to whom. In one's experiment, 43% (or 14 of the 32 users one inspected) had some or all of the data set to 'Public' and of those 42% had sleep and body data 'Public' (which are both forbidden by Fitbit's well-being program). It is worth noting that when users opt for the 'Public' option you are able to look back at their information for as long as they have been wearing the fitness tracker (days, months, years).

Figure 4 - Twitter "Fitbit Stats" - Search Experiment



My fitbit #Fitstats_en_GB for

Kathryn Gallagher @kat13gall · 8h
My fitbit #Fitstats_en_GB for 3/23/2016: 20,180 steps and 13.7 km traveled.
fitbit.com/user/3C6CSF

Ian Billings @ianb86 · Mar 22
My fitbit #Fitstats_en_GB for 3/21/2016: 6,542 steps and 5.1 km traveled.
fitbit.com/user/22PXKJ

Stewart Rogers @TheRealSJR · Mar 15
My fitbit #Fitstats_en_GB for 3/14/2016: 1,943 steps and 0.9 miles traveled.
fitbit.com/user/22FBT8

Paul Kinder @pjkinder · Mar 15
My fitbit #Fitstats_en_GB for 3/14/2016: 16,234 steps and 6.9 miles traveled.
fitbit.com/user/47JMKF
1 1

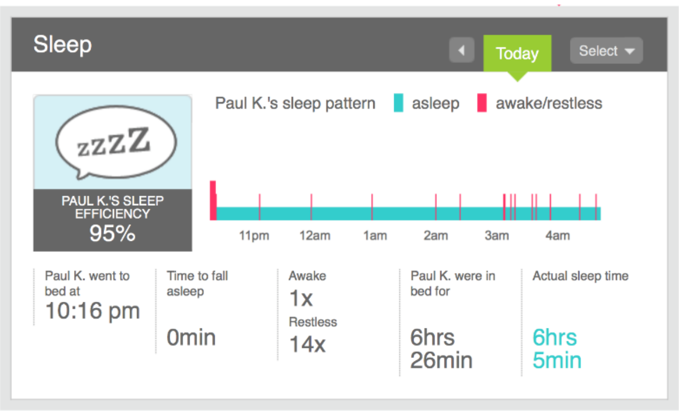
Nathan @nathan57971 · Mar 13
My fitbit #Fitstats_en_GB for 3/13/2016: 19,049 steps and 13.8 km traveled.
fitbit.com/user/264TJX
1

Gary Scott @ralligaz · Mar 13
My fitbit #Fitstats_en_GB for 3/12/2016: 31,884 steps and 13.6 miles traveled.
fitbit.com/user/375T98

DrGandalf @drgandalf52 · Mar 13
My fitbit #Fitstats_en_GB for 3/12/2016: 7,249 steps and 5.2 km traveled.
fitbit.com/user/3K8K8Y

Whilst Fitbit therefore provides abundant privacy settings and visualisations to control and visualise what data can be seen by whom on individual profiles, it does nothing to inform users of the potential privacy implications of sharing such data. Users may be inclined to share through lack of awareness, as the experiment has highlighted. Therefore, although users must opt in to sharing individual information when participating in well-being programs, employers could simply find the employees account using the above method and identify this information regardless. This is in addition to potentially gaining access to forbidden data. Figure 5 shows a user's sleep information and shows the extent of information which can be accessed by other users or third-parties when profiles are set to "public" (even the explicit time a user went to bed and for how long they slept). A complete set of what can be accessed is shown in Appendix D. In addition, the control offered when signing up to well-being programs is not as comprehensive as public profiles. Fitbit present users with a box stating what the employer has asked for and are given the option to accept, with no control over which aspects the employer can or cannot see (only preventing individual weight, BMI and sleep statistics). The employer is given the option to decide what elements they want to track at an individual or aggregate level and the employee is asked to opt in. Fitbit also state that user's data falls under the employee's privacy policy when opting in to such programs. Fitbit therefore do little to provide users with control when participating in well-being programs and the repercussions of this need to be explored.

Figure 5 - Sleep Information from Fitbit Profile (experiment uncovering, forbidden information)



Paul K.'s sleep pattern 🟦 asleep 🟥 awake/restless

PAUL K.'S SLEEP EFFICIENCY 95%

Paul K. went to bed at 10:16 pm

Time to fall asleep 0min

Awake 1x

Restless 14x

Paul K. were in bed for 6hrs 26min

Actual sleep time 6hrs 5min

Possible Utilisation of User Data

The utilisation of data is essentially how Fitbit or third-parties can exploit user data and for what purposes. Fitbit maintain a policy of only utilising data that cannot identify an individual and state the following in their privacy policy[6]:

> *De-identified data that does not identify you may be used to inform the health community about trends; for marketing and promotional use; or for sale to interested audiences.*

Fitbit go onto to slightly elaborate:

> *Fitbit may share or sell aggregated, de-identified data that does not identify you with partners and the public in a variety of ways, such as by providing research or reports about health and fitness or in services provided under our Premium membership. When we provide this information, we take legal and technical measures to ensure that the data does not identify you and cannot be associated back to you.*

Whilst Fitbit therefore state they take measures to ensure data cannot be traced to an individual, they provide no explanation or examples of such measures. They also appear to have full control over whom they share this data with and for what purpose, stating "interested audiences" and providing limited examples of such purposes. Fitbit also indicate they will

[6] https://www.fitbit.com/uk/privacy – Accessed 8th Feb 2016

share user's personal information with business partners whenever is considered necessary, such as the enforcement of law or when communicating with credit card companies. Fitbit also have the right to exploit user's content as specified in their terms of use[7].

> *By making Your Content available on or through the Fitbit Service you grant to Fitbit a non-exclusive, transferable, sublicensable, worldwide, royalty-free license to use, copy, modify, publicly display, publicly perform and distribute Your Content only in connection with operating and providing the Fitbit Service.*

It is therefore apparent that there are no obligations on Fitbit as to how they may use the data, both aggregated data and content which is uploaded to the service. The reasoning for exploiting one's data are not fully explained, for example "in connection with operating and providing the Fitbit Service". Consequently, by agreeing to Fitbit's privacy policy and terms of service, users effectively are giving away their content and rights to such content to Fitbit.

[7] www.fitbit.com/terms - Accessed 8th February 2016

Soft Systems Methodology

In order to further guide an analytical study of some representative data sets from a wearable device, the dimensions of the problem outlined above will be modelled using Soft Systems Methodology (SSM). SSM fundamentally attempts to provide a "soft investigation" (e.g. what operations should the system be performing) to raise knowledge and appreciation into a problem situation amongst a group of stakeholders. This can be used to pave the way for the "hard" investigation (e.g. how the system should do it), derived from the set of actions produced to improve the situation (recommendation section). SSM may be used to analyse any problem or situation, but it is most appropriate where the problem:

> *Cannot be formulated as a search for an efficient means of achieving a defined end; a problem in which ends, goals, purposes are themselves problematic"* (Checkland, 1999)

SSM will therefore be exceptionally useful and applicable to the problem outlined in the previous section, as one looks to model the dimension and its separate problematic purposes (e.g. security). The set of actions which are generated will drive part of a data analysis study and also guide the recommendations section (how to protect privacy when sharing data). For the purpose of this study, the system in consideration will be Fitbit's.

Alternative methods

One considered using Systems Dynamics, opposed to SSM. Systems Dynamics, unlike SSM, utilises stocks, flows, feedback loops (and time delays) to model a system to better understand its behaviour. One decided to use SSM instead as the intention was to visualise the dimensions of the problem to enhance understanding of what the system should be performing, the conceptual model allowed one to have a general additional understanding of 'how'. Whilst Systems Dynamics provides a greater exploration of the 'how', it was not the intention to fully explore this and one did not need to explore policies or the impact of influences on the system, something Systems Dynamics is superior in providing.

CATWOE Analysis

A CATWOE analysis is used during SSM to guide a perspective of the problem through a controlled modelling process. A CATWOE essentially is the basis from which a well formed root definition can be constructed, it consists of six elements with the first letter of each making up the mnemonic C.A.T.W.O.E. The process by which we identify the knowledge relating to each of these elements is defined as a "C.A.T.W.O.E. analysis". Firstly, the transformation has to be identified, from which the problem solver can gradually work through the remaining elements. Each element represents a question, as per below:

1. **Customers/Client**

   What or who benefits from the completion of the transformation?

2. **Actor**

   Who carries out the transformation for the customers/client?

3. **Transformation**

   What happens from the start to the finish point?

4. **Weltanschauung or Worldview**

   What is the justification for the transformation?

5. **Owner**

   Who owns, is answerable and has the authority to cease existence of the system?

6. **Environment**

   What can be said to influence but not control they system?

The knowledge derived from those questions will form the basis of a root definition. It is of paramount importance that the root definition has been formulated and structured properly because only the content included in the definition can be utilised to construct a "conceptual model". Checkland (1999) suggests a possible structure of the root definition, this will be applied in this project:

'A system to do X, by Y in order to do Z'

***Transformation**:*

The dimension of the problem has been heavily analysed in addition to related work, this has allowed for the identification of the transformation. One has identified an innovative market which has established itself in the wearable scene, corporate wellness. This market essentially sees employees part with their data for an incentive. The research carried out has identified apprehensions from consumers towards providing employers with their data, mainly through fear of it negatively impacting them, this is primarily due to a lack of trust. One has justified the lack of trust and negative impact opinion by identifying insufficient security in Fitbit's devices, this allowed for persistent monitoring of devices (including at an employee's workplace). One has also identified several implicit privacy inferences, including productivity, mood and pregnancy uncovering. One assumes users would not be aware of any of those three inferences. One has also identified you can gain access to user's data (including employers and including forbidden data) through a simple search of a user's social media and subsequent Fitbit profile (if set to "Public"). One has also identified minimal control offered to employees when given the option to 'opt in', this allows for this to take place. These are all privacy violations and need to be addressed. Therefore, the intended start point and finish point can be identified:

> *Reduce and maintain privacy violations against Fitbit users wearing the device for an incentive*

Worldview:

The research also allows one to identify the weltanschauung or worldview, which is what reason justifies the completion of the above transformation. One has identified that an increase in security will protect user's data. In addition, one has identified a scenario in which Fitbit gave users greater control, they changed their default setting of a user's activity to 'private' opposed to 'public', this had originally been 'public' in an attempt to improve engagement in the social scene, unfortunately this had unintentionally revealed user's sexual activity on search engines. Fitbit released a statement stating "we certainly did not intend or expect the sharing of intimate information" (Hill, 2011). The increase in awareness and control, has consequently led to the problem being solved and the prevention of a privacy violations (you can no longer find intimate information about users). Thus, this approach is justification for the completion of the above transformation. Therefore, the weltanschauung or worldview can be identified:

The belief that by providing Fitbit users with an increased presence of information about privacy implications and greater control of the data they share with employers, whilst continuing to keep them informed of future privacy implications and improving device security will result in a reduction of privacy violations

Client:

The clients or customers can be identified as the beneficiary of the transformation; in this instance this will be Fitbit Users (employees in this particular problem). The employees will expectantly benefit from the increased awareness of privacy implications and increased control over what they chose to share, as well as enhanced security. Therefore, the client can be identified:

Fitbit Users

Owner:

The owner can be identified as those responsible for answering, or those that have the power to cease the system to exist, in this instance, this will be Fitbit and the employer. Fitbit have the power to stop making the devices and partnered system, employers and users alike use the system to access and control their data. Similarly, when granting access to an employer as part of a wellness program, employee's data is then governed by the employer's privacy policy and employers obviously also have the power to cease wellness programs. Therefore, the owners can be identified;

Fitbit and Employer

Actors:

The actors can be identified as those who facilitate the transformation to the client, in this instance, two actors have been identified. Firstly, the Fitbit users (employees) have been identified as actors behind the system, this is because they will have to champion change by pressing the issue with the owners of the system. The owners being Fitbit and the Employer, the need for championing change is because currently they would appear to have no concern over current control and awareness of privacy implications when users share data in their wellness programs or on their public profiles. Whilst Fitbit are keen to implement security features deemed suitable, they have yet to do so. In addition, another actor that has been identified is Fitbit developers, once the issue has been pressed to them by the users, the recommendations for improving the situation (or actions) must then be actioned by the capable and appropriate developers. Therefore, the actors can be identified:

> *Fitbit users and Fitbit developers*

Environment:

The environmental constraints can be identified as what influences but does not control the system, in this instance, four have been identified. Firstly, there is a constraint around the potential prospect of users being disinclined to make use of the increased information presence or control (my experiment identified that whilst users on their personal profile are given ample control, the vast majority do not make use of it). Fitbit developers could theoretically implement such actions and users could not adopt them. In addition, research has identified relevant legislation that will be introduced in the very near future, it's vital that Fitbit and Employers move to be in line with the relevant regulations (Fitbit are already HIPAA compliant). Finally, the security mechanisms which help protect user's data are influenced not only by the rush to the market, but also the fragmentation of the Android system. The fragmentation of the Android system means that if security measures such as LE privacy were implemented, they would not work on all devices and thus, restrict their ability to be competitive across platforms. This is something which has been identified as key to Fitbit's success and the reason for apprehension in implementing. In addition, the social aspect of Fitbit has been deemed important, such that they used to set users profile to 'public' by default in order to increase interactions. Consequently, the implementation of control features in employee well-being programs may adversely affect the visible benefits and subsequent participation rates, thus also competitiveness. Finally, one has identified the possibility that employees feel inclined to 'opt in' due to being made an offer they can't refuse (e.g. cannot afford to not have lower health care costs). Therefore, the environmental constraints can be identified:

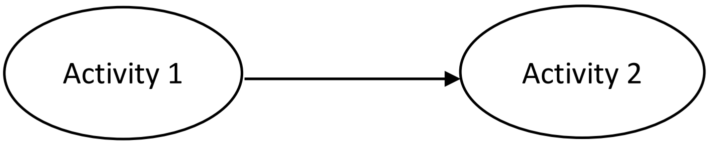
> *Fitbit users' may be disinclined to learn to understand privacy implications or make use of increased control features, Fitbit users' may be inclined to 'opt in' due to feeling unable to decline the incentive, Complying with relevant regulations and Fitbit themselves may be apprehensive to increase security, control and information presence through fear of reducing competiveness*

Root Definition

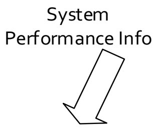
> *A Fitbit owned system, operated by employers where Fitbit developers can reduce and maintain privacy violations against Fitbit users wearing the device for an incentive, by providing Fitbit users with an increased presence of information about privacy implications and greater control of the data they share with employers whilst continuing to keep them informed of future privacy implications and improving device security, at the same time as complying with relevant legislation and giving consideration to the fact that Fitbit users may be disinclined to learn to understand privacy implications or make use of increased control features, or may be inclined to 'opt in' due to feeling unable to decline the incentive and Fitbit themselves may be apprehensive to increase security, control and information presence through fear of reducing competiveness.*

Conceptual Modelling

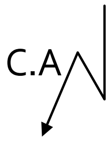
Whilst the root definition explains exactly what the system will do in order to solve the situation deemed problematic, one has not identified what needs to be completed (or how) in order to complete the actions expressed in the root definition. This is the reason for the conceptual model. In order to identify the activities and relationships which make up the model, verbs from the root definition are used to describe an activity. The relationships are symbolised by linking different activities with arrowed lines (Checkland, 1999). Thus, the primary purpose of constructing such a model is to identify all of the activities required within the system for it to function as intended, whilst outlining how to go about doing so (methods and activities).



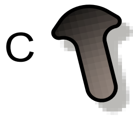
The arrows show logical dependencies, an arrow in the direction from activity 1 to activity 2 as shown above means that activity 2 is dependent upon activity 1. Generally speaking, the dependency is that activity 2 requires some form of output from activity 1. Wilson and Checkland have differing views on how to introduce control mechanisms to monitor the performance of the system, this project takes Wilsons view, as outlined below:



The block arrow shown above represents activity performance information, this identifies within the system where the performance of the activity and its dependencies are monitored to identify exactly how they are being executed in relation to solving the problem. The monitoring then leads to a decision, if what is being executed is achieving the intended goal then no action is taken, but if the goal is not being met then control actions are required. This is shown below ("C.A" with an arrow), this is placed and directed outside the activity box.

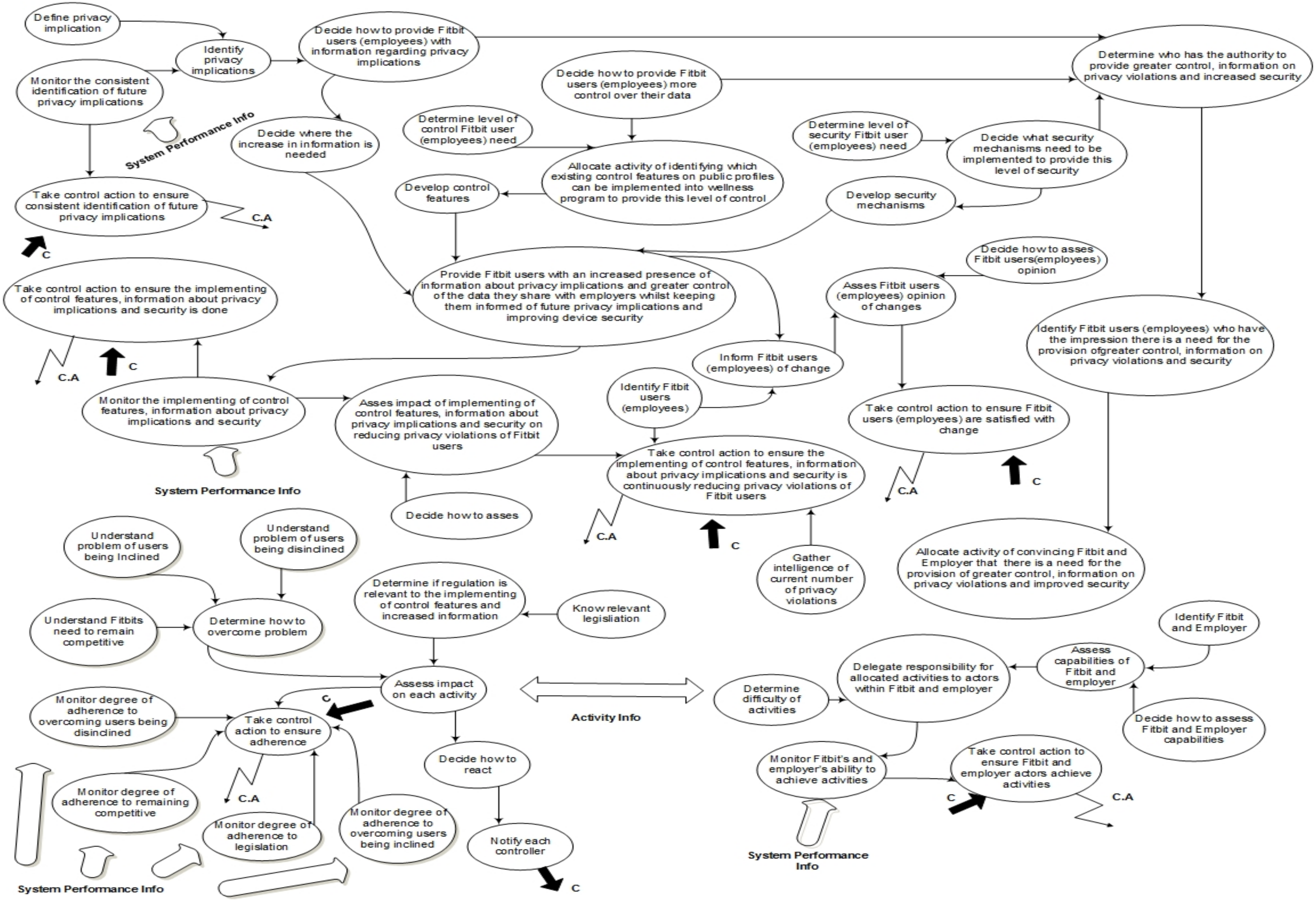


The intention of control action is to address situations where the intended objective is not being met, actors can then take action to ensure the system addresses the problem (thus, It goes onto function as originally intended). Activity information is highlighted when it can affect 'actors' and thus, they need to subsequently be informed in order to address how it impacts each of them.



A block arrow with a C represents where control is required, its direction indicates in what context (taking action is inward to activities, notifying controllers is outward from activates).

Analysis of the sections within the Conceptual Model can be found in Appendix E.


Define privacy implication
Identify privacy implications
Monitor the consistent identification of future privacy implications
System Performance Info
Take control action to ensure consistent identification of future privacy implications
C.A
C
Decide how to provide Fitbit users (employees) with information regarding privacy implications
Decide where the increase in information is needed
Decide how to provide Fitbit users (employees) more control over their data
Determine level of control Fitbit user (employees) need
Allocate activity of identifying which existing control features on public profiles can be implemented into wellness program to provide this level of control
Develop control features
Determine who has the authority to provide greater control, information on privacy violations and increased security
Determine level of security Fitbit user (employees) need
Decide what security mechanisms need to be implemented to provide this level of security
Develop security mechanisms
Provide Fitbit users with an increased presence of information about privacy implications and greater control of the data they share with employers whilst keeping them informed of future privacy implications and improving device security
Take control action to ensure the implementing of control features, information about privacy implications and security is done
C.A
C
Decide how to asses Fitbit users(employees) opinion
Asses Fitbit users (employees) opinion of changes
Inform Fitbit users (employees) of change
Identify Fitbit users (employees) who have the impression there is a need for the provision ofgreater control, information on privacy violations and security
Monitor the implementing of control features, information about privacy implications and security
Asses impact of implementing of control features, information about privacy implications and security on reducing privacy violations of Fitbit users
Identify Fitbit users (employees)
Take control action to ensure Fitbit users (employees) are satisfied with change
C.A
C
System Performance Info
Take control action to ensure the implementing of control features, information about privacy implications and security is continuously reducing privacy violations of Fitbit users
Decide how to asses
C.A
C
Gather intelligence of current number of privacy violations
Allocate activity of convincing Fitbit and Employer that there is a need for the provision of greater control, information on privacy violations and improved security
Understand problem of users being Inclined
Understand problem of users being disinclined
Determine if regulation is relevant to the implementing of control features and increased information
Know relevant legisliation
Understand Fitbits need to remain competitive
Determine how to overcome problem
Identify Fitbit and Employer
Assess capabilities of Fitbit and employer
Delegate responsibility for allocated activities to actors within Fitbit and employer
Determine difficulty of activities
Assess impact on each activity
C
Activity Info
Monitor degree of adherence to overcoming users being disinclined
Take control action to ensure adherence
Decide how to assess Fitbit and Employer capabilities
Monitor degree of adherence to remaining competitive
C.A
Decide how to react
Monitor Fitbit's and employer's ability to achieve activities
Take control action to ensure Fitbit and employer actors achieve activities
C.A
C
Monitor degree of adherence to legislation
Monitor degree of adherence to overcoming users being inclined
Notify each controller
C
System Performance Info
System Performance Info

Data Analysis

Experiment

This analysis was carried out by using real-world, self-generated datasets from Fitbit devices. Fitbit are the global leader in fitness tracking devices and provide functionality to export the data collected, hence choosing them. The purpose of this analysis is to demonstrate the possible privacy implications that are implicit in a user's health, activity and sleep records collected by "smart sensors" embedded in the devices. The possible inferences that can be made as a result of collecting one's records is also analysed. This is driven from the conceptual model, in which control action needs to be taken to identify privacy implications (as this currently has not been fully achieved in the real world).

Datasets

Three datasets were used to carry out this analysis. Firstly, one personally wore a Fitbit and collected a months' worth of health, activity and sleep records over the period 03-11-2015 through until 03-12-2015. Secondly, a publically available dataset provided by Furberg (2015) was used, this contained some of the users sleep and all of the user's health and activity records over the period 10-22-2011 through until 09-20-2014. Lastly, a kind user of the Fitbit forums requested to support the project and provided me an export of his health and activity records over the period 01-01-2015 through until 05-03-2016.

Approach

To analyse the potential impact of analysing a user's health, activity and sleep records can have on their privacy, the datasets were classified into those three variables. The data which makes up each variable can be seen in Figure 6 below.

Figure 6 - Data within Health, Activity and Sleep Variables

Activity	Calories Burned Steps Distance Floors Minutes Sedentary Minutes Lightly Active Minutes Fairly Active Minutes Very Active
Health	Weight BMI
Sleep	Minutes Asleep Minutes Awake Number of Awakenings Time in Bed

Before analysing the data, it was important to identify the possible questions which can be applied to the dataset variable, this will help in identifying relationships. The following questions were identified and can be applied to the dataset. When partnered with further knowledge the employer may have about the employee, these can allow inferences to be made.

1. What was a user's health/activity/sleep records for a particular day?
2. What was a user's health/activity/sleep records for a particular day in comparison to another day?
3. What was a user's health/activity/sleep records during leisure time compared to work time?
4. What was a user's average health/activity/sleep records for a particular week?
5. What was a user's average health/activity/sleep records for a particular week compared to another week?
6. What was a user's average health/activity/sleep records for a particular month?
7. What was a user's average health/activity/sleep records for a particular month compared to another month?
8. What was a user's average health/activity/sleep records for a particular year?

9. What was a user's average health/activity/sleep records for a particular year compared to another year?
10. What was a user's average health/activity/sleep records for a particular season?
11. What was a user's average health/activity/sleep records for a particular season compared to another season?

Microsoft Excel and IBM SPSS 20 were both used to analyse and represent the data.

Results

User's records can be extracted in the form of daily statistics of the variables shown in figure 6. For example, in my self-generated dataset, my records for Thursday 3rd November 2015 show the following:

Activity: 1,504 calories burned, 3,810 steps, 2.66KM distance travelled, 14 floors climbed, 1,262 minutes sedentary, 86 minutes lightly active, 0 fairly active, 0 very active
Health: 8.79 stone in weight, 21.26 BMI
Sleep: 430 minutes asleep, 18 minutes awake, 8 awakenings and 456 minutes in bed.

This arguably straightforward and seemingly innocuous data on health, activity and sleep can be analysed and partnered with other information the employer potentially has about an employee to identify information that can be considered to compromise an employee's privacy. Analysis will investigate the relationship between variables and periods of time as follows.

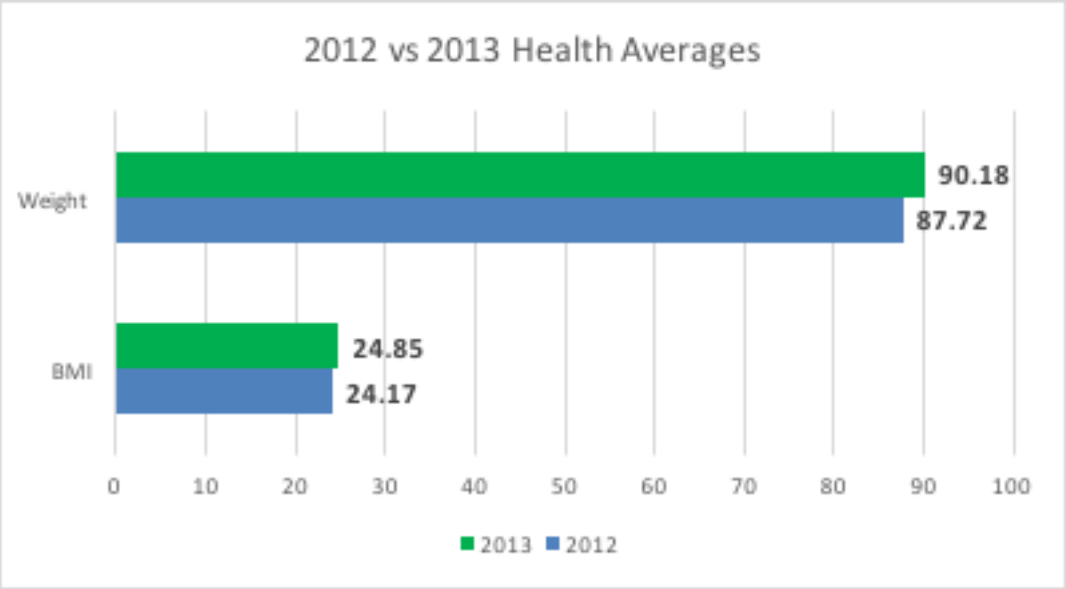
- ***Degree of association between activity and given time frame*** – This will investigate the relationship between a user's activity records over differing periods of time. Particular focus is on the surveillance aspect of activity data.
- ***Degree of association between health and given time frame*** –This will investigate the relationship between a user's health records over differing periods of time. Particular focus is on the identification of eating dis-orders and employee productivity.
- ***Degree of association between sleep and given time frame*** – This will investigate the relationship between a user's sleep records over differing periods of time. Particular focus is on productivity analysis in partnership with surveillance (coping ability).

- ***Degree of association between sleep, health or activity over a given time frame*** – This will investigate the relationship between a user's health, activity or sleep over differing periods of time. Elements of interest will be relationships between sleep and productivity, and the inferences possible from access to all three variables in relation to mental health.

Degree of association between health and given time frame

(Furberg, 2015) provided a dataset of health data over the period of roughly three years, from this it was possible to plot question 9. Results are in Figure 7 below.

Figure 7 - Health Comparison over Two Years



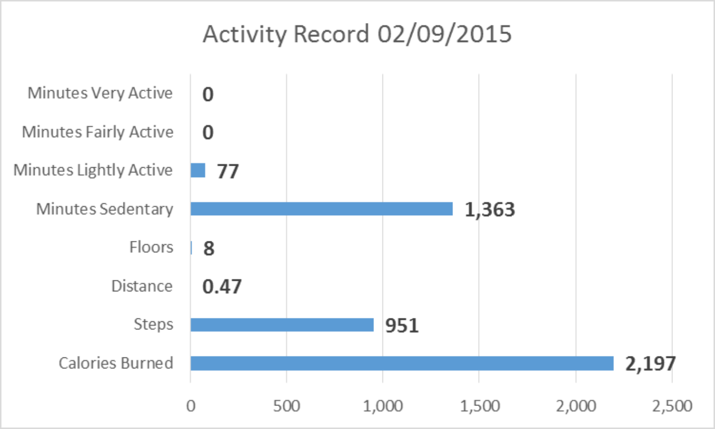
In this example, two years have been compared back to back, this being 2012 and 2013 respectively. The daily weight and BMI which Robert entered each day was averaged over the course of the two years, the result are presented above. The results of the analysis show that Robert's BMI and weight were on average 0.68 and 2.46KG lower in 2012, compared to 2013. The analysis therefore identifies a trend, Robert's weight and BMI are both increasing, and the employer can make inferences from this. The employer could take from this information that the employee has become lazier and is less inclined to be productive or presentable at work. A study by Bilger, et al., (2013) acknowledges that just 5% weight loss reduces both absenteeism by 0.258 days per month (p-value: 0.093) and the likelihood of showing low presentism (Stanford SPS-6 score between 7 and 9) by 2.9 percentage points (p-value: 0.083). Robert's weight has seen a 2.8% increase and the employer could therefore potentially expect the opposite. Effectively the employer can categorise those who are likely to be presentable and present in work, compared to those who are not.

In addition, when coupled with the fact Solicitors Crossland Employment (2016) found that nearly half of 1,000 recruiters said they would be less inclined to recruit an applicant if they were obese, with comments such as "wouldn't be able to do the job required" alongside "are unable to play a full role in the business", additional potential privacy implications arise. There is the possibility for identification of weight disorders, this is true for existing disorders and identifying trends towards a disorder. Employers can essentially monitor health activity as demonstrated above and note when the BMI is close to exceeding extremely high or low levels (<18.5 is generally considered anorexic with > 30 considered obese). Employers then may project the thoughts outlined above into their actions towards the employee and discriminate. While in the UK there are regulations to protect workers, both those seeking jobs and those already within a company, if the discrimination is implicit in data that the user is unknowingly providing it would prove difficult to identify discrimination. The invasion of privacy is fundamentally the catalyst of both inferences.

Degree of association between activity and given time frame

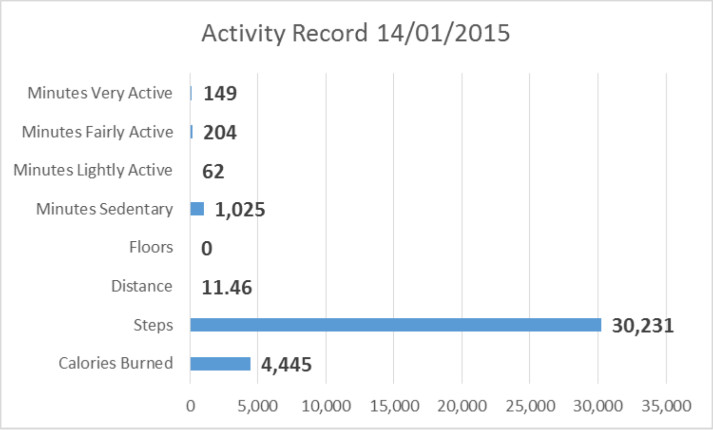
Chris an avid member of the Fitbit forums kindly provided oneself with an export of his health and activity records over a 15-month period. From this it was possible to plot question 1, twice. One analysed Chris's data on two particular days and results are shown in Figure 8 and 9 below.

Figure 8 - Activity Record Analysis - 1



In this example Chris's activity on Wednesday 2nd September 2015 was analysed, as shown in Figure 8 above. The results of the analysis show that he was particularly inactive on this day, making only 951 steps covering a short distance of 0.47KM. He also spent no time fairly or very active at all. The analysis therefore shows he did not move much on this particular day and when coupled with information the employer may have over the employee, inferences can potentially be made. If the employer was aware that the employee was supposed to be at a conference that day away from the office, and they know that on average a male takes roughly 5000 steps per day, they can make inferences that the employee lied about their whereabouts.

Figure 9 - Activity Record Analysis - 2



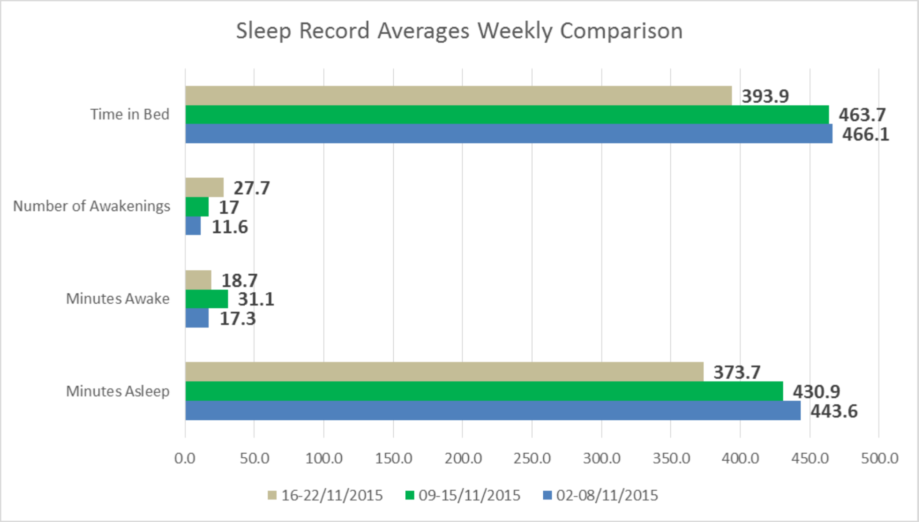
Similarly, as shown above in Figure 9, Chris was particularly active on Thursday 14th January 2015. He made 30,231 steps and covered a staggering 11.46KM in distance. He also spent a combined 353 minutes very or fairly active. The analysis therefore shows he did move a lot on this particular day and when coupled with information the employer may have over the employee, inferences can potentially be made. If the employer was aware that on this day he told them he was ill or suffered an injury and wasn't able to attend work (e.g. sick leave), then they can make inferences that Chris is lying about said illness or injury.

Both of these examples are serious breaches of one's privacy and can even be considered surveillance.

Degree of association between sleep and given time frame

One wore a Fitbit device and logged ones sleep records for a month, from this one was able to plot question 5. One analysed one's sleep data over two different weeks and compared the averages, as shown below in Figure 10.

Figure 10 - Sleep Analysis over Three Different Weeks

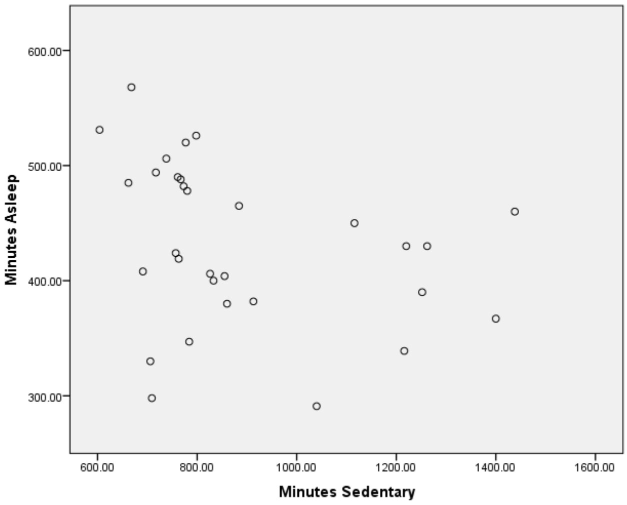


In this example three weeks have been compared back to back. The first week commencing Monday 2nd November 2015, the second Monday 9th November 2015 and the third commencing Monday 16th November 2015. The focus of the analysis initially is on the second and third week. The analysis shows that one slept on average 57.2 more minutes, one also had 10.7 less awakenings in the second week compared to the third. One also spent 12.4 minutes more awake and 69.8 more minutes in bed. This analysis shows that one had considerably better sleep in the second week compared to the third, from this inferences can be made when coupled with further information the employer may have on the employee. If the employer knows that the employee was given increased responsibility, such as a new project or an 'acting' role, at the beginning of the second week, they can make the inference that the employee is not capable of coping with the increased responsibility. They could further analyse this by taking the average from the additional previous week (or even a month), as shown in Figure 10. The further analysis leaves no room for doubt that the third week has seen a considerable drop in sleep averages across the board, the employer can then draw conclusions from this. This information is implicit in data and the employee may show capability to cope in the workplace, they could however be suffering outside of work. This is a breach of their privacy.

Degree of association between sleep, health or activity over a given time frame

One wore a Fitbit device and logged one's sleep, health and activity records for a month. From this one was able to analyse if there was a correlation between sleep quality (minutes asleep) and activity (minutes sedentary), as shown below in Figure 11. The graph shows an inverse correlation, this being that when one spent more minutes asleep, one spent less time sedentary during the day. Therefore, the inference can be made that productivity is linked to sleep quality and the employer can identify those who are not likely to be productive through monitoring their sleep quality (as well as taking into account the above analysis on sleep). This is similar to the study by Wisbey (2012) outlined in the first section and again is information implicit in data, it is also a breach of the employee's privacy.

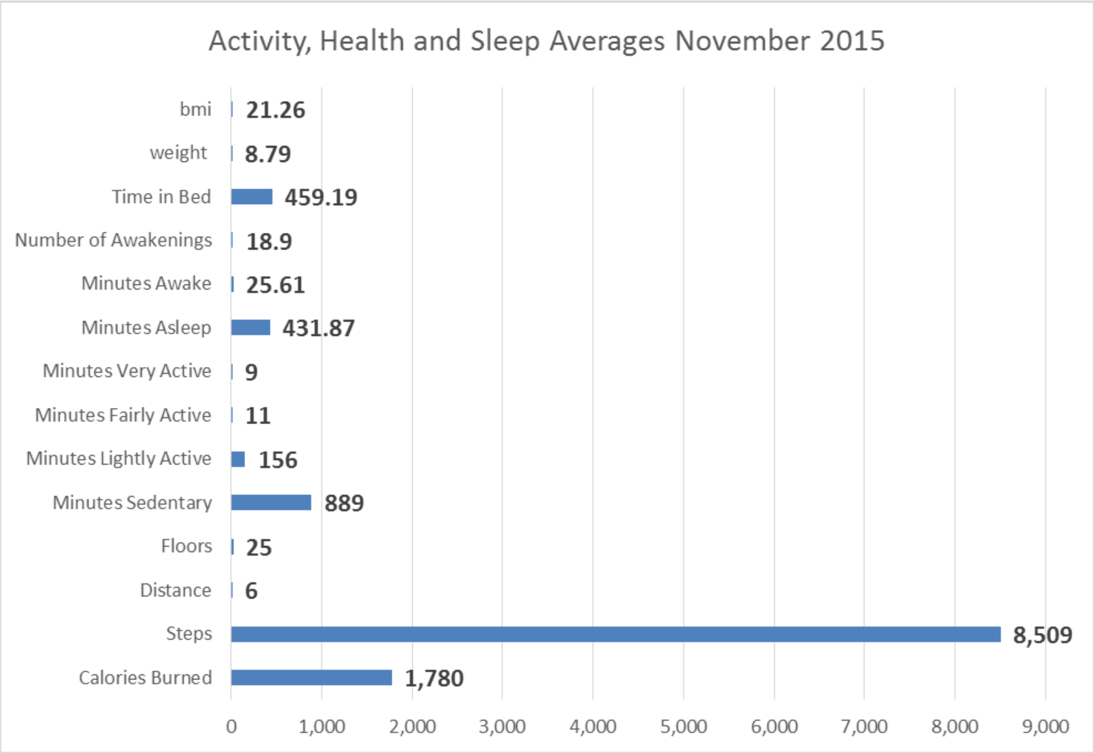
Figure 11 - Scatterplot of Minutes Asleep Compared to Minutes Sedentary



Employers obviously want healthy, active and motivated workers. User data can help categorise those who are, this can be done by analysing all three of the variables over the course of a month. Figure 12 shows one's averages of each of the variables, over the month November 2015. The analysis shows that one is in good health, one has a healthy BMI and weight, one is sleeping a sufficient amount and one is averaging above the average steps for a male. The employer would appreciate this snapshot, but would likely not appreciate if it showed the opposite. If the employer identified an employee with poor health, sleep and activity, they can potentially identify the mental state an employee is likely to be in and categorise them as a result (e.g. healthy and coping, unhealthy and not coping). A study by Karagöl, et al. (2014)

showed a positive correlation between BMI being high and depression. In addition, when partnered with a separate study by Taylor PHD, et al. (2015), which identified people with insomnia had greater depression and anxiety levels than people not having insomnia, they were also 9.82 and 17.35 times as likely to have clinically significant depression and anxiety respectively. It is apparent the insight an employer can get, they can potentially identify the mental state of an employee through information implicit in the data and discriminate as a result.

Figure 12 - Snapshot of a User's Activity, Health and Sleep over a Month



A recent case shows that discrimination against mental health within the workplace already exists. The case involved a lady who had a history of depression and applied for a job at Law firm DLA Piper. The lady received a job offer but it was subsequently retracted, she claims, after she revealed her history of her battle with depression, although the company claim it was in fact due to the recession and not at all linked to her mental health. Although an Employment Tribunal did not agree with the ladies claims and argued she was not suffering with "clinical depression" during the course of the incident, it is still possible that the disclosure of mental health condition was the reasoning behind the withdrawal (Outlaw, 2010). It is therefore again inferences derived from the data, which employees would not know could be achieved, that breaches their privacy.

The identification of these implicit privacy inferences provides motivation to identify if users are aware of such possibilities and if they are subsequently concerned, in addition to identifying if this affects their willingness to share data with an employer.

Questionnaire Approach

Questionnaire Tool

Prior to building the questionnaire one felt it would be beneficial to take into consideration the best tool to do so. Two of the most popular tools were taken into consideration:

1. Google Forms
2. Survey Monkey

One decided to explore the advantages and disadvantages of each service before reaching a decision. (Analysis of tool was provided by Marrs (2014))

Google Forms

Advantages	**Disadvantages**
• Can create unlimited number of surveys • Unlimited number of questions in various styles (open ended, closed ended) • Participants responses are automatically populated and made available to export in a spreadsheet (useful for analysis) • No limit on the number of respondents • Themes are available (can make it look more presentable which is likely to attract more participants) • Skip logic can be implemented (if respondents answer no to a question can jump forward) • This tool is completely free and can be distributed easily with a short URL • Links to google account (drive)	

Survey Monkey

Advantages	**Disadvantages**
• Can create unlimited number of surveys (Initial plan stated two would be created) • 15 different question types • Limited themes • This tool is completely free and can be distributed easily with a short URL	• Cannot export data to spreadsheet • Limited to 10 questions • Limited to 100 respondents • Lengthy signing up process

Decision

The original intention was to explore further tools, but after discovering how powerful Google Forms was in comparison to a top competitor, the decision was made to go with Google Forms. Google Forms not only provided unlimited questions and respondents, which was where the competitor fell short, it also allowed the export of data which is fundamental for the analysis afterwards. In fact, Google Forms had no disadvantages at all.

Questionnaire Objectives

Having identified the tool that would be used to create the questionnaire, it was determined that a plan would be established regarding what was sought to be accomplished from the questionnaire. Consequently, one came up with a series of aims which would ideally be achieved from the completion of the questionnaire. The aims were also paired with corresponding objectives to ensure the best chance of achieving each aim. The aims and objectives were:

Aim: To acquire responses on familiarity with wearable technology and fitness tracker functionality, usage of fitness trackers and factors which influence behaviour when purchasing fitness trackers.
Objective: The objective is to gather responses regarding awareness and behaviour in relation to wearable technology. It is fundamental to understand how familiar users are with wearable technology alongside if they currently use a tracker because if they are unfamiliar then they cannot relate in the same manner as those who are aware of functionality and

restrictions. However, the scope of the project is anyone who could be employed and potentially given a fitness tracker by that employer so it is important to have possible and current consumers. Likewise, it is also key to identify if privacy is a factor which influences behaviour when purchasing a wearable device, or if it is not significant when purchasing.

Aim: To acquire responses on sharing preferences for collectable types of data, to see if employers could obtain the information regardless if employees "opt in" (as per previous twitter experiment). In addition to identifying if users are willing to part with data for an incentive.

Objective: In addition to wanting to understand respondent's awareness and behaviour in relation to wearable technology, one wanted to identify respondents sharing preferences of specific types of data collected to note if respondents are putting themselves at risk without awareness of doing so. Therefore, the objective of this aim is to identify whom respondents would be willing to share body, activity, GPS, sleep and heart rate with given the options which Fitbit currently provides; Nobody, Friends and Family, Public. Through understanding this it is possible to identify how many would likely be putting themselves at risk to privacy violations (important to note employers would need not employees to 'opt in' if they share data with public on their personal profile). In addition, the objective of this aim is to understand if respondents would be willing to share all of the above data with an employer for an incentive, this will allow one to identify if incentives can manipulate behaviour, as identified in background research.

Aim: To acquire responses on attitudes towards derived privacy inferences from a real world dataset collected by a wearable fitness tracker. In addition, include inferences discovered through background research. Furthermore, identify if knowledge of privacy inferences affects sharing behaviour and attitudes towards better management of their data.

Objective: The users would be asked to state their attitude towards potential privacy violation scenarios from data analysis and research. Designing the questionnaire in this format provides the opportunity to revisit participants sharing preferences with an employer for an incentive, given awareness of the privacy implications in doing so. The hypothesis is that users are seemingly unaware of the inferences that can be made, thus by presenting them with them and asking if they would still be willing to share, one can understand levels of awareness and then subsequent behaviour. The behaviour could be that users feel they need better visibility, accessibility or control of their data and the objective is to identify if this is the case. The behaviour will be analysed by presenting statements which aim to improve the situation and asking users to state whether they feel each is required.

Questionnaire Constraints

The major constraint around the questionnaire is the number of respondents. In order for this to be a successful piece of research the number of respondents needs to be such that it can be reliable. The intended audience for this survey is anyone who is at working age (likely to be asked by an employer to use a fitness device). In Cardiff the population of people at working age is 230,400. The margin of error, or how much the opinions and behaviour of the sample survey is likely to deviate from the total population, will be 10%. Although a lower margin of error is deemed better it is unlikely given the duration of this project that this will be attainable. The confidence level will be 95%, this is the amount of uncertainty that can be tolerated. Given the above statistics and placed into the below formula provided by Raosoft (2016), the recommended sample size one is looking to achieve is **96**.

The sample size *n* and margin of error *E* are given by

$$x = Z({}^{c}/_{100})^2 r(100\text{-}r)$$

$$n = {}^{Nx}/_{((N\text{-}1)E^2 + x)}$$

$$E = \text{Sqrt}[{}^{(N - n)x}/_{n(N\text{-}1)}]$$

Where *N* is the population size, *r* is the fraction of responses that you are interested in, and *Z*(*c*/100) is the critical value for the confidence level *c*.

Questionnaire Design

In addition to creating aims and objectives, one researched best practice in regards to the design of the questionnaire to ensure quality results. In addition to already choosing the optimal tool, a series of factors were taken into account and have been outlined below.

1. Length of questionnaire

A study by Galesic & Bosnjak (2009) noted that the longer the stated length of a questionnaire, the less respondents started and completed the questionnaire. It is therefore vital that the questionnaire is designed to be long enough that it completes the above aims, but no longer as to lose participant retention and completion rates. The aim is that the questionnaire should take no longer than 5-10 minutes (the study found 10 minutes was optimal out of 10, 20 and 30 minutes).

2. Language style

Ambiguity is a pitfall for questionnaires which can lead to unreliable answers, if respondents are not fully aware of what is being asked then one cannot expect them to answer properly. It is therefore vital that the correct language style (professional, technical, slang etc.) is taken into account. Since this questionnaire is aimed at anyone who is or could be employed (professionals) and it is a technical project, one had to take into account the level of technicality and professionalism when designing the questionnaire. The questionnaire could not be too technical but must convey the technical aspects deemed relevant (e.g. GPS) and in order to address this in a professional manner one designed ‘Hints’, which explained the relevant technical terms. An example of a ‘hint’ can be seen below:

Q: With whom would you be willing to share activity data with?

‘Hint’: Activity data is: Steps, Distance, Floors climbed, Calories Burned, Minutes Sedentary and Active Minutes

3. Answer Style

The aims above in some instances will require respondents to select one or more options when answering, or multiple choice (e.g. factors taken into consideration when purchasing), it is therefore important that this is implemented in a suitable way such that it gathers what is required. In addition, some questions will provide participants with multiple answers but require them to only select one (e.g. who they would be willing to share _____ data with), it is again important that the options are given but controlled in a way such that only one may be selected.

4. Questionnaire Layout

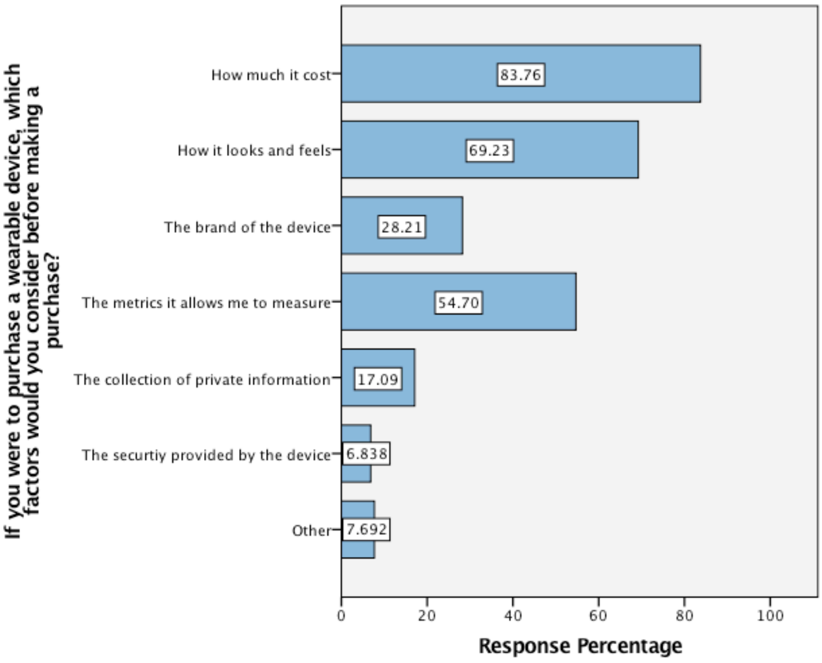
Several factors were taken into consideration when choosing the layout of the questionnaire. Firstly, bias was taken into consideration. Bias in a questionnaire can lead to the answering of questions in a manner that does not reflect the actual views of the participant and it's vital this is addressed. Since the questionnaire will present users with privacy implications derived from background research and data analysis, in an attempt to gauge the level of concern, it was important to include facts that whilst true, were not as dramatic as others. For instance, informing a participant that an employer could identify if females are pregnant is likely to concern them, but informing a participant that the data is used to improve insurance premiums for them and the company, is not. It is important to have both. Secondly, the use of open ended and closed-ended questions was also addressed. Closed ended questions do not allow for the expression of a true feeling, but rather force a response and will only be used in questions which this is deemed suitable, for instance when asking if participants currently use a fitness tracker or not, yes or no would suffice. The advantage of this is that it is time efficient (something which has already been taken into account) and is easier to interpret when analysing. In questions which it is deemed required for an open ended question, for instance when asking if the respondents have any other views, open ended responses are required. The advantage is that you gauge the true opinion, the disadvantage is that it is time consuming and harder to interpret because responses are subjective. Lastly, the placement of questions was considered, it was deemed important that the answers are not influenced by the question order. An example of this would be to ask for participant's level of concern regarding a scenario which invades their privacy and then asking with whom they would be willing to share data, the respondent may not have been aware of the implication and would likely change their sharing preference as a result.

Question validations and the questionnaire pilot can both be viewed in Appendix F. Questionnaire results and the questionnaire distributed can be viewed in a separate submission.

Questionnaire Analysis

The questionnaire data was analysed using IBM SPSS and the result are presented below. 117 participants completed the survey (21 higher than the intended sample size), of which 58% were young adults in the age group 18-25, with a further 15% falling in the 26-35 category. Those who participated were almost equally split between male and female at 60% and 40% respectively. The vast majority of participants were full-time employees (57%), with a further 28% falling into the student category. Most of the participants did not currently use a fitness tracker (66%), however, there was a large proportion either very familiar (31%) or somewhat familiar (46%) with the concept of wearable technology. In addition, only 14% were somewhat unfamiliar or very unfamiliar with the concept. The device cost was the most common factor participants would consider if they purchased a fitness device, with 83% of participants opting for this. This is followed by how it looks and feels, the metrics the device allowed them to measure and the device brand, representing 69%, 55% and 28% respectively. Intriguingly, only 17% and 7% opted for security or privacy, showing users don't feel this is fundamental. Results to this particular question are illustrated in Figure 13 below. The rest of this section explores the analysis of results from the different sections.

Figure 13 - Factors Taken into Consideration if Purchasing a Wearable Device

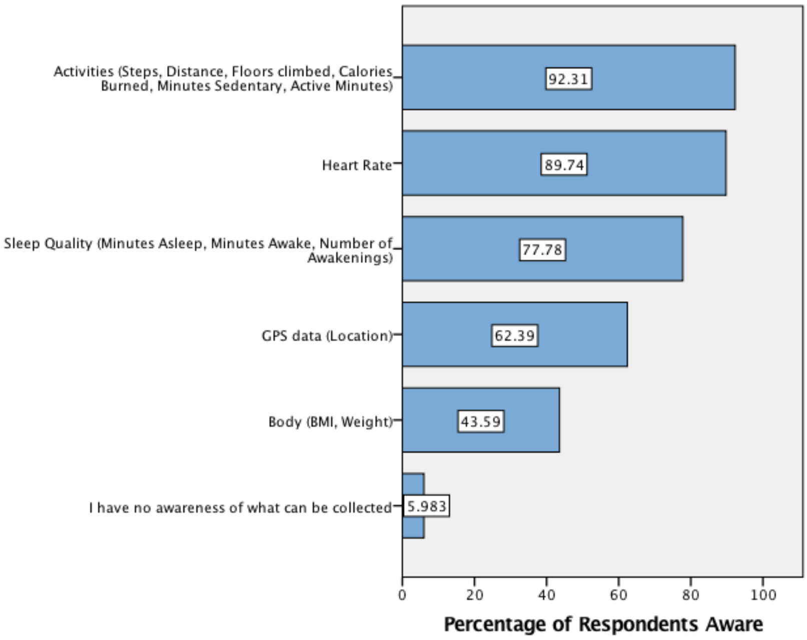


The results are frequently analysed against user profiles in this section (e.g. age, gender, wearable usage), the graphs which support this type of analysis are in Appendix G.

Knowledge of potential information collected by wearable fitness trackers

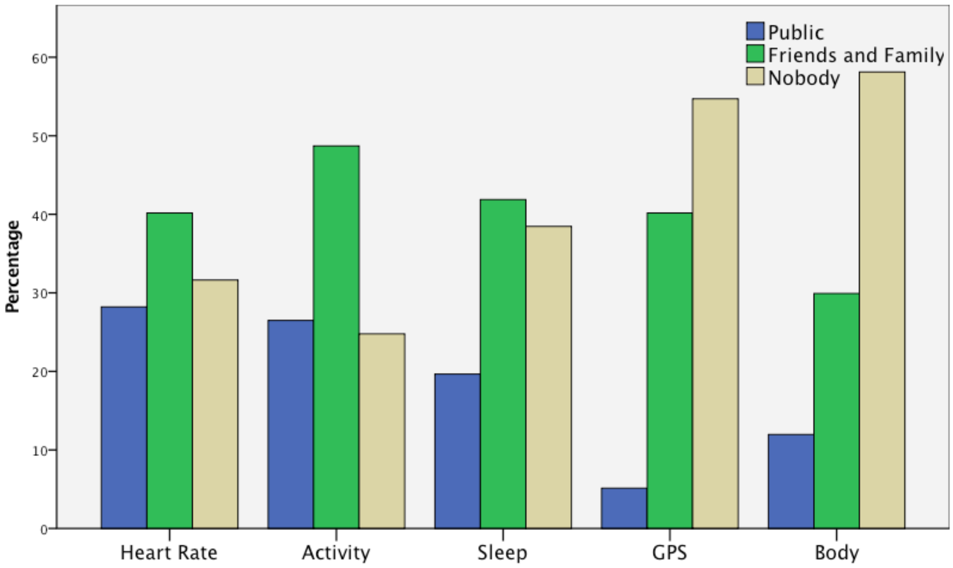
Here, the awareness of the potential information which can be collected from a wearable fitness tracker is examined and analysed against users' profiles. In general, the majority were aware of what information could be collected and only 6% had no awareness at all. Participants were presented with 5 potential collectable pieces of information relating to wearable fitness trackers and then were asked if they are aware these can be collected. Result are shown in Figure 14 below.

Figure 14 - Users Awareness of the Potential Information Collected by Wearable Fitness Trackers



Considerably less than half (30%) of participants acknowledge awareness of all five, of those 86% are either "very familiar" or "somewhat familiar" with the concept of wearable technology. Most participants are aware that activity, heart rate and GPS data can be obtained, with 92%, 90% and 62% opting for this respectively. Participants were generally unaware of body data (43%), this relates to BMI and weight. The reason for this maybe because it is not tracked through a sensor, but rather manual entry by a user. Interestingly, those who currently wear fitness trackers only make up 45% of those aware of all five. There was no correlation between age and gender in relation to awareness.

Figure 15 - Users Sharing Preferences



Sharing Preferences of Potential Data Collected

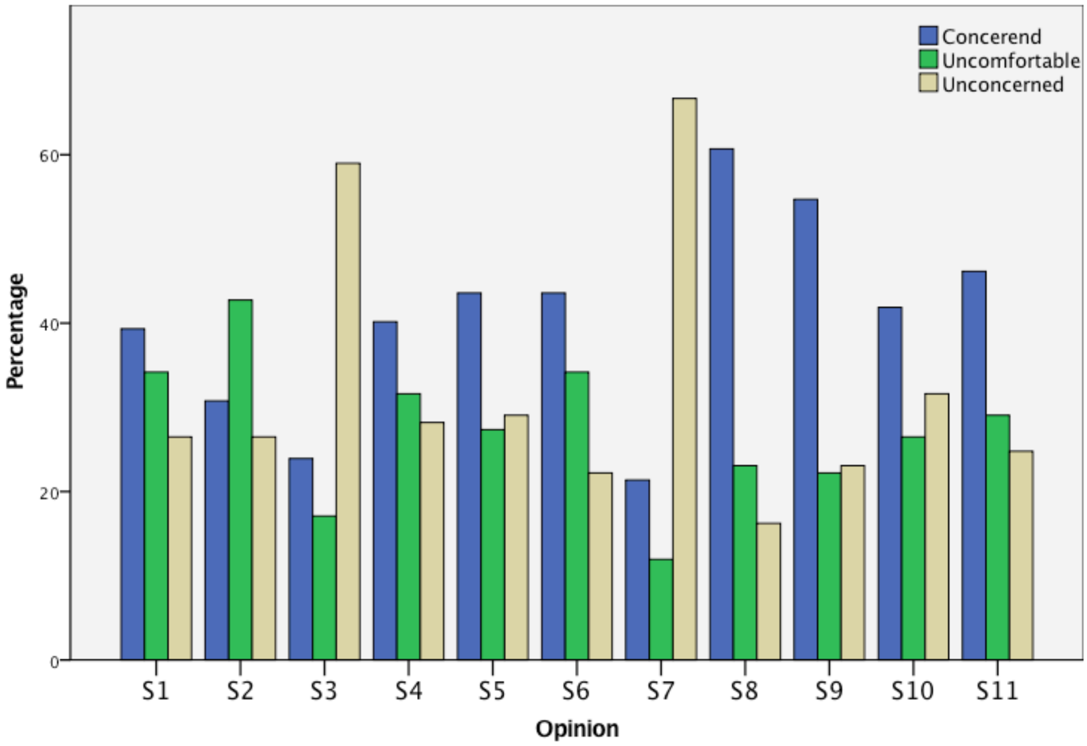
Here, the sharing preferences of potential information which can be collected from a wearable fitness tracker is examined and analysed against user profiles. In general, users were unwilling to share heart rate, activity, sleep quality, GPS or body data with the public at all, with a mere 28%, 26%, 20%, 5% and 12% opting for this preference respectively. Participants were presented with 5 questions, and were asked to indicate, for each statement (relating to a different piece of collectable information, shown above), whether their sharing preference to the question is either Public, Friends and Family or Nobody. Result are shown above in Figure 15.

Interestingly, age, gender and use of a fitness banned all played a big factor in this section. Firstly, those who were 60+ would not be willing to share any of the information with the public at all and only 33% would share with friends and family for all 5. The vast majority therefore chose private (66%). In addition, the only age group willing to share GPS with the public was 18-25, with 9% opting for this preference. Furthermore, gender played an unforeseen role, males in every question were more lenient in sharing their data with the public and chose this 21% of the time, compared to the females 16%. Men seemingly either wanted to share with the public as outlined above, or nobody (48%) or were far less inclined to opt for friends and family, only opting for this 31% of the time, compared to the females 46%. Unsurprisingly, those who currently did not use a wearable fitness tracker were considerably more likely to choose the sharing with nobody preference, they did so 10% more often than those who did. Awareness of each type of data being collected didn't seem to play a massive factor and was somewhat contradictory, in some instances no awareness (body and activity) led to being less likely to choose sharing with nobody (13% and 21% respectively) and in others (heart rate, sleep) led to being more likely to choosing the nobody preference (7% and 12% respectively). Interestingly this provides a key insight into how participants are putting themselves at risk to exploitation by a motivated third-party (including employer) when opting for 'public', they would be susceptible to the earlier experiment in which one derived information from a user's account (assuming they share on a social platform).

Perceptions of Possible Privacy Implication and security threats

Here, users' attitude towards the inference by the application of personal information and potential security breaches of wearable devices is examined. In particular, the question aims to gauge users' opinion of possible inferences about the user's health (both mental and physical), activity at different times, sleep at different times and privacy threats in relation insufficient security of some devices. Participants were presented with 11 statements, shown below and were asked to indicate, for each statement, whether their reaction to the possibility of the statement is either Unconcerned, Uncomfortable or Concerned. The result can be seen below in Figure 16.

Figure 16 - Participants Reactions to Potential Privacy Inferences



- **S1**: Your employer can identify if female employees are pregnant through monitoring heart-rate data.
- **S2**: Your employer can identify what time you went to bed and your sleep quality each day.
- **S3**: Your employer uses the data collected from employees to get the best insurance rates for the company.
- **S4**: Your employer can monitor your sleep before and after an increase in responsibilities and identify if your sleep quality has been impacted and thus identify your ability to handle those responsibilities.
- **S5**: Your employer can monitor your BMI and weight over periods of time and potentially predict/identify obesity or anorexia.
- **S6**: Your employer can monitor your level of activity even when you are not at work, for instance, when you have informed them of an injury or illness or during leisure time.
- **S7**: Your employer can increase the health and fitness and overall well-being of its employees.
- **S8**: Your employer (on certain devices) can modify and essentially falsify data generated by your fitness tracker, like the number of steps you have made.
- **S9**: Your employer (on certain devices) can persistently monitor the location of your fitness tracker at a given point in time whilst at work.
- **S10**: Your employer can potentially identify if you are likely to be suffering from depression.
- **S11**: Your employer can use data collected from a fitness tracker to dispute an injury claim in court.

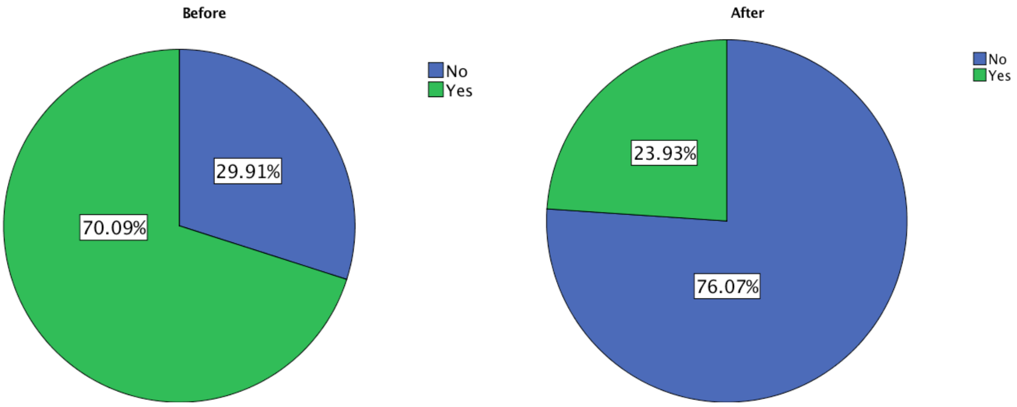
In general, participants seemed to be concerned about the statements, with 67% either ‘Concerned’ (60%) or ‘Uncomfortable’ (40%). As expected, over half the responses to S3 (Employers using data for best insurance rates – 59%) and S7 (Employer increasing well-being of employees – 67%) were unconcerned (included to minimise bias). On quite the reverse, participants were most concerned with S8 and S9, relating to the falsifying of data and persistent tracking whilst at work, with the ‘Concerned’ category recording 61% and 55% respectively. Statement S2, involving sleep timing and quality, was the only to score predominantly ‘Uncomfortable’, corresponding to 43%. Statements S11, suggesting the employer can use data to dispute claims in court and S6, signifying the employer can monitor activity away from work and S5, indicating employer's ability to identify anorexia and obesity, were of noteworthy unease to participants, 46%, 44% and 44% respectively specified they are 'Concerned' about these statements. Whilst females opted for concerned 3% more than males, as expected, males were less concerned about S1 relating to employers identifying if female employees are pregnant, with 34% opting for 'Concerned', compared to the females 43%. Females were also more significantly worried than males in relation to S5, relating to employers identifying anorexia and obesity, with 49% opting for 'Concerned', compared to the males 36%. There was a negative correlation between age and concern; concern decreases considerably with increase in age group, with 60+ opting for concerned 24% less than those under 18. In fact, those 60+ were unconcerned 76% of the time, compared to the 26-35's 38%. There was a positive correlation between those who do not currently use a fitness tracker and concern, with 71% of those who didn't opted for 'Concerned' (59%) or 'Uncomfortable' (41%) compared to those who did, with only 61% opting for 'Concerned (61%) or 'Uncomfortable' (39%).

Repeat question

In this section, participant's choice on whether they would be willing to share their data with an employee for an incentive is explored. One decided to choose a repeat question as a means of identifying if the hypothesis of the study is correct - that participants are generally unaware of the inferences that can be made from analysing their data, additionally, if they were made aware they would be less inclined to sharing their data. Firstly, the participants were presented with the question (would they be willing to share all of the informed collectable pieces of information with an employer for an incentive), then they were presented with the above 11 statements, then they were presented with the question again to see if making them aware of inferences had an impact on their decision. The results are displayed below in Figure 17.

The results clearly support the hypothesis of the study and show that awareness is woefully inadequate at this point in time, with participants shifting from 70% yes, to 76% no after being made aware of privacy inferences.

Figure 17 - Participants Willingness to Share with an Employer for an Incentive

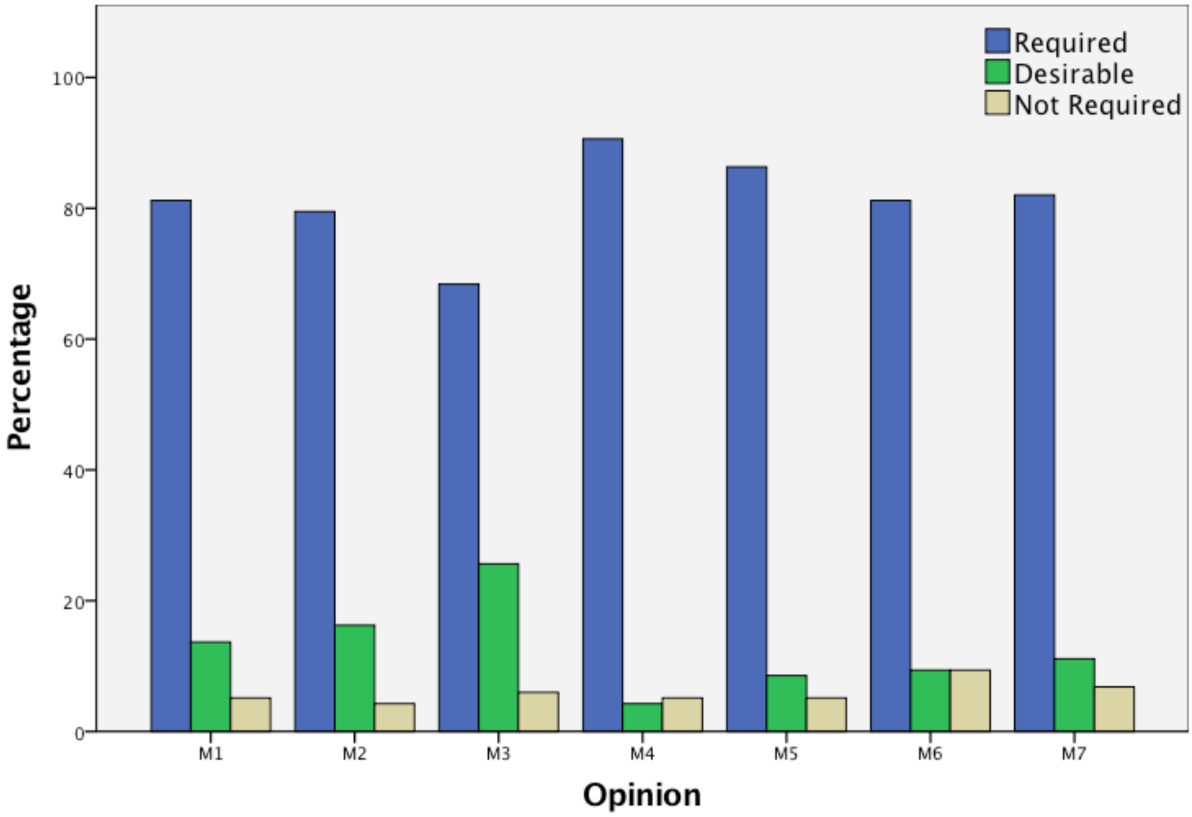


In the initial question there was a positive correlation between age and respondents saying ‘No’, as age increased the likelihood of them sharing with employers significantly decreased. Those 60+ opted ‘No’ 100% of the time, compared to under 18 and 18-25’s 25% and 28% respectively. Those 60+ remained unwilling to share, there was no other correlation in age after being informed. Gender played a role, males initially were 7% more likely to have chosen ‘No’ than females. In addition, once being informed of potential privacy inferences, males stood their ground more and were 2% more likely to opt for ‘Yes’. Unsurprisingly, those who currently use a fitness tracker were in both instances of this question more likely to opt for ‘Yes’ (this is assumingly due to a greater prior awareness). This will help shape the recommendation section as it can be identified from this that awareness plays a big factor in influencing behaviour and increasing participation.

Managing Personal Information

Here, participants’ views on managing and controlling their data generated through ‘smart sensors’ in wearable devices are explored. This includes several aspects related to awareness and honesty, how employee’s data is shared, stored or viewed by their employers and whether employers need to only opt for specific devices. The following statements were presented to the participants at the end of the questionnaire, after being informed of the potential inferences, and they were asked to rate whether they felt each was: ’Required, Desirable or Not Required. Results are given in Figure 18 below; they show a substantial requirement for these to be used to prevent privacy threats when employers share data generated from wearable fitness trackers.

Figure 18 - Participants Desire for Managing Information Grouped by Statement



- **M1** - Employers should increase awareness of what types of data can be collected from wearable fitness trackers
- **M2** - Employers should be more open and honest and make employees more aware of the potential applications of their data
- **M3** - Employers should only receive employee's data in a grouped form so individuals can't be identified
- **M4** - Privacy policies should be put in place to protect employees and their data
- **M5** - Employees should always be given the option to "opt out" of wearing fitness trackers for incentives
- **M6** - Employees should have the right to ask employers to delete any data held about them obtained from a fitness tracker
- **M7** - Employers should only use fitness trackers fitted with appropriate security measures which protect employee's data

Overall, 81% of participants would suggest they are 'required', 13% are content with just 'Desirable' and only 6% think they are 'Not required'. In general, M4 was the most favoured, with 91% stating this was ‘Required’ and only 4% suggesting it was ‘Not Required’. The vast majority rarely saw ‘Not Required’, with M6 being the least popular, at 9%. Females were 6% more likely to choose ‘Required’ (84%) than males (78%), although both chose ‘Not required’ exactly the same amount (6%). A positive correlation generally existed between participants age (60+ were an anomaly choosing ‘Not Required’ 76% of the time) and their tendency to opt for ‘Required’. The younger groups (under 18 and 18-25) had the lowest desire for ‘Required’, with 82% and 80% respectively, with this rising to 93% and 90% for the older groups (36-45 and 45-60). As expected, participants who currently use a fitness tracker were less inclined to opt for ‘Required’ or ‘Desirable’ and did so 4% less.

Respondents Own Views and Opinions

Here, participants who kindly added some extra feedback at the end of the questionnaire with opinions and views are explored. This question removed the specific boxes and allowed participants to put down any additional methods which need to be considered to protect employee data (e.g. open ended response opposed to closed), as outlined in the questionnaire plan. In general, the comments were mainly around health professionals making use of the data which can be collected from fitness trackers and employee’s having greater control, there were some very useful inputs as outlined below.

One respondent can be quoted as saying “If privacy policies are put in place and written correctly there shouldn't be a big need and/or concern for people's privacy unless the company violate this.” This respondent also opted for ‘Required’ when presented with the M4 statement, relating to privacy policies being put in place to protect employee’s data. This respondent however touches on two good points which will help the recommendation section of this project. Firstly, the privacy policy has to be written correctly such that it fundamentally protects employees from discrimination and/or invasion of privacy. Secondly, there must be measures put in place to assist employees if the company choses to violate the policy such that violations can be detected and dealt with accordingly (perhaps laws). The action to be taken from this can be summarised by quoting another respondent, who very convincingly put forward a great statement “The type of data shared should be explicitly agreed between employer and employee. Various disclaimers should be documented which protect the employees' rights within an organisation in regard to any legal issues.”

Several respondents touched on an aspect which one had not touched on previously, but one which is very applicable and credible. This is in relation to health official’s access to data. One respondent can be quoted as saying “I would be willing to share such data with a health professional should it be required and only with my specific consent”, another said “Feedback to doctor/NHS medical record is more important than employer”. The comments suggest that participants feel that whilst employers may not necessarily require the data collected from the fitness trackers, health officials could benefit. Essentially the kinds of inferences (obesity, mental health) which can be made would be very beneficial for a health official to know in order to provide an applicable treatment, providing consent was given, this could prove vital in minimising the poor health of employees.

There were several control aspects touched on by respondents in relation to anonymity (“All data should be anonymized”), and what the employer can visibly see (“Employees should have more control over aspects the employer can see”). Anonymising data is a valid and credible point, although careful attention would have to be applied in workplaces with few employees as it could prove easy to identify who the data came from, regardless if anonymised (this was touched on in M3 above). In addition, it could prove beneficial for employees to have an interface in which they can control which aspects of the data collected they share with the employer (like that which is provided on personal profiles). However, given the questionnaire results in which many were persuaded by an incentive to opt in sharing data and then quickly changed their mind once being informed of the possible inferences, one feels awareness is more vital. In summary, inferences which are implicit in data over periods of time are not easily recognisable and it’s important to make employees aware, in addition to providing them with more control.

One respondent touched on everything one has mentioned above and added an additional comment about leisure time, they can be quoted as saying “would not be keen for a company to collate data about my whereabouts after works time as this is my personal time. Although I am not breaking laws or causing mischief I prefer to keep my private life private.” In addition, another respondent touched on this aspect and can be quoted as saying “I think that except for activity level items (steps, calories burned, etc.), employers should only collect/use (employee allowed) fitness tracker info collected during working hours, not personal time. So no GPS or heart rate in the evening or weekend, no sleep records on Friday or Saturday and definitely nothing on sick days (could be running to the loo or taking care of a sick family member) which could be misinterpreted and/or misrepresented”. Essentially this shows participants feel very strongly about the collection of information during their personal time for two reasons, firstly, they see this as their private time and secondly, because the data could be misinterpreted. These are both valid points and will help shape the recommendation section of this report, employees could well have a high activity on a sick day but could very well be looking after someone else, opposed to them being ill. The employer may interpret this as them lying, when in actual fact they were honest and doing a trustworthy deed. Furthermore, it is not up to the employer to be placing surveillance outside of work hours.

Interviews

In addition to the survey, an interview has been designed to extract more open ended responses. The interview is also used to identify any gaps in the proposed draft recommendations (M1-M7), or things that one may have not considered. The main intention of the interviews was to achieve the following:

1. Which recommendations participants felt were the most applicable
2. Any problems participants had with the proposed recommendations
    a. Specifically, any which they felt are not relevant
    b. Any which they felt would require additional input or altering
3. If participants felt the proposed recommendations were sufficient enough to protect their privacy and if they were put in place would it alter their intent to share with an employer

The interviews initially began by analysing each participant's awareness of fitness trackers (what they collect and the concept in general), along with a basic outline of what this project is intending to achieve. This moved onto identifying if they would be willing to share the information with an employer for an incentive. This question would then be presented again once presenting participants with possible privacy implications. Finally, the set of recommendations would be presented to participants.

Below outlines the response from one participant, the remaining 2 responses can be found in Appendix H.

Amy McDonough, VP & GM, Fitbit Wellness, could not specifically comment on the recommendations provided when approached, however, Amy directed me to Fitbit's wellness pledge, alongside a video of her testifying in front of the House of Representatives subcommittee on employee wellness. The wellness pledge has been incorporated in the recommendations to identify compliance. The speech has been written up and is alongside the other interview responses in Appendix H, it has also been addressed in the recommendations where possible (especially those in which Fitbit are not compliant).

Name: **Daniel Ide**

Interview time: **6:00pm**

Interview Date: **19th April 2016**

Dan is 23 years old and he works full time for a worldwide catering company. He attends the gym regularly and uses an Apple Watch to track his health and fitness. He likes to separate work and personal time.

> *I am very familiar with the collectable pieces of information, although this has developed significantly since I began using my Apple Watch.*
>
> *I do not share any of my data with anyone on any platform.*
>
> *I would not be willing to share with an employer for an incentive, I am keen to get involved at work, but would not like to be "tracked".*
>
> *I was not aware of any of those possibilities apart from obviously the employer being able to improve the health of its employees, they are very concerning and really make you think.*
>
> *Yes, I still would not be willing to share my information, in fact, I would go on to advise nobody to after those revelations.*
>
> *I don't really think it's up to the employer to inform you what is collected or what can be done with it, I think that's down to the employee to identify, it's down to the employer to not exploit that however. I think grouped form is great although I still feel that I am providing my data and with enough analysis it could be linked back to me from a group. Definitely think that only collecting data during work hours can only be a good thing, also think that incentives should be altered to meet this. A privacy policy is a good idea, it should be sure to include limitations as well what it does cover (so employees can identify the risks, as I said earlier I feel this is their responsibility not the employer). No brainer that you should be given the option to opt out and data about you deleted, this should be instant and not tied to incentive dates. Agree security should be sufficient although this affects the world and not just corporate wellness, also means the price could increase. Health officials having access to data could be beneficial for all involved, providing consent is given.*

> *I think that the manufactures should provide sufficient information such that the employer can seek and find what they need to know, not the employer.*
>
> *Yes, I feel this would improve the situation and minimise the implications you revealed to me, although I still would like to keep my work and personal life separate.*

The interviews and feedback from the end of the questionnaire essentially allowed multiple perspectives to be taken into consideration in relation to specific recommendations. Furthermore, the respondent's feedback was also useful in identifying aspects which previously were not thought about. For instance, ensuring that employers are also protected within their privacy policy. The feedback will be implemented when addressing each complete recommendation.

Recommendations / System and Device Requirements

This section sets out to identify a set of recommendations which fundamentally aim to protect user's privacy, in the context of sharing information with an employer for an incentive. This section also maps the recommendations against the current market leader Fitbit, providing a gap analysis (where they do not currently meet each proposed recommendation)[8]. Furthermore, this section will also identify the progress the market leader has made over time where possible (identifying if recommendations have or have not always been met). The recommendations (in blue) also have a set of accompanying requirements, both non-functional and functional. A functional requirement essentially specifies something the system should do; a non-functional requirement describes how the system works. Each requirement has a subsequent acceptance criterion, acceptance criteria are a set of statements, each with a clear pass/fail result, that specify both functional and non-functional requirements. In each of the recommendations the priority of the requirements has been identified by following the MoSCoW notation (Must, Should, Could, Won't). MoSCoW is a prioritisation technique which helps rank order of importance amongst requirements, this is not to say that all the requirements shouldn't be met, but rather some are more vital than others if faced with constraints, like time (Business Analyst Learning, n.d.). A template for the requirements is shown below in Figure 19. An additional compliance report has been completed in regards to Jawbone (another leading manufacturer), and can be found in Appendix I.

Figure 19 - Requirement Template

ID	
Requirement	
Justification	
Acceptance Criteria	
Fitbits Compliance	

[8] * Currently the majority of manufacturers in the market do not allow for visibility of their corporate well-being systems and as such it is not possible to carry out heuristic evaluations of their systems, but one can make use of what is publically available and provided by their VP Amy to determine gaps in meeting proposed recommendations.

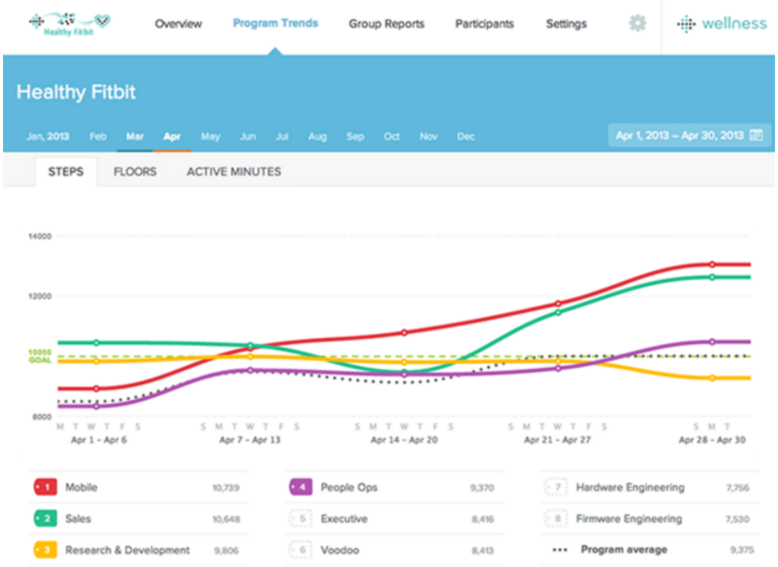
Participant's data must only be collected in aggregate form, apart from activity data, which must only be collected during working hours and must provide the user with the option to allow for this to be collected at an individual level (activity data is required to see if some individuals meet health targets). Employee's data must only be collected once 'opting in' and they must be provided with an option to 'opt out', with their data being removed if so. Participant's weight and BMI and sleep timings (e.g. Fred went to bed at 7pm) must never be tracked.

Table 1 - R1.1

ID	R1.1
Requirement	The interface **must** only display participant's data in aggregate form across all platforms and devices once they have 'opted in'. Except for when individuals have 'opted in' to allow for individual activity data, in which case the interface **must** display individual activity data.
Justification	This was identified in the PWC (2015) study and the qualitative analysis that individuals were more open to participating and protected, when data is aggregated (it prevents employer from identifying private information which can invade privacy related to individual data, as identified in the data analysis). This links to requirement R3.7. Activity data may be required at individual level to see if an individual meets requirement for cheaper health care.
Acceptance Criteria	The Interface displays only an aggregated chart of participant's data. The interface only includes individual activity data once users have been provided the opportunity to 'opt in', and opt to do so. The interface is the same on mobile and desktop.

<table>
<tr>
<td><b>Fitbit Compliance</b></td>
<td>Fitbit are <b>compliant.</b> Fitbit display data in an aggregate form and activity data in an individual form (only once an individual has opted in, as shown in Figure 22 below) as shown in Figure 20 below.

Figure 20 - 'Aggregate Tracking'[9]



</td>
</tr>
</table>

Table 2 - R1.1.1

ID	R1.1.1
Requirement	The interface **must** provide an option to 'opt in' to wellness program.
Justification	The user must be granted the choice to 'opt in' to the program, this links to requirement R3.1.1.
Acceptance Criteria	The user Is presented with a dialogue box asking them to 'opt in' prior to data being tracked.
Fitbit Compliance	Fitbit are **compliant.** See Figure 22 below. Amy's speech also highlighted the importance of 'opting in' and voluntary contribution to the program, this is something Fitbit are very passionate about.

Table 3 - R1.1.2

ID	R1.1.2
Requirement	The interface **must** provide an option to opt in for individual activity data to be tracked.

[9] https://www.fitbit.com/uk/fitbit-wellness - Accessed 4th April 2016

Justification	The user must be granted the choice to 'opt in' to the allowing of individual activity tracking.
Acceptance Criteria	The user Is presented with a dialogue box asking them to 'opt in' prior to individual activity data being tracked.
Fitbit Compliance	Fitbit are **compliant.** See Figure 22 below.

Table 4 - R1.1.3

ID	R1.1.3
Requirement	The interface **must** provide the option to select which days/times of the week users data is made available.
Justification	Qualitative research identified that users were not happy with being tracked outside of work hours, the data analysis study shows inferences which are derived from this type of surveillance.
Acceptance Criteria	The interface does not include any data which is outside the individuals working hours.
Fitbit Compliance	Fitbit are **not compliant.** Fitbit current allow for the tracking outside of work hours (Saturday/Sunday), be it aggregated or individual and provide no control over collection timings. (Shown above in Figure 20 and below in Figure 21.)

Table 5 - R1.1.4

ID	R1.1.4
Requirement	The interface **must** provide an option for individuals to 'opt out' of wellness program.
Justification	The survey identified that users wanted the option to 'opt out'. Relates to requirement R3.9. There should be no punishment in doing so.
Acceptance Criteria	The interface provides users with the option to revoke access from a third-party.
Fitbit Compliance	Fitbit are **compliant.** Fitbit currently provide the option to revoke third-party access. Amy's speech addressed this, Fitbit believe that

	participation should be voluntary and there should be no repercussions for saying no or ‘opting out’.

Table 6 - R1.1.5

ID	R1.1.5
Requirement	The interface **won’t** include weight, BMI or sleep timings data.
Justification	Survey identified this was a concern for individuals in regards to tracking of sleep timings, and respondents were very unwilling to share body data. Data analysis has identified that these are a catalyst for privacy implications and serve no real purpose being tracked (Average aggregate time spent in bed still provides an idea of insomnia).
Acceptance Criteria	The interface contains no information about participant’s weight or sleep. The system does not store any information relating to employee sleep or weight.
Fitbit Compliance	Fitbit are **Not compliant.** Fitbit currently provide the option to track individual sleep timings with consent, but do not provide the ability to track employee’s BMI or weight. Fitbit allow for the displaying of weight, BMI and sleep timings on individuals profiles (as per ones experiment this can lead to third-parties getting visibility of data without consent, providing profile set to ‘public’ or “friends and family”).

R1.2-1.3.1 – Amy’s speech identified that Fitbit believe that community is key to fostering healthy behaviour. In addition, Fitbit believe that by promoting fun and rewarding community driven experiences, you will ultimately reap the rewards of stronger results. Therefore, comparison metrics across teams and the ability to set goals are key to supporting this belief, it’s clear why there is compliance across the board here.

Table 7 - R1.2

ID	R1.2
Requirement	The interface **should** display participant's information grouped by team.
Justification	This could allow for comparison of teams across a company to encourage participation. Must be careful in teams where it could be possible to identify individuals.
Acceptance Criteria	The interface displays all teams' aggregate information separately.
Fitbit Compliance	Fitbit are **compliant.** Fitbit currently provide the option to group information by teams, as shown above in Figure 20.

Table 8 - R1.2.1

ID	R1.2.1
Requirement	The interface **could** provide comparison metrics.
Justification	This could provide motivation to participate and retain Fitbit's competitiveness.
Acceptance Criteria	The interface allows for the comparison of teams in relation to aggregate data. E.g. team 1 done 20,000 steps this week, team 2 did 30,000.
Fitbit Compliance	Fitbit are **compliant.** Fitbit allow for the comparison against teams and the overall program as shown above in Figure 20, as-well as individual comparisons against everyone (e.g. how do I compare to a 50 year old man).

Table 9 - R1.3

ID	R1.3
Requirement	The interface **must** display when targets have and have not been met (e.g. 1,000 steps a day)
Justification	This is fundamental, incentives are given on the basis of completing goals.

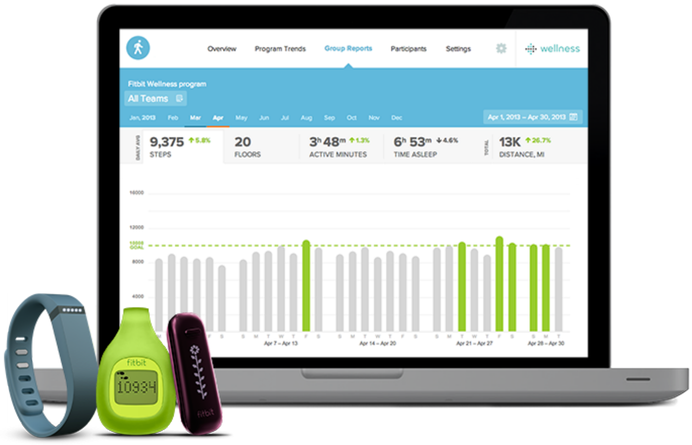
Acceptance Criteria	The Interface displays when all targets have and have not been met.
Fitbit Compliance	Fitbit are **Compliant.** Figure 21 shows the UI (User interface) Fitbit use. The green bars are those that have met the target and the green dotted line is the set target. *Figure 21 - Fitbit Wellness UI - Goals*[10]  Overview Program Trends Group Reports Participants Settings wellness Fitbit Wellness program All Teams Jan, 2013 Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Apr 1, 2013 – Apr 30, 2013 DAILY AVG 9,375 ↑5.8% STEPS 20 FLOORS 3h 48m ↑1.3% ACTIVE MINUTES 6h 53m ↓4.6% TIME ASLEEP TOTAL 13K ↑26.7% DISTANCE, MI 16000 12000 10000 GOAL 8000 4000 fitbit 10934

Table 10 - R1.3.1

ID	R1.3.1
Requirement	The interface **must** allow for the administrator to set goals.
Justification	The system must allow for the setting of goals in order for employees to work towards them and receive an incentive.
Acceptance Criteria	As an administrator I have the ability to set goals.
Fitbit Compliance	Fitbit are **Compliant.** Fitbit boast on their well-ness page[11] that they offer the ability to set goals.

[10] https://www.fitbit.com/sg/fitbit-wellness - Accessed 7th April 2015

[11] https://www.fitbit.com/sg/fitbit-wellness - Accessed 7th April 2015

Fitness tracker should be fitted with appropriate security measures which protect user's data.

All of the below requirements are applicable to Amy's speech. Amy identified that whilst programs aim to give employee's the opportunity to live healthier, happier and more active lives, inherent in this mission is the need to implement data security. Fitbit are not compliant in several instances regarding device security, however, the speech perhaps gives an insight into the future of this area, and perhaps compliance may be addressed in the near future to support the mission.

Table 11 - R2.1

ID	R2.1
Requirement	The unique identifier broadcasted by the device **must** not be fixed e.g. The device must include LE privacy (changing MAC address).
Justification	This prevents the persistent monitoring of devices by a third party (employer).
Acceptance Criteria	The unique identifier (MAC Address) broadcasted by the device are not fixed.
Fitbit Compliance	Fitbit are currently **not compliant**. Hilt, et al., (2016): acknowledged that Fitbit stated the following in regards to becoming compliant in the future: *Fitbit stated it was interested in implementing LE Privacy and that their wearable devices could support it. However, the company asserted that the fragmented Android ecosystem, in which some devices do not support LE Privacy, prevented them from implementing the feature.*

Table 12 - R2.2

ID	R2.2
Requirement	The system **must** have HTTPS encryption
Justification	Prevents eavesdroppers from collecting and tampering with user's data. (Hilt, et al., 2016) (E.g. steps cannot be falsified to meet

	incentives, important also in regards to law as data can be used to influence court cases. Also prevents visibility of data to motivated parties)
Acceptance Criteria	User page requests are encrypted and decrypted, as well as pages returned by the web server.
Fitbit Compliance	Fitbit are **compliant**. This is a basic technical security mechanism (encryption) for protecting the transmission of personal information, Fitbit have always been compliant in meeting this.

Table 13 - R2.2.1

ID	R2.2.1
Requirement	The system **must** use SSL Pinning
Justification	*Certificate pinning involves an application relying on its own set of trusted certificates when communicating with other servers using transport layer encryption (i.e. TLS). By using its own set of certificates, the application does not inherently trust certificates identified as being legitimate by the device operating system. This protects against man in the middle attacks.* (Hilt, et al., 2016).
Acceptance Criteria	Application flags third party installed additional certificate authorities as untrusted and ceases processing the HTTP request.
Fitbit Compliance	Fitbit are **not compliant.** They do not currently use SSL Pinning as identified by Hilt, et al., (2016).

Employers have a privacy policy which fundamentally protects both them and employees.

Amy’s speech highlighted how important Fitbit feel privacy policies, but also laws and regulations are in this market. Fitbit believe that employers should make employees aware of how their data will be used, R3.3 & R3.5 focus on this aspect (Fitbit are compliant in both). Fitbit also state they are focused on supporting employers with identifying and streamlining applicable laws and regulations that govern the wellness programs, Fitbit currently comply in this area (R3.4), but do not provide users with the ability to read an employer’s policy prior to partaking (R3.1.1). Amy’s speech did little to address limitations, this is expected as it is bad press, but this fundamental and should be provided to employees. Finally, incentives are touched on numerous times in Amy’s speech, as is the focus on not punishing those who do not partake (this is key for those who feel they have no choice but to partake to obtain an incentive). Incentives drive participation and thus, results (which the speech highlighted are both incredible in regards to Fitbit).

Table 14 - R3.1

ID	R3.1
Requirement	The system functionality **must** be driven by policy whenever possible, across all platforms and devices.
Justification	This is fundamental, the policy will have requirements (see 3.2-3.9) which protect users (employee’s data is governed by employer’s policy when ‘opting in’) and it’s important the system matches these requirement to ensure compliance.
Acceptance Criteria	The system functionality correlates to the privacy policy.
Fitbit Compliance	Fitbit are **compliant**. Currently, Fitbit align all functionality with their privacy policy. This isn’t to say that their privacy policy is perfect (it has improved drastically in the last 18 months), but that they align the functionality of their devices and system to meet what they say they are going to do. Fitbit’s privacy policy[12] has previously been ambiguous, for instance the section regarding default settings previously stated:

[12] https://www.fitbit.com/us/company/previousprivacypolicy - Accessed April 8 2016

	The privacy settings on new Fitbit accounts are set to reveal minimal data about you with the purpose of getting you active and involved with Fitbit This is very ambiguous; it does not mention what is minimal data. This has been changed and the default setting is now always set to private for all collectable pieces of data. In addition, in relation to employees directing them to share data with employers, Fitbit state that this data is then governed by the employer's privacy policy, unless consent is revoked in a user's Fitbit account settings. Whilst Fitbit therefore have improved in enhancing its privacy policy with respect to user's privacy and give them control to whom their data is shared with, it's important to take into consideration the requirements of the employer's privacy policy under which it will then be governed. (Requirements 3.2-3.9). Amy's speech showed how strongly Fitbit believe in policies that fundamentally protect users' data.

Table 15 - R3.1.1

ID	R3.1.1
Requirement	The system **must** have a pop-up message in which the user must agree to the policy before giving access to data to third-parties.
Justification	It is important that the users agree to the policy prior to the data being made available to the third-party (employer).
Acceptance Criteria	The policy includes technical limitations of the system and devices
Fitbit compliance	Fitbit are **not compliant.** Despite Informing them of basic terms (shown in Figure 22 below) it does not allow the user to read the third-party policy which governs those terms prior to joining the program.

Table 16 - R3.2

ID	R3.2
Requirement	The policy **must** include technical limitations with the system and devices (e.g. no Bluetooth LE privacy).
Justification	User's need to understand the limitations in the security of the system and devices to understand if they are making themselves vulnerable to privacy implications.
Acceptance Criteria	The policy includes all technical limitations of the system and devices
Fitbit compliance	Fitbit are **not compliant**. Fitbit currently do not outline in their policies any limitations their system or devices provide (including accuracy, in which Fitbit only accept it is not intended to match medical equipment's accuracy). As outlined in the security section previously Fitbit gave little examples of data security, however Fitbit previously offered a better example in their prior privacy policy[13]: *We use a combination of firewall barriers, encryption techniques and authentication procedures, among others, to maintain the security of your data and to protect Fitbit accounts and systems from unauthorized access. When you register for the Service, Fitbit requires a password from you for your privacy and security. This password is stored in an encrypted fashion on our systems.*

Table 17 - R3.3

ID	R3.3
Requirement	The policy **must** include what information the employer has access to.

[13] https://www.fitbit.com/us/company/previousprivacypolicy - Accessed 6th April 2015

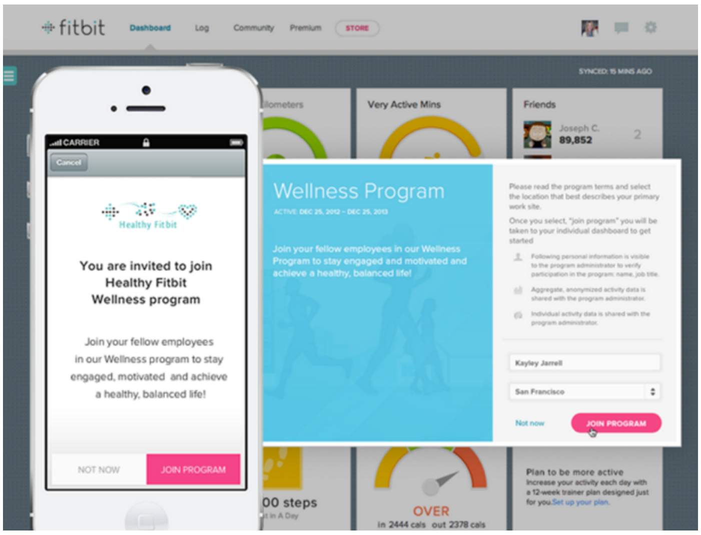
Justification	Awareness was identified as a key requirement from the survey, it is vital employee's know what they are giving away when participating in well-being programs.
Acceptance Criteria	The policy outlines in full all information which will be visible and accessible to the employer once an employee 'opts in'.
Fitbit Compliance	N/A (This falls under the employer policy) (However Fitbit are **compliant** in informing individuals of what they are giving away when 'opting in' as can be seen in Figure 22 below.) *Figure 22 - Well-Being 'Opt in' Page*[14]  You are invited to join Healthy Fitbit Wellness program Join your fellow employees in our Wellness program to stay engaged, motivated and achieve a healthy, balanced life! Wellness Program ACTIVE: DEC 25, 2012 – DEC 25, 2013 Join your fellow employees in our Wellness Program to stay engaged and motivated and achieve a healthy, balanced life! Please read the program terms and select the location that best describes your primary work site. Once you select, "join program" you will be taken to your individual dashboard to get started Following personal information is visible to the program administrator to verify participation in the program: name, job title. Aggregate, anonymized activity data is shared with the program administrator. Individual activity data is shared with the program administrator. Kayley Jarrell San Francisco Plan to be more active Increase your activity each day with a 12-week trainer plan designed just for you.Set up your plan. fitbit Dashboard Log Community Premium STORE SYNCED: 15 MINS AGO CARRIER Cancel Healthy Fitbit NOT NOW JOIN PROGRAM ilometers Very Active Mins Friends Joseph C. 89,852 2 Not now JOIN PROGRAM 00 steps t in A Day OVER in 2444 cals out 2378 cals

Table 18 - R3.4

ID	R3.4
Requirement	The policy **must** include which laws the program is covered under.
Justification	It is important to the employee's know how they are protected, this was identified as a key comment from the survey (protect violations) and interviews (protect both the employee and employer).
Acceptance Criteria	The policy outlines in full, with applicable examples, which laws the well-ness program is covered by.
Fitbit Compliance	N/A (This falls under the employer policy) (However, as identified in the dimensions of the problem section, Fitbit do state laws under

[14] https://www.fitbit.com/sg/fitbit-wellness - Accessed 7th April 2015

	which they operate, but provide no examples. Fitbit have recently offered **HIPAA compliant** capabilities, a big step in protecting wellness customers. In a press release[15] Fitbit stated: *The U.S. Health Insurance Portability and Accountability Act (HIPAA) is the primary U.S. law governing the security and privacy of personal health information used by health insurance plans and other covered entities.* *We prioritize protecting our consumers' privacy and keeping their data secure")*

Table 19 - R3.5

ID	R3.5
Requirement	The policy **must** include who the employer will share employee's data with.
Justification	It is vital that users know the potential utilisation of their data by the employer and third parties, this was highlighted as a key requirement in the survey, and this will also be linked to R3.6 as other third parties will have their own privacy policy.
Acceptance Criteria	The policy outlines in full, with examples, who the employer will share participants of well-being programs data with.
Fitbit compliance	N/A (This falls under the employer policy). (However, Fitbit are **compliant** in informing users in their policy briefly of whom the data will be shared with (although provide little examples e.g. "interested audiences) and in what state (aggregated), and set by default profiles to 'private'. However they were not previously so considerate and prior to August 8 2011, had set information to default 'public.

[15] https://investor.fitbit.com/press/press-releases/press-release-details/2015/Fitbit-Extends-Corporate-Wellness-Offering-with-HIPAA-Compliant-Capabilities/default.aspx - Accessed 6th April 2016

Table 20 - R3.6

ID	R3.6
Requirement	The policy **must** include what separate privacy policies the employer is following.
Justification	If the employer is to share data with an insurance company for instance, in order to offer health care rewards, it is important it outlines the privacy policy of that insurer so employees can identify what they are governed by outside of the employer.
Acceptance Criteria	The policy includes in full each policy which is also followed by the employer in addition to the employer privacy policy.
Fitbit Compliance	N/A (This falls under the employer policy). (However, Fitbit are **compliant**. They inform users of the cookies and data analytics platforms they use in their privacy policy[1] and the associated privacy policies of those platforms (including MixPanel[16] and Google[17]). They also inform users that their data is governed by a third-party privacy policy when users direct Fitbit to share with them.

Table 21 - R3.7

ID	R3.7
Requirement	The policy **must** include what measures have been put in place to stop identifying individuals from grouped data
Justification	Experts identified that results can be re-identified by using public databases and the grouped data (Rijmenam, 2016).
Acceptance Criteria	The policy outlines in full each measure and law that is put in place to prevent identifying individuals from grouped data.

[16] https://mixpanel.com/privacy/ - Accessed 6 April 2016

[17] https://www.google.com/intl/en/policies/privacy/ - Accessed 6 April 2016

Fitbit Compliance	N/A (This falls under the employer policy). (However, Fitbit are **compliant.** They state in their privacy policy[18] the following: *When we provide this information, we take legal and technical measures to ensure that the data does not identify you and cannot be associated back to you.* However, this is slightly ambiguous in that it provides no explicit examples.

Table 22 - R3.8

ID	R3.8
Requirement	The policy **must** include what incentive the employer can expect to receive in return for participating in the well-being program and meeting targets.
Justification	Employer's behaviour is influenced by incentives as identified by PWC (2015) and the survey (70% said they would share data with their employer for an incentive), although this shouldn't compromise privacy, it is still important to identify what they can expect in return for parting with data. Interviews also identified that the reward was key to their willingness to participate. Must however ensure that the incentive is not overly generous, this could force less fortunate employees to part with data through being enticed with a deal they cannot refuse, when they otherwise would not.
Acceptance Criteria	The policy outlines in full what the employer will receive in return for completing targets.
Fitbit Compliance	N/A (This falls under the employer policy). However, Amy's speech highlighted that by engaging participants and rewarding them you can expect to see better participation rates and results. Fitbit therefore support the notion of incentivising participants.

[18] https://www.fitbit.com/uk/privacy – Accessed 8th Feb 2016

Table 23 - R3.9

ID	R3.9
Requirement	The policy **must** include how employees can go about being forgotten (data held about them being removed).
Justification	This was identified as a key requirement in the qualitative analysis, it is important participants are given the option to remove any data about them from the system.
Acceptance Criteria	The policy outlines in full how the employee may remove data held about them. The system must not contain information about this employee once request has been made, within two weeks.
Fitbit Compliance	N/A (This falls under the employer policy). (However, Fitbit are **partially compliant** in informing users about (and giving) the right to delete their data. Although, Fitbit will continue to use de-identified historical data. Fitbit also provide the option for users to revoke access from a third-party (employer), however, Fitbit do little to explain if this also deletes the data held by said third-party and pass the responsibility onto the third-parties policy.)

Employee’s data can potentially be shared with a health official, providing employee has given consent.

Table 24- R4.1

ID	R4.1
Requirement	The user **must** be allowed to control if they would like to share data with a health official or not, within their privacy settings.
Justification	Participants of the survey stated they would be willing to provide data to a health official in order to minimise the risk to their health, this differs from the employer having access.
Acceptance Criteria	As a user I am able to share my information with a health official by selecting a tick box within the privacy settings interface.
Fitbit Compliance	Fitbit are **Not Compliant.** However, Amy’s speech highlighted that there is a shift from focusing on diet and exercise to mental health (amongst other things). This could therefore be seen in the future.

Table 25 - R4.1.1

ID	R4.1.1
Requirement	The system **must** not allow health officials to have access to data from the interface if the user has not selected this in their privacy settings.
Justification	It is important that the users agree to visibility of data prior to the data being made available to the health official.
Acceptance Criteria	Data which has not been selected to be shared with health officials in not displayed by Fitbit to health officials.
Fitbit compliance	N/A.

Table 26 - R4.1.2

ID	R4.1.2
Requirement	The user **should** be allowed to control what aspects of their data the health official will see.
Justification	Users may only wish to share certain aspects applicable to their condition with health officials whilst keeping other aspects private.

Acceptance Criteria	Data which has not been selected to be shared with health officials in not displayed by Fitbit to health officials.
Fitbit compliance	N/A

Manufacturers should inform users of the types of data collected and inform them of privacy inferences which are implicit in their data and not noticeable from the interfaces they are accustomed to. Manufacturers should also provide accessibility to user's data in the form of an export to allow them to conduct their own analysis.

Table 27 - R5.1

ID	R5.1
Requirement	The interface **must** have information informing users of the types of data collected and inform them of potential privacy inferences which are implicit in the collected data.
Justification	Participants of the survey and interviews stated they felt it was up to the manufacturer to provide and employee to become more aware and not the employer.
Acceptance Criteria	The interface informs users in full about the types of information collected by the device and the potential inferences that can be made from it.
Fitbit Compliance	Fitbit are **partially compliant.** Fitbit's website currently does an excellent job at informing users of the specifications and functionality of their various bands and watches. In fact, even back in 2008 when Fitbit prepared to launch their first tracker they included a comprehensive FAQ (Frequently asked questions) section. The section outlined how the Fitbit worked and what it tracked, how accurate the device was, how the sleep tracking worked and its potential, and even how the data is taken from the device to the website. Since 2008, Fitbit have maintained this strong approach of informing users and has even established an online community and customer support department to further help users. Fitbit do not inform user of any privacy inferences which can be identified from collected data.

Table 28 - R5.2

ID	R5.2
Requirement	The system **must** provide the option to export collected data to a file.
Justification	Access to data is fundamental for users to be able to analyse their data and identify any trends themselves which may be useful.
Acceptance Criteria	As a user I have access to an exportable file of all minute by minute data.
Fitbit Compliance	Fitbit are **partially compliant.** Although Fitbit provide export functionality they do not provide it to the lower levels of granularity despite it being possible. In addition, Fitbit do not provide heart rate data. Fitbit also charge for the access (with the exception of one month's free export) and only allow for 30 day instalments (although they previously did not have this restriction).

Changed and Extra Deliverables

Changed Deliverables

The initial plan stated the goal of producing and disseminating two questionnaires. The first questionnaire would be to identify the current awareness and sharing behaviour of participants in relation to wearable fitness trackers. The second would be to identify if user's behaviour and subsequent need for greater awareness, control and visibility changed, once presented with privacy inferences derived from the collection and provision of data. However, given the time constraint surrounding the project it was decided to merge the two questionnaire ideas into one questionnaire, with multiple sections. In addition, the information required in order to model the problem was identified from up to date research, which was sufficient in providing enough detail. Thus, there is only one deliverable in regards to questionnaires. The intention was also to interview participants in regards to the questions to gather more open ended responses. Furthermore, a focus group was planned to identify the feasibility of recommendations. Due to the time constraint and the logistics behind organising a Focus Group, one decided it would be more beneficial to have one set of interviews to identify feasibility of recommendations. The questionnaire also received 117 respondents (of which some responded with open ended answers), which meant that it provided a great deal of information and eradicated the need for both interviews and a focus group. I was also able to obtain information from a credible source (VP Fitbit Corporate Wellness) which further eradicated the need for a focus group.

Extra Deliverables

One has taken the opportunity to define each recommendation as a set of functional and non-functional requirements. Although not initially planned, this could prove very effective in allowing future work a baseline for producing a system and accompanying policy, these will protect user's privacy. Although the requirements are not a complete set and one does not believe they all are applicable to every situation, they can still be utilised and adapted as deemed fit. One also utilised two additional data-sets (in addition to a personally collected one) in the data analysis, this enabled much more thorough data mining and identification of privacy inferences. One has also looked into two case studies which support the project (Appendix A and B), both have transformed in modern times and are relevant to the area studied. One has also mapped requirements against an additional manufacturer, Jawbone. One also carried out a successful experiment for obtaining user data without permission, this wasn't planned.

Evaluation of Work Completed and Reflection on Learning

The selection of appropriate methodologies has been of paramount importance in the effective completion of this project. The use of Soft Systems Methodology to model the dimensions of the problem in relation to stakeholders involved was particularly useful. The C.A.T.W.O.E Analysis, Root Definition and Conceptual model proved very effective in identifying how the system should be working and what needs to be done in order to achieve this. Consequently, the model was able to drive an analytical data study which essentially identified privacy inferences, these inferences are the backbone to a large part of the questionnaire. Therefore, the ultimate strength of the project lied in the ability to not only produce applicable and relevant background research to enable the modelling of the problem dimensions, but also the identification of privacy implications from the data analysis study. The questionnaire results supported the hypothesis of the study and extracted exceptionally useful responses (both closed and open ended), from a large number of respondents. The questionnaire responses and interview results were also the backbone of the recommendation section, having such a large number respond proved vital in establishing a complete set which took into consideration multiple perspectives. The recommendations were tailored from extensive feedback and as a result were more comprehensive. The weakness of the project was the inability to have access to corporate well-being systems in order to do a thorough gap analysis. None the less, with publically available information and making use of the content provided by Amy, VP of Fitbit's wellness business, it was possible to carry out basic gap analysis of two manufactures. In addition, it would have been even better had one of been able to do more widespread data analysis with different types of data (heart-rate, GPS), but this was met with difficulties (explained below). Furthermore, had one of been able to utilise SPSS's 'missing data' feature (it was not included in the version I was able to obtain and costs a considerable amount), it would have allowed for more comprehensive data analysis where the data had gaps in the acquired datasets.

SSM

Despite identifying through background research the dimensions of the problem, I was still unclear as to how the project pieced together as a whole. SSM allowed me to identify the problem as an undivided picture, opposed to each individual separate area of the problem dimension, which in itself was problematic. The structure and clarity of the otherwise amorphous problem situation allowed for a clear focus on the particular system under investigation, this essentially provided me with greater clarity on the project as a whole. SSM allowed me to identify links between areas of the project, for instance, the data analysis was driven by the control action required to identify privacy inferences. This would subsequently go onto drive a questionnaire asking for participant's level of concern in relation to those inferences. The inclusion of multiple perspectives in relation to stakeholders in SSM meant that derived recommendations had a higher likelihood of being deemed feasible from all of those involved in the system. In addition, the identification and inclusion of multiple stakeholders and environmental factors helps to link patterns amongst stakeholders, both when they agree and disagree, as well as identifying the assumptions the system is based on. The only weakness I found during using SSM is that by nature it is a systems way of thinking and does not inherently provide a formal structure or approach to tackling a system. This meant that at times it was difficult and complex to identify problems within the dimension, and it was problematic in itself to find where they fit in regards to the overall system.

Questionnaire/Interviews

A large area of the project was the creation and distribution of a questionnaire. This would be the first time I would ever complete a questionnaire and thus it was deemed necessary to identify a series of objectives, this would ensure that it achieved what was intended when choosing this as a method. I also researched the best approach in regards to design and layout. The research was useful in identifying suitable length of the questionnaire and applicable designs, these would help remove ambiguity and really attain what was deemed required from the objectives. However, I feel there was a missed opportunity in regards to the proposed recommendations at the end of the questionnaire. I feel that it could have been much more beneficial to the overall recommendation section if more time was spent identifying methods for protecting user privacy, specifically in regards to control and increased visibility of user data. In addition, it was clear that respondents were inclined to want every recommendation and thus, it became hard to gauge which were the most important. However, the number of respondents and the inclusion of an open ended question at the end, meant that I was able to make use of excellent amount of feedback from participants. Respondents providing extra feedback was not required, but proved very effective in shaping the recommendations. One particularly useful input was several respondents touched on the forwarding of data to health official's, which was a route I initially had not thought about, but was extremely relevant. The analysis of the questionnaire required the steep learning curve of SPSS, although it was time consuming and difficult to learn, it proved excellent in allowing for in depth analysis in regards to mapping questions against differing user profiles (e.g. identifying people who currently use a fitness tracker were more inclined to share with an employer even if they were informed of possible privacy inferences). In regards to interviews, they allowed more focused direct and open feedback from a respondent and allowed for the complete removal of any ambiguity in questions, as they provided the opportunity to clarify questions. The feedback was therefore not only more reliable, but also actually contained several new insights into the proposed recommendations. The negative aspects of the interviews were that they proved to be characteristically subjective and thus, it was challenging to tackle this when analysing the feedback. The information provided by Amy McDonough, VP & GM Fitbit Wellness, was excellent in identifying the holistic picture of the wellness market, from benefits to their vision and beliefs, all of which are key to this report. This inevitably helped address recommendations and compliance in regards to Fitbit. I think by attaining feedback from such a credible and applicable source shows the initiative I used when completing this project.

Data Analysis

The support of the identification of privacy inferences was to acquire real-world data from a fitness tracker. I feel that I done incredibly well to obtain three different sets of data, which all had different types of data, all over differing periods of time. The benefit of this was that it allowed for more complete analysis and ultimately the identification of more patterns (e.g. comparing health year on year or sleep over a month). I found this section particularly difficult and initially struggled to plan how I would go about mining the data. I had a rough idea of the inferences I thought would be possible, but had little idea of how to mine the data such that it would show the possibility. Dr Alia Abdelmoty gave me the insight as to look at the data from a minimalistic perspective (e.g. how active was someone over a month/year/day), rather than looking directly for inferences. This essentially meant that by simply mapping the data I could visualise trends and add more detail to these trends in order to show possibility of inferences. I could not export heart rate data using Fitbit's website (currently doesn't provide this feature) and was unable to obtain any from other sources. I also could not manage to obtain location data, although I collected this data over a month, upon exporting the data, it was corrupt (Fitbit's forums state this is common). I feel that if I was able to obtain these pieces of data I would have been able to do even more wide-ranging analysis and identify further potential privacy inferences implicit in user data. None the less, I managed to identify a number of inferences implicit in user data, these have not previously been discovered.

Recommendations

The recommendations were an accumulation of the whole report and its separate deliverables. SSM, qualitative and quantitative research all identified key considerations which were taken into account when completing the recommendations. SSM identified the overarching recommendations in regards to control, awareness and security, whilst addressing the environmental constraints (e.g. laws). Data analysis identified inferences from which it was possible to derive recommendations which can address them (e.g. do not monitor weight or BMI and you would remove the ability to identify eating disorders). The interviews allowed for more in depth opinions and differing visions of each recommendation. As mentioned, I feel the questionnaire could have done more in terms of recommendations for protecting privacy, specifically in regards to control and visibility. On reflection, giving users greater access and thus visibility to their data over longer periods of time than the snapshot they are accustomed to, would have been a good recommendation to present to respondents for feedback. Providing users with more control of their data has been a key element throughout the recommendations section, but was not heavily touched on when gathering qualitative data and rather just addressed the aggregation of user data. It could have been beneficial to gauge more precise feedback, rather than just sharing preferences. Through carrying out a gap analysis in the form of compliance statements against acceptance criterion, it was essentially then possible to revisit the conceptual model and identify which areas in the real world system differ from the model. Mapping two different manufacturers allowed for two different perspectives and showed how companies differ (or are similar) in their approach to this new market.

In general, the completion of this project has essentially been making use of an accumulation of everything I have learnt during university and placement year, alongside the development of new skills. The project has significantly improved a number of the skills as outlined below.

Completing a project of this size independently over several months has meant that I have built upon my time management skills. In particular, the prioritisation of work load has been a key focus during the project. There were areas of the project seen as fundamental for the consolidation of it as a whole, such as SSM and the data analysis. The prioritising came hand in hand with scheduling key activities to ensure enough time was allocated to each, although I lost time at the beginning of the project, due to worries surrounding my hypothesis and personal adversity, perseverance and guidance from weekly meetings with Dr Alia Abdelmoty meant I was able to get back on track, and even ahead of my plan.

A key skill which I have developed during university and applied to this project was critical thinking. I had to see logical connections between sections and within each section The project is essentially a product of independent thinking and has seen me significantly develop my ability to reason with ideas and ultimately construct logical, structured arguments. Consistently I have had to evaluate research alongside the guidance from my supervisor, as well as observe when conducting the interviews. Essentially the evaluation led to identifying how justifiable arguments or ideas were in relation to supporting the hypothesis of the study and thus, if they should be included. Complexity is inevitable in a project of this size and it took great motivation and consistent working patterns to eradicate complications, this required in depth critical thinking.

My research and reading skills have also been utilised heavily and advanced throughout this project. A key to success in this area was the documentation of everything I found, this enabled critical thinking at a later stage. The identification of relevant material called for quick thinking and lots of reflection. I had to quickly identify if material was relevant, then reflect in a systematic way, using logical reasoning, if it was going to support the project (decision making has therefore also been heavily used and improved). This was difficult at first as I was not naturally able to digest research papers to identify key arguments, but rather taken back by the volume of content. However, I learnt to identify and spot key pieces of information and add meaning to that information, this led to gathering knowledge and ultimately allowed for the completion of this report.

A project of this size requires strong management, as such my project management skills have been called upon and developed significantly. In particular, my communication skills. I have had to listen and understand a great deal of information (e.g. interviews, supervisor guidance) and then convey this in an appropriate way, both orally and in writing. I have also had to manage risks, including other work commitments during the project and the prospect of delayed deliverables (like questionnaire responses). I have also had to manage tasks and this developed as a result of an initial struggle. I struggled as I attempted to view the work as one single piece, opposed to breaking it down into sections which could then be tackled separately and subsequently pieced together. The problem with this was confusion, pressure and complexity that need not have been there. Through learning to tackle the project as small, manageable tasks it helped relieve these issues and essentially made it easier to recognise links.

All of the above skills have been utilised to fundamentally improve my ability to solve problems. I used all of the above skills to enable myself to organise and categorise work in terms of known and unknown pieces of information, from which, I applied an appropriate methodology to identify the unknown. This meant I produced a consolidated set of relevant material consistently, this proved vital in tackling the problems faced and completing the project.

Overall I am proud of the work completed and take pride in the skills that I have developed as a result of completing this project. The project has taken a great deal of effort and has been very difficult at times, although it has ultimately been very rewarding.

Conclusion

The purpose of this section is to recognise to what degree the aims established at the begging of the project have been met, whilst also highlighting any significant findings of this study.

Aim: *Identify what data can be collected, how the data is collected, how the user can access this data and how the data can be used on wearable devices e.g. Fitbit*

The study has seen this aim be completed in **full**. In depth background research into Fitbit and fitness trackers functionality allowed for one to identify everything that was outlined in this aim. In addition, one also looked at the laws and security surrounding the device as these were identified as applicable once research was underway.

Aim: *Model the dimensions of the problem to identify potential changes which can drive recommendations for improving user awareness on privacy and an analytical study of data*

The study has seen this aim be completed in **full**. The problem was initially analysed using background research to identify relevant stakeholders, as well as the areas which themselves are problematic within the different dimension of the problem. This analysis was then used to follow Soft Systems Methodology in order to model the problem and its problematic areas identified amongst several stakeholders. This essentially allowed for the data analysis to be undertook, this in turn drove recommendations.

Aim: *Investigate current attitudes and behaviour to privacy implications of users of wearable IoT devices*

The study has seen this aim be completed **partially**. Although one investigated the attitudes and behaviour surround privacy implications of wearable devices, one did not do this completely through primary research and instead utilised secondary research as well, I also collected comments from users in relation to privacy concerns from leading technology websites (as shown in Appendix C). The reasoning for this was therefore the time constraint of the project and the identification of up to date, relevant information already available. The merge of the questionnaire into separate sections also allowed for the extraction of behaviour and awareness.

Aim: *Identify current threats to users "Privacy" using wearable devices*

The study has seen this aim be completed in **full**. The fundamental idea of this aim was to identify threats in addition to those identified through data analysis. One identified from multiple studies and reports several privacy inferences, this allowed one to identify a more complete set of threats that can be considered to compromise user privacy. These were later presented to participants of the quantitative research.

Aim: *Identify any changes in behaviour or attitudes to privacy threats when providing previous participants with results of analytical study and research (potential privacy threats)*

The study has seen this aim be completed in full. Although one did not extract initial views through primary research, one was able to design the questionnaire in a way which tested the hypothesis of the study. The hypothesis of the study was proved correct: Users are generally unaware and concerned about the potential privacy implications, and this altered the willingness to participate in corporate wellness programs. Fundamentally, this drove recommendations for protecting privacy.

Aim: ***I**dentify a set of recommendations for protecting privacy when using wearable IoT devices like Fitbit*

The study has seen this aim be completed in full. One established a set of recommendations derived from background research and the qualitative research. The recommendations were also mapped against two manufacturers, this identified gaps in the current wearable market in relation to meeting proposed requirements.

This paper investigated the privacy implications of the provision and collection of health, activity and sleep data from employees by employers. The paper and hypothesis are supported by data analysis of real-world data set from a Fitbit. The results show that not only is it possible to derive personal information about users (the main inferences have been highlighted below), but that employers can potentially get access to this data without requiring an employee to 'opt in'. The main inferences identified by primary research were:

- Surveillance of employee's activity
  - Both during work hours and in leisure time
- Surveillance of employees sleeping habits
- Identification of physical disorders (anorexia, obesity)
- Identification of mental disorders (anxiety, depression)
  - Categorising the mental or physical state of employees
- Categorising the likelihood of productivity at work

In addition, the hypothesis of the study has been supported with the application of a survey and interviews. The survey and interviews identified that users are unaware of potential privacy implications. Their behaviour and need for control, awareness and visibility is impacted as a result. The study has then identified a set of recommendations which will significantly improve the situation and if followed, will provide sufficient and effective privacy. The recommendations explicitly highlight where current market leaders in corporate wellness are falling short.

Future Work

Although this project has identified privacy inferences implicit in user data and provided a set of accompanying recommendations for protecting the privacy of users, it can be further progressed in a number of ways:

- Demographics can play an important role in user's tendency to participate. Future work should identify suitable incentives which do not compromise users based on demographic factors.
- Identify what needs to be put in place to completely remove the possibility of re-identification from grouped aggregate data, including when partnered with public data.
    - Identify how many people need to be in a group to stop the re-identification of an individual
    - Identify what laws and complete security measures need to be followed (in addition to those outlined in the recommendation section)
- Explore privacy inferences implicit in user GPS and heart-rate data when also partnered with further information the employer may have on an employee.
- Identify any further privacy inferences obtained if data down to lower levels of granularity (e.g. minute by minute) is analysed.
- Produce a Privacy Policy which can be followed by manufacturers and employers which is compliant with all recommendations.
- Explore the development of a corporate wellbeing system which is compliant with all recommendations.
    - Identify a comprehensive set of requirements for a complete new system alongside acceptance criterion.
    - Conduct a questionnaire which analyses user's opinion, focused more on control and accessibility driven improvements.
    - Identify the system design, including:
        - System software & hardware architecture
        - Database design
        - Interface design including inputs and outputs
        - Detailed hardware and software design
        - Interface architecture and a detailed interface design

    - System integrity controls (e.g. who can have access to what?)
- Identify use case diagrams to represent how a user will interact with the system.
- Implement the system.
- Test the comprehensive functional and non-functional requirements against the acceptance criterion.
- Conduct user-testing of the system.
    - Utilise personas and nelsons heuristics.
- Evaluate the systems compliance against recommendations, whilst taking into consideration changing needs (maintaining recommendations to meet change, for example new laws).
    - Make changes where necessary if the system does not comply.

Appendices

Appendix A – Modern Day Encryption Dilemma

Encryption fundamentally seeks out to convert data or plain text into cipher text (which will appear to be random gibberish to anyone who intercepts), the cipher text has to then be decrypted with a password or key in order to return the original plain text. The benefit of this process is that data or plain text is only visible to those authorised to view it, hence it provides security and privacy. This poses a series of challenges for an organisation like the FBI, whom rely heavily on intercepted messages or data held on devices to help with the capturing of criminals or terrorists. Most recently the FBI were seeking the assistance of the incredibly popular Apple, the FBI required access to one of the San Bernardino shooters iPhone. The assistance the FBI aimed to acquire was essentially a backdoor built into a custom version of the iOS software (the backdoor being allowing the OS to attack iPhone encryption, allowing a passcode to be input electronically which would allow for a "brute force" attack). iPhones are incredibly personal devices with incredible amounts of personal information from photos, health data, passwords, addresses, photos to emails and messages (similar to some data found on wearable devices), which law abiding citizens deserve the right to be protected. Apple was not prepared to co-operate and engaged in a legal battle with the FBI, in a public statement Apple gave its reasoning. Firstly, Apple argued that in developing such a backdoor they expose the personal information identified above and more, placing public privacy and safety at risk. Secondly Apple argued that if they were to obey, they would set a legal precedent in which they could be forced to expand their co-operation with the FBI (they could in future be forced to provide location tracking or recording conversations) (Apple, 2016). The FBI eventually found assistance from a different organisation whom used a flaw in Apple's security to bypass the device (BURGESS, 2016). The importance of this battle can be seen when noting that several large organisations, including Google, stood behind Apple in their fight for user privacy and safety. Similarly, the actions of WhatsApp in the wake of the battle show that the encryption is here to stay. WhatsApp has moved to offer full end-to-end encryption of all messages sent through the service, something Apple's iMessage service already possessed. WhatsApp touched on the above case in their press statement, stating that whilst they identify the difficulties law enforcements face, weakening encryption only entices cybercriminals, hackers and rouge states and fundamentally affects the law abiding citizen. WhatsApp also touched on an incredibly important and applicable point, as stated by cofounders Jan & Brian (2016):

> *We live in a world where more of our data is digitized than ever before. Every day we see stories about sensitive records being improperly accessed or stolen. And if nothing is done, more of people's digital information and communication will be vulnerable to attack in the years to come. Fortunately, end-to-end encryption protects us from these vulnerabilities.*

The importance and relevance of this in the fitness tracking and wearable market is that personable information is being collected by the devices, it is of paramount importance to protect this data from vulnerabilities and subsequent exposure to motivated parties. It is not unrealistic to say that a Fitness tracker (with notification, location, and messaging abilities) could be the centre of a similar legal battle. Whilst Apple have been identified as using credible security on their Apple Watch in a study outlined in this report, the backdoor exploited by the FBI without their assistance proves no company is perfect in their security, not even those without financial constraints. Essentially, the incredible advancement's in not only technology, but companies view and stance on encryption for its users, means that consumers must rely on the company in order to be protected. Market competitiveness, start-ups with lack of exposure and knowledge, ignorance or even law enforcements cannot get in the way of the modern day view on encryption; the law abiding citizen deserves the right to privacy and security. The devices need to represent this view in their technical abilities and the limitations of devices needs to be presented to users and addressed where possible. This will allow for transparency and on-going trust between manufacturers of wearable devices and those who rely on them to protect their incredibly personal data.

Appendix B - Modern Day Data Breach Dilemma

The storing of user data on servers or in 'the cloud' means that it's nigh on impossible for organisations to completely protect user's data. In addition, the availability of more personal information (with the advancements in smartphones, wearable device etc.) means that hackers have a new direction and types of data to use for extortion or harm. In the 2016 Data Breach Industry Forecast by (Experian, 2016) identifies that health care data is worth up to 10 times more than credit care information on the black market, showing the significant shift in direction. It would appear that security attacks are more advanced than the security measures set out to protect data. This is identifiable in some alarming statistics from the forecast report, 91% of all healthcare organisations have reported at least one data breach in the last two years. In addition, this is forecasted to show no signs of slowing down with a key takeaway from the forecast being attacks on medical insurers and large hospital networks, mainly due to the increase in saleability and profitability from derived data, not due to ease of attack. There was a total of 110 data breaches recorded from the start of 2016 to March 1st and from those nearly 1.8 million records have been exposed (IDTRC, 2016). In one particular breach (the largest ever) recorded 950,000 subscribers to Centre Corps medical information being unaccounted for (Ausick, 2016). Whilst fitness trackers do not include health data to such a degree as medical records from insurance and hospitals, they still contain enough information to ignite the fuel for hackers to attempt to extort users. The identification of pregnancies, whereabouts, mood and even eating disorders are all valid pieces of knowledge which could be used as a threat towards users, and it's clear that no data is safe from attacks, especially medical data. The shift from stealing identities and credit card fraud to the focus on medical data poses a real risk for fitness trackers and the data security, the fire has been lit and there is serious motivation for unauthorised retrieval of user data from servers.

Appendix C – Opinions and Concerns in relation to Wearable Fitness Trackers

In order to understand further consumers concerns, in relation to fitness trackers, one explored comments on wearable posts which were posted on news and technology websites. The comment is analysed and then the report seeks to identify if the opinion expressed in the comment is justifiable.

Table 29 - Comments in relation to Wearable Privacy Concerns

Comment	**Analysis**
Why worry? You want to know my heart beat? How active I am and how well I sleep? I'll tell you, just ask. BUT - I keep the GPS turned off when not in use for walks, etc... I am not worried about my Fitbit being hacked. The data is only valuable to me. [19]	This comment shows the opinion that it appears many consumers have, that their data is only valuable to them (excluding location data), and that even in the wrong hands it poses no real threat. This provides motivation to analyse data, this will allow one to identify the threat it possesses.
Yeah, I'm really worried that someone could steal the fact that I walk at least 10,000 steps a day! What a load of scaremongering nonsense! [20]	This comment shows a similar opinion to the comment above, the opinion that the data is useless regardless if anyone has access. This could be naive and there is again motivation to do data analysis to understand if this opinion is warranted, or indeed naïve.
You may not sell the raw data, but you sell the aggregate results of information that was unknowingly provided to you by consumers.[21]	This concerns is touching on the notion that although individually identifiable information isn't sold, aggregate data is and is done so unknowingly to those providing.

[19] http://www.dailymail.co.uk/sciencetech/article-3429067/Is-fitness-tracker-putting-privacy-risk-Claims-selling-wearables-leaking-data-turned-off.html - Accessed 4th May 2016

[20] http://www.dailymail.co.uk/sciencetech/article-3429067/Is-fitness-tracker-putting-privacy-risk-Claims-selling-wearables-leaking-data-turned-off.html - Accessed 4th May 2016

[21] http://www.businessinsider.com/senator-warns-fitbit-is-a-privacy-nightmare-2014-8?IR=T - Accessed 4th May 2016

	Provides motivation to see if users really are unaware.
Given that wearable tech is going beyond merely health and fitness apps, it's imperative that the security for all these smart devices are kept in tune with the amount of personal data they would be interfacing with.[22]	This comment touches on a very important point and one which has been addressed in this report. The point is that as wearable tech gathers much more personal data through advancements, the security needs to advance as well to protect users' data. This provides motivation to see if this is currently the case.

[22] http://www.computerworld.com/article/2855567/data-from-wearable-devices-could-soon-land-you-in-jail.html Accessed 4th May 2016

Appendix D – Extent of Information Available from Fitbit Personal Profile (Experiment)

Figure 23 - Calorie Profile Information

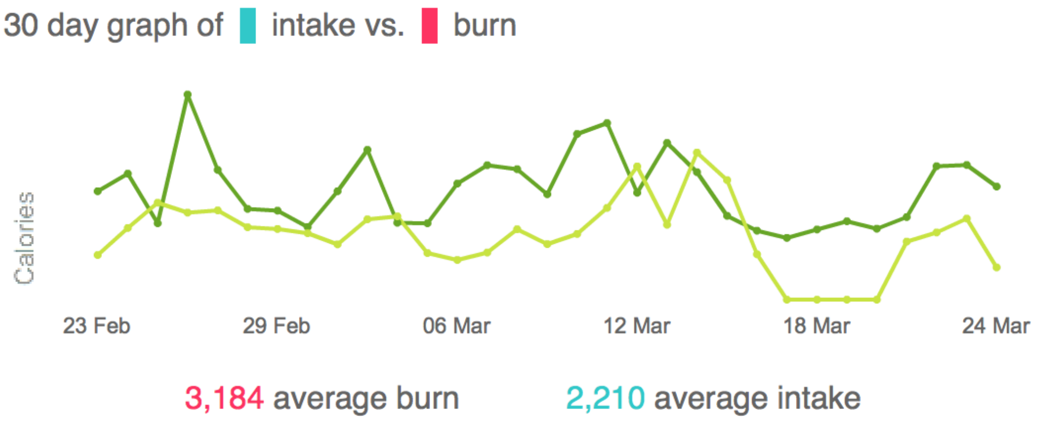


Figure 24 - Activity Profile Information

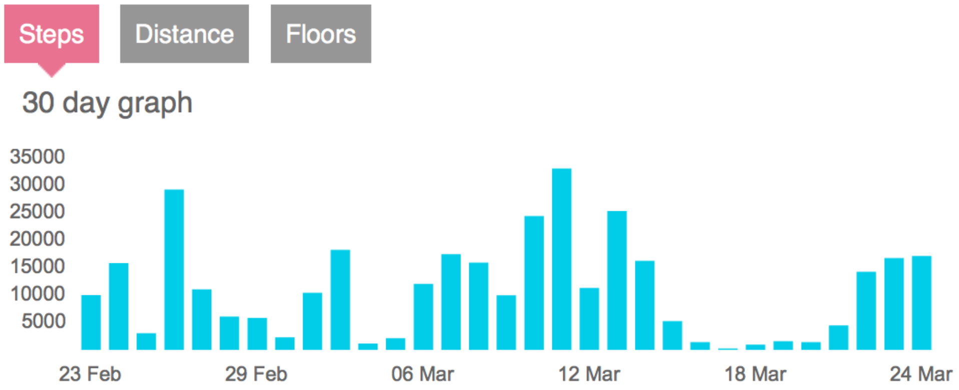


Figure 25- Further Activity Profile Information

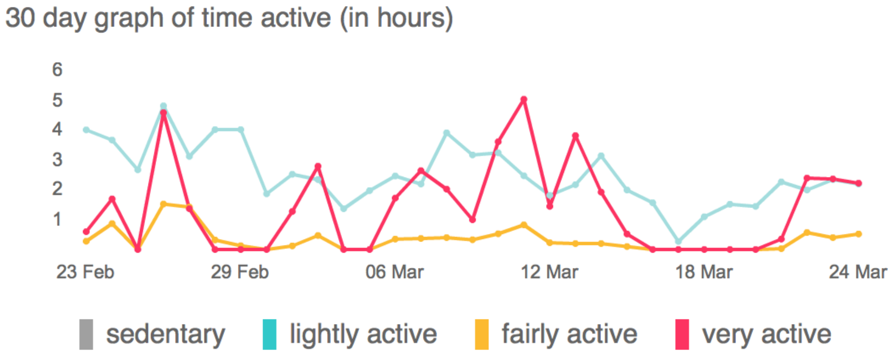
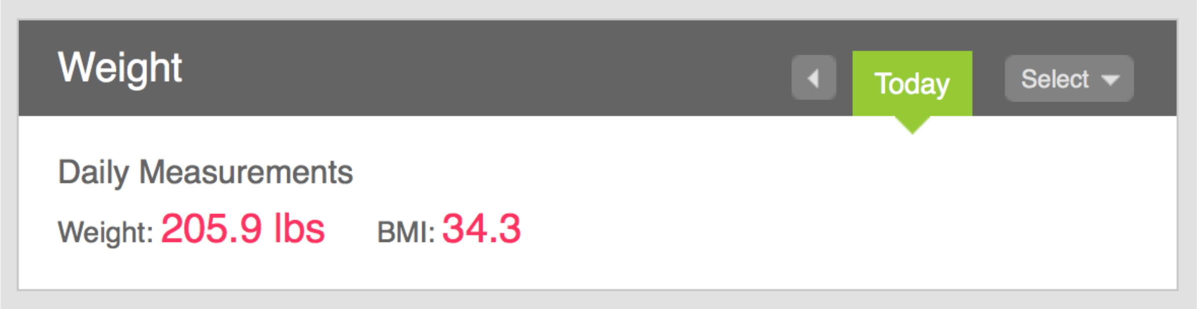


Figure 26 - Weight and BMI Profile Information



Weight

Daily Measurements

Weight: 205.9 lbs   BMI: 34.3

Figure 27 - Weight Profile Information (Further)

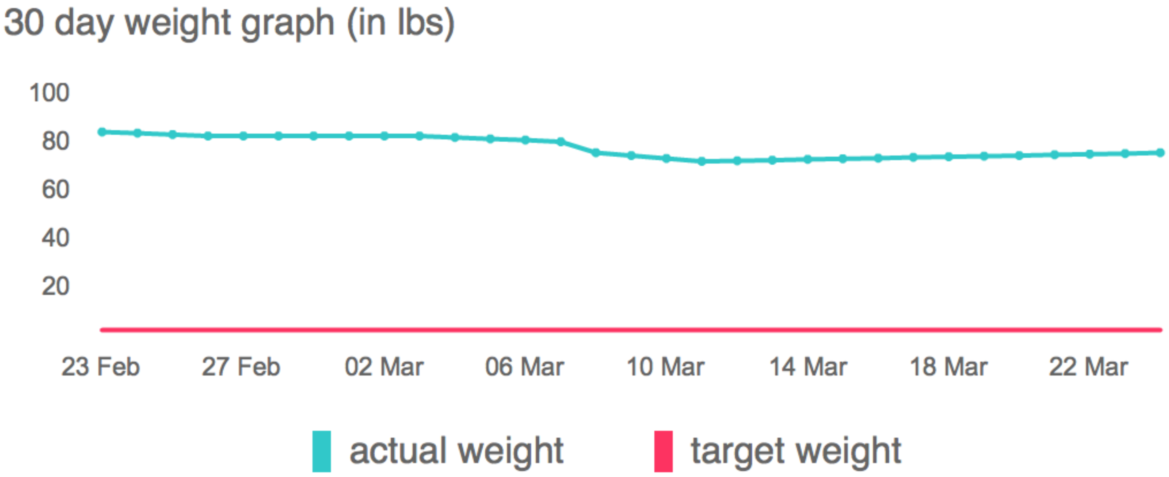
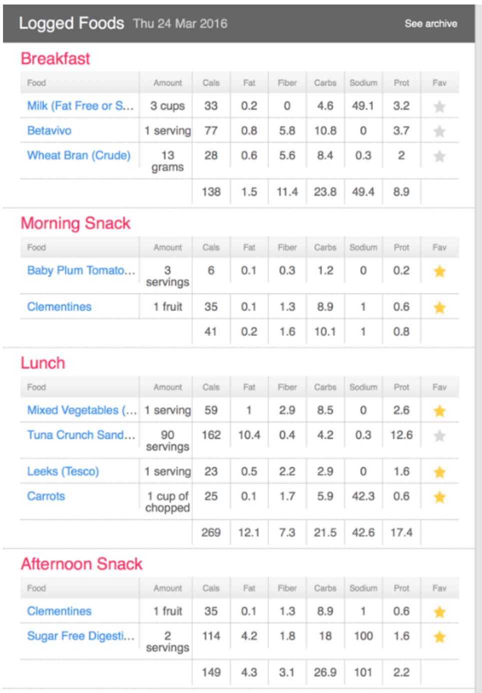


Figure 28 - Food Log Profile Information



Logged Foods Thu 24 Mar 2016 See archive

Breakfast

Food	Amount	Cals	Fat	Fiber	Carbs	Sodium	Prot	Fav
Milk (Fat Free or S...	3 cups	33	0.2	0	4.6	49.1	3.2	☆
Betavivo	1 serving	77	0.8	5.8	10.8	0	3.7	☆
Wheat Bran (Crude)	13 grams	28	0.6	5.6	8.4	0.3	2	☆
		138	1.5	11.4	23.8	49.4	8.9	

Morning Snack

Food	Amount	Cals	Fat	Fiber	Carbs	Sodium	Prot	Fav
Baby Plum Tomato...	3 servings	6	0.1	0.3	1.2	0	0.2	★
Clementines	1 fruit	35	0.1	1.3	8.9	1	0.6	★
		41	0.2	1.6	10.1	1	0.8	

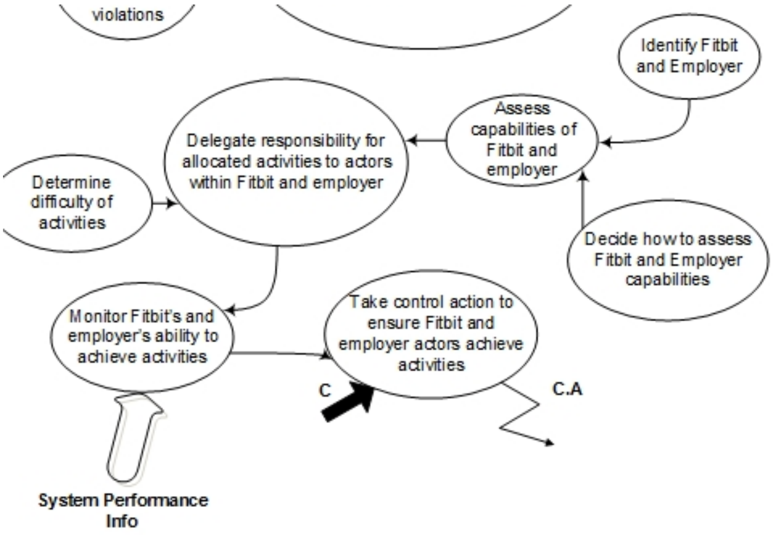
Lunch

Food	Amount	Cals	Fat	Fiber	Carbs	Sodium	Prot	Fav
Mixed Vegetables (...	1 serving	59	1	2.9	8.5	0	2.6	★
Tuna Crunch Sand...	90 servings	162	10.4	0.4	4.2	0.3	12.6	☆
Leeks (Tesco)	1 serving	23	0.5	2.2	2.9	0	1.6	★
Carrots	1 cup of chopped	25	0.1	1.7	5.9	42.3	0.6	★
		269	12.1	7.3	21.5	42.6	17.4	

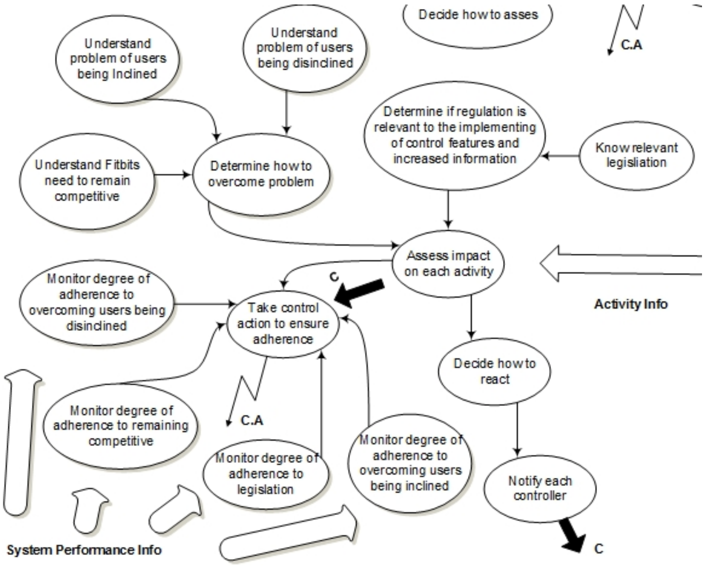
Afternoon Snack

Food	Amount	Cals	Fat	Fiber	Carbs	Sodium	Prot	Fav
Clementines	1 fruit	35	0.1	1.3	8.9	1	0.6	★
Sugar Free Digesti...	2 servings	114	4.2	1.8	18	100	1.6	★
		149	4.3	3.1	26.9	101	2.2	

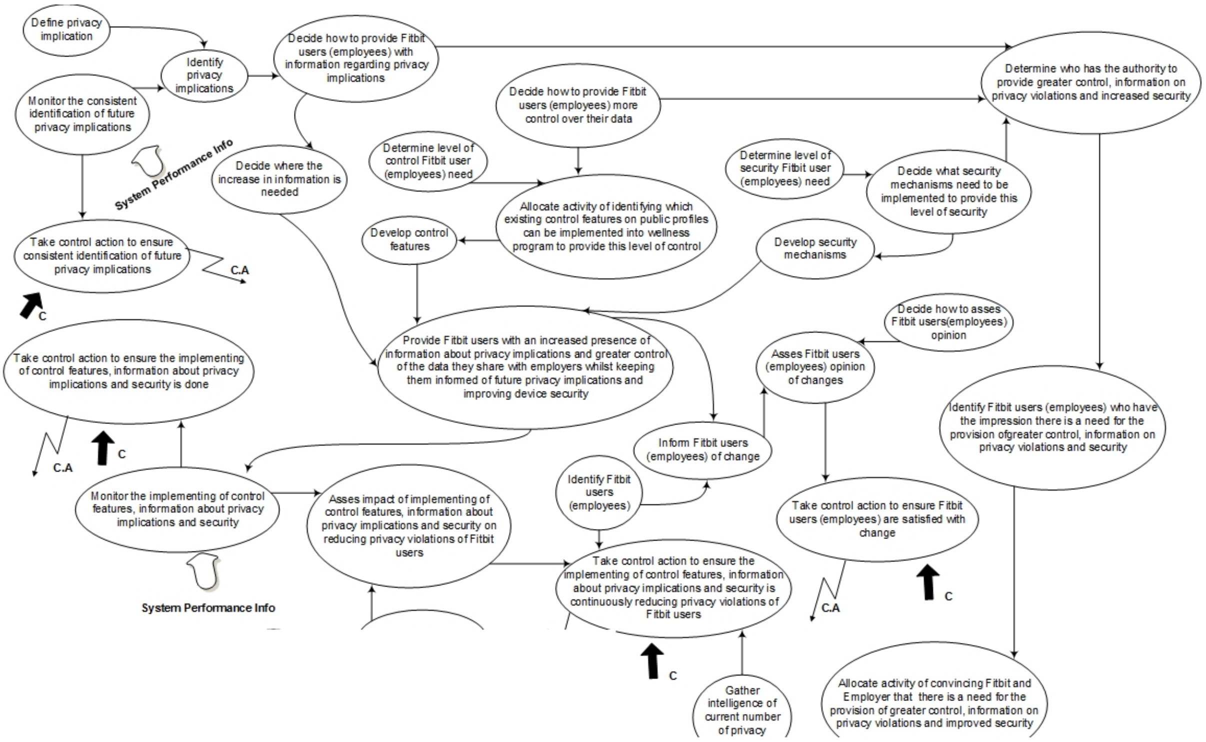
Appendix E – SSM Conceptual Model Analysis


violations
Identify Fitbit and Employer
Assess capabilities of Fitbit and employer
Delegate responsibility for allocated activities to actors within Fitbit and employer
Determine difficulty of activities
Decide how to assess Fitbit and Employer capabilities
Monitor Fitbit's and employer's ability to achieve activities
Take control action to ensure Fitbit and employer actors achieve activities
C
C.A
System Performance Info

This section of the Conceptual Model is focused on ensuing the correct delegation and completion of derived actions. Firstly, those who are going to be assigned activities (in this case this will be Fitbit and the Employer) need to be identified. Once identified, these individuals then need to be assessed in regards to their capability. The reason for this is because all activities identified will also be assessed in regards to their difficulty. Through assessing both, one can then ensure the correct delegation of work, such that those who are delegated work are capable of completing the work. Their needs to be consistent monitoring to determine regularly if those assigned are still capable and completing activities, this ensures consistent performance of the system as it is supposed to function.


Decide how to asses
C.A
Understand problem of users being Inclined
Understand problem of users being disinclined
Determine if regulation is relevant to the implementing of control features and increased information
Know relevant legislation
Understand Fitbits need to remain competitive
Determine how to overcome problem
Assess impact on each activity
Activity Info
Monitor degree of adherence to overcoming users being disinclined
C
Take control action to ensure adherence
Decide how to react
Monitor degree of adherence to remaining competitive
C.A
Monitor degree of adherence to legislation
Monitor degree of adherence to overcoming users being inclined
Notify each controller
C
System Performance Info

This section of the Conceptual Model is focused on addressing the environmental constraints and the potential impact they could have on the system. Essentially, the four key activities are understanding the four environmental constraints identified previously. Once understood (or in the case of legislation, knowledge is required of the actual legislation and if it's applicable), the problem then has to be overcome, a suitable method therefore needs to be determined. However, once a solution has been determined (or if the legalisation is deemed applicable) it is then vital to identify the impact this could have on the other activities (e.g. new legalisation could mean the changing of what security must be included). The impact and subsequent applicable reaction, must then be communicated to the relevant assigned actors so they can take action. This ensures that the system will function as intended as much as possible, even if activities are impacted by environmental constraints.


Define privacy implication
Identify privacy implications
Decide how to provide Fitbit users (employees) with information regarding privacy implications
Monitor the consistent identification of future privacy implications
System Performance Info
Decide where the increase in information is needed
Decide how to provide Fitbit users (employees) more control over their data
Determine level of control Fitbit user (employees) need
Allocate activity of identifying which existing control features on public profiles can be implemented into wellness program to provide this level of control
Develop control features
Determine who has the authority to provide greater control, information on privacy violations and increased security
Determine level of security Fitbit user (employees) need
Decide what security mechanisms need to be implemented to provide this level of security
Develop security mechanisms
Take control action to ensure consistent identification of future privacy implications
C.A
C
Take control action to ensure the implementing of control features, information about privacy implications and security is done
Provide Fitbit users with an increased presence of information about privacy implications and greater control of the data they share with employers whilst keeping them informed of future privacy implications and improving device security
Decide how to asses Fitbit users(employees) opinion
Asses Fitbit users (employees) opinion of changes
Identify Fitbit users (employees) who have the impression there is a need for the provision ofgreater control, information on privacy violations and security
C.A
C
Inform Fitbit users (employees) of change
Identify Fitbit users (employees)
Monitor the implementing of control features, information about privacy implications and security
Asses impact of implementing of control features, information about privacy implications and security on reducing privacy violations of Fitbit users
Take control action to ensure Fitbit users (employees) are satisfied with change
System Performance Info
Take control action to ensure the implementing of control features, information about privacy implications and security is continuously reducing privacy violations of Fitbit users
C.A
C
C
Gather intelligence of current number of privacy
Allocate activity of convincing Fitbit and Employer that there is a need for the provision of greater control, information on privacy violations and improved security

This section of the Conceptual Model is focused around addressing the transformation, in this instance, this is the reduction of privacy violations against those wearing a fitness tracker for an incentive. The transformation is supported by the worldview. The worldview is the belief that by increasing device security, privacy information and control features provided to users, you will reduce the number of privacy violations. Privacy implications therefore have to be defined and monitored, this ensures that new and existing implications are identified and users can educate themselves (once it has been identified where the increase in information is needed). In regards to control, it first has to be determined the level of control they need, such that they are sufficiently protected. From this, it will then be possible to adapt what is provided on personal profiles (which has previously been identified as much more comprehensive than what is provided within the wellness programs) to provide users with the control they require. Finally, the level of security which users require to safeguard their data needs to be determined, this can then be implemented. We can then return to the transformation, the implementation of the above three improvements has to be monitored in several instances. Firstly, it has to be monitored to ensure that it is in fact being implemented after it has been determined what is required. Secondly, it then needs to be monitored to determine if the implementation of the three improvements has actually reduced privacy violations (this is why current level of violations needs to be determined, to compare present with the future) and achieved the transformation. Finally, users' reaction to the implementations has to be monitored, one cannot reduce privacy violations but then upset users. This could then see a decrease in participations in the program, hence the important of monitoring their opinion. There is also the need to identify those who feel change is needed, these people can then be responsible for championing change within their employment, who can then address Fitbit. For this, those with the authority to actually address this situation need to be identified and they must then be allocated the activity of championing the change with Fitbit and their Employer.

Appendix F – Questionnaire Pilot and Question Validations

Question Validation

The questionnaire can be viewed in a separate submission.

- ***Demographic information***

Questions one (age), two (gender) and three (occupational status) are all basic demographic information which is vital in understanding how privacy affects awareness and behaviour across user profiles. The analysis and comparison could prove extremely important in driving recommendations for protecting consumer privacy, recommendations regarding wellness programs could be tailored to specific categories of people based on this question analysed against further questions.

- ***Wearable Awareness***

Question four (familiarity with wearable technology) is aimed to separate those who know about wearable technology from those who do not in order to again analyse awareness and behaviour across a differing profile. This is in addition to question five (usage of fitness tracker), which aims to understand the awareness and behaviour amongst those who do and also do not currently use fitness trackers, with the assumption that those who do are more likely to be aware. Furthermore, question six (factors influencing decision making) is aimed to identify if participants place privacy as a priority when choosing a device and was inspired by LICBS & Zeno (2014). Finally question seven (awareness of types of data collected) aims to understand the percentage of users or potential users that are aware of which types of data can be collected by a wearable fitness tracker.

- ***Sharing Preferences***

Questions eight through to twelve are all aimed at identifying the sharing preferences of participants, in relation to collectable pieces of information from a fitness tracker. It is important to identify with whom participant would be willing to share each with as each correspond to differing potential inferences.

Question thirteen aims to identify the percentage of people who would be willing to share all of the information with a consumer for an incentive prior to informing them of the possible inferences. This is then asked again in question 15 post informing them to see if there is a change in behaviour from which one can identify the level of awareness of privacy inferences in addition to how this impacts behaviour in relation to sharing and need for control and awareness.

- ***Privacy facts***

Question fourteen aims to identify participant's opinion in relation to 11 statements about possible applications of data generated by a fitness tracker. These facts are all possible and are derived from thorough background research and data analysis carried out on real-world datasets from a wearable fitness tracker. The statements are a mix of seemingly positive and negative facts to minimise the effect of bias. The analysis of respondent's answers ought to be thought-provoking in seeing if it affects their sharing preference.

- ***Better Control and Awareness***

Question fifteen aims to identify participant's opinion in relation to seven control and awareness raising features, respondents will be asked to state if they feel each is required or not. All eight are not complex in nature and will help drive the recommendation section. They all attempt to provide consumers with more awareness (e.g. informing users of what types of data can be collected) or more control (e.g. have the right to be forgotten). Through understanding those which respondents feel are most fundamental it will allow oneself to better understand how to draw up the recommendations for protecting consumer privacy.

Pilot

The final stage in the planning was to carry out a pilot questionnaire, this can be viewed below.

IBM SPSS

The decision by oneself to use IBM SPSS to analyse the data despite no prior knowledge of the program, was because of the easy statistical analysis the program provided. Although SPSS required data to be coded (as opposed to Excel which does not), once the data was inserted it allowed for superior manipulation of questions in order to analyse against user profiles and thus was chosen to use. In addition, SPSS is a true statistical package which provides easy and fast access to numerous statistical tools which can be utilised in analysis. The SPSS coding can be viewed as a separate '.sav' submission,

Questionnaire Pilot

My initial plan outlined my desire to carry out a pilot of the questionnaire, the reasoning behind this is that it will enable me to get a differing opinion from a small sample size of people and potentially benefit the survey, prior to being distributed. The potential benefits anticipated are:

- Identify if the time taken to complete is reasonable
- Identify any questions which contain ambiguity or are too complex by nature
- Identify if the potential responses given to questions are suitable and adequate
- Identify any mistakes e.g. spelling, consistency throughout the questionnaire
- Identify any questions respondents feel aren't required

The procedure I followed in order to improve the internal validly of a questionnaire was provided by Peat, et al., (2002).

- Administer the questionnaire to pilot subjects in exactly the same way as it will be administered in the main study
- Ask the subjects for feedback to identify ambiguities and difficult questions
- Record the time taken to complete the questionnaire and decide whether it is reasonable
- Discard all unnecessary, difficult or ambiguous questions
- Assess whether each question gives an adequate range of responses
- Establish that replies can be interpreted in terms of the information that is required
- Check that all questions are answered
- Re-word or re-scale any questions that are not answered as expected
- Shorten, revise and, if possible, pilot again.

Pilot one – James

James took 4 minutes and 34 seconds to complete the survey, below the stated 5-10 and one is content that this is long enough to extract required information, but short enough to retain participation and focus.

James observations and my subsequent actions were as follows:

1. James commented on the question: "If not, why do you not use a wearable fitness tracker?" the following "why there is no option for cost?"
   a. I informed him that the following question was targeted at factors taken into account when buying a wearable fitness tracker, his response was that this seemed like a duplicate of questions and as a result I removed this question from the questionnaire as I agreed with his perspective

2. James commented on the question: “If you were to purchase a wearable device, which factors would you consider before making a purchase” the following “why can I only select three”
    a. My response was that the intention of the question is to identify your top three factors of consideration when purchasing a device hence the limit
3. James commented on the question: “your employer can potentially identify if you are likely to be suffering from depression” the following “isn’t this the same as obesity and anorexia being discovered?”
    a. My response was that one was physical illnesses and the other was mental and that they differ in nature, he agreed.
4. James commented that the potential privacy implication scenario’s outlined in section two were too wordy and could do with being simplified as it was taking too long to read, he specifically said “I don’t need reminding what activity data is or what sleep quality is, simplify it”
    a. James comments were taking on board and I amended the questions to remove complexity and repeat information
5. James commented on the potential improvements section that there could also be a “desirable” option as “required” and “not-required” didn’t provide him with adequate opportunity to reflect his thoughts
    a. I agreed with James comments and added the extra option

Pilot two – Matthew

Matthew took 3 minutes 56 seconds to complete the survey, this could be related to the improvements made after the initial pilot.

Matthew’s observations and my subsequent actions were as follows:

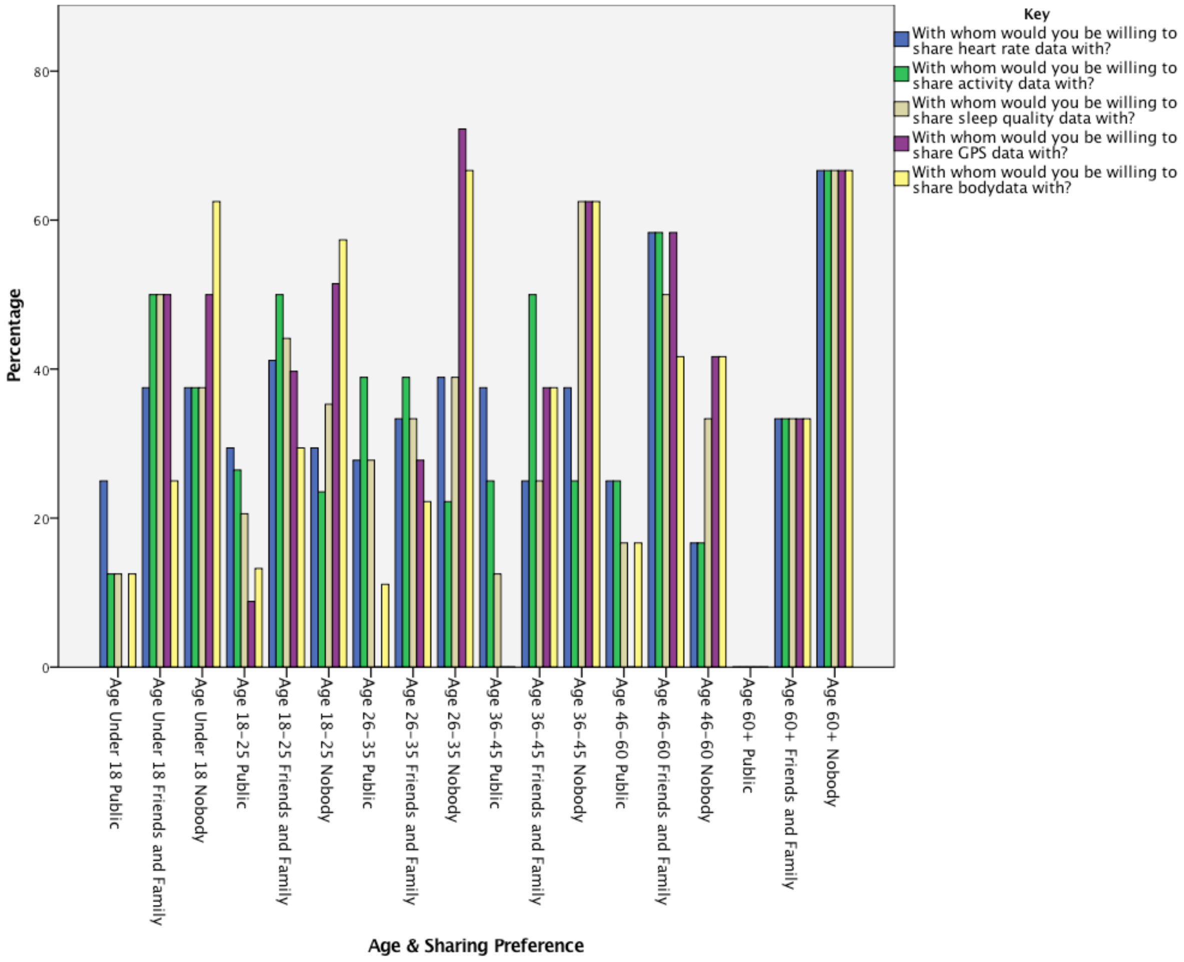
1. Matthew commented on the scenario: “employers use the data collected to get the best insurance premiums” the following “this is ambiguous, who is benefiting? Me or the company, who is getting better premiums?”
    a. I agreed with Matthews comments and amended to show that it was in fact the employer benefiting
2. Matthew commented on consistency he stated “the inclusion of the term smart sensors just threw me off and was not mentioned in the prior section”
    a. I amended the questionnaire to remove this term and ensured it was consistent throughout stating “data collected from a wearable fitness tracker”

3. Matthew commented on the potential improvement opportunity “employers should only receive data in an aggregated form which de-identifies individuals” the following “this could be misleading and can be simplified, I had to read this twice, aggregated and de-identified are too complex”
    a. I amended the questionnaire to state the following instead “your employer should only receive employee’s data in a grouped form so individuals can’t be identified”
4. Matthew commented on the potential improvement opportunity “employers should create and uphold privacy policies” the following “what do you mean by uphold?”
    a. I informed him that this meant the policies should be adhered to by the employer but agreed it was ambiguous and amended to “privacy policies should be put in place to protect employees and their data”
5. Matthew commented on the potential improvement opportunity “employers should only use fitness trackers with the appropriate security measures which prevent the falsifying of data and tracking of location” the following “this took far too long to read, could simply just be “employers should only use fitness trackers with appropriate security measures which protect employee’s data”
    a. Agreed and amended.

Appendix G – Supporting Graphs

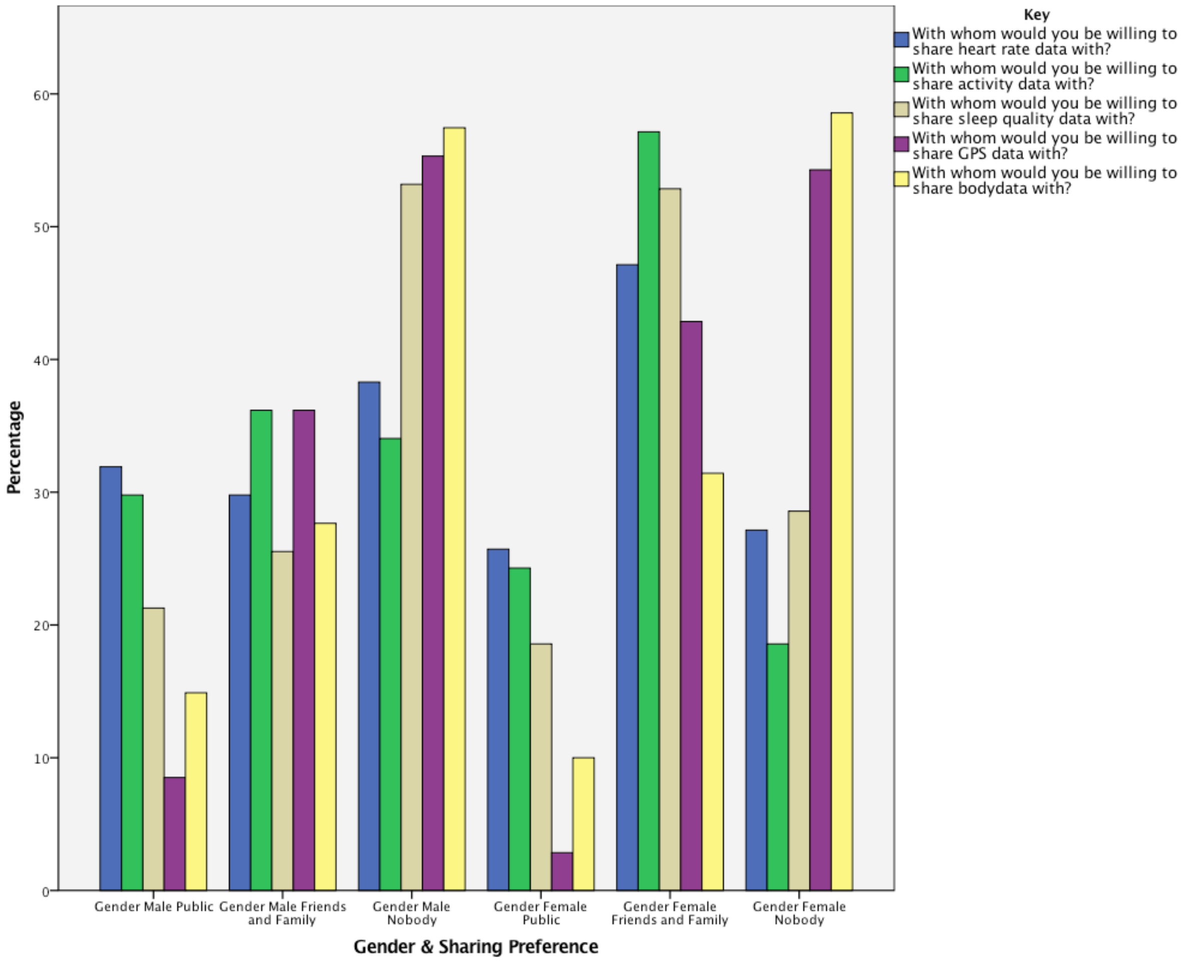
These graphs are to support the questionnaire analysis. The analysis saw differing user profiles be compared against specific questions to identify correlations, the derived correlations are from the below graphs.

Figure 29 – Participants Sharing Behaviour, Compared Against Age



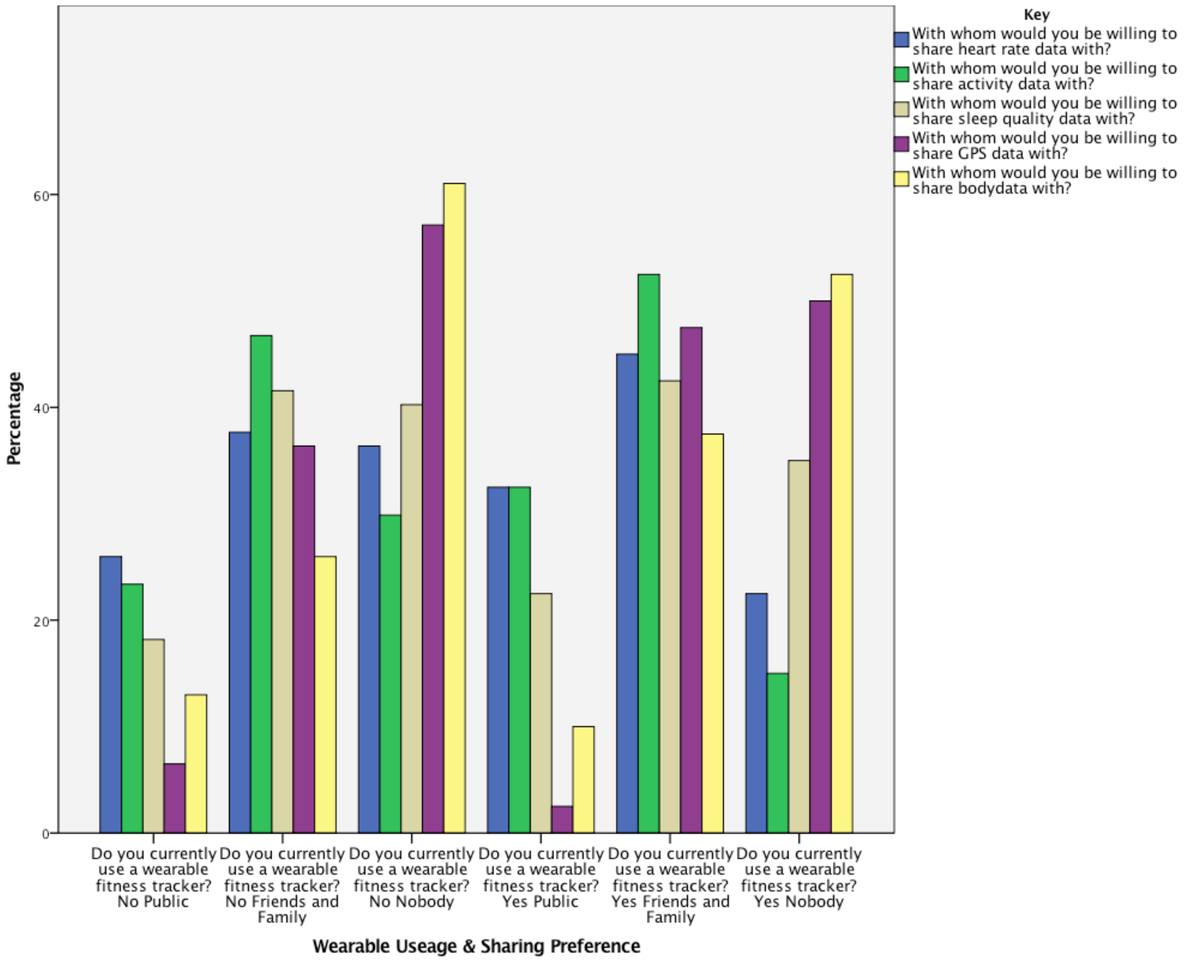
This graph shows with whom participants would be willing to share various types of data with and is compared against age.

Figure 30 - Participants Sharing Behaviour, Compared Against Gender



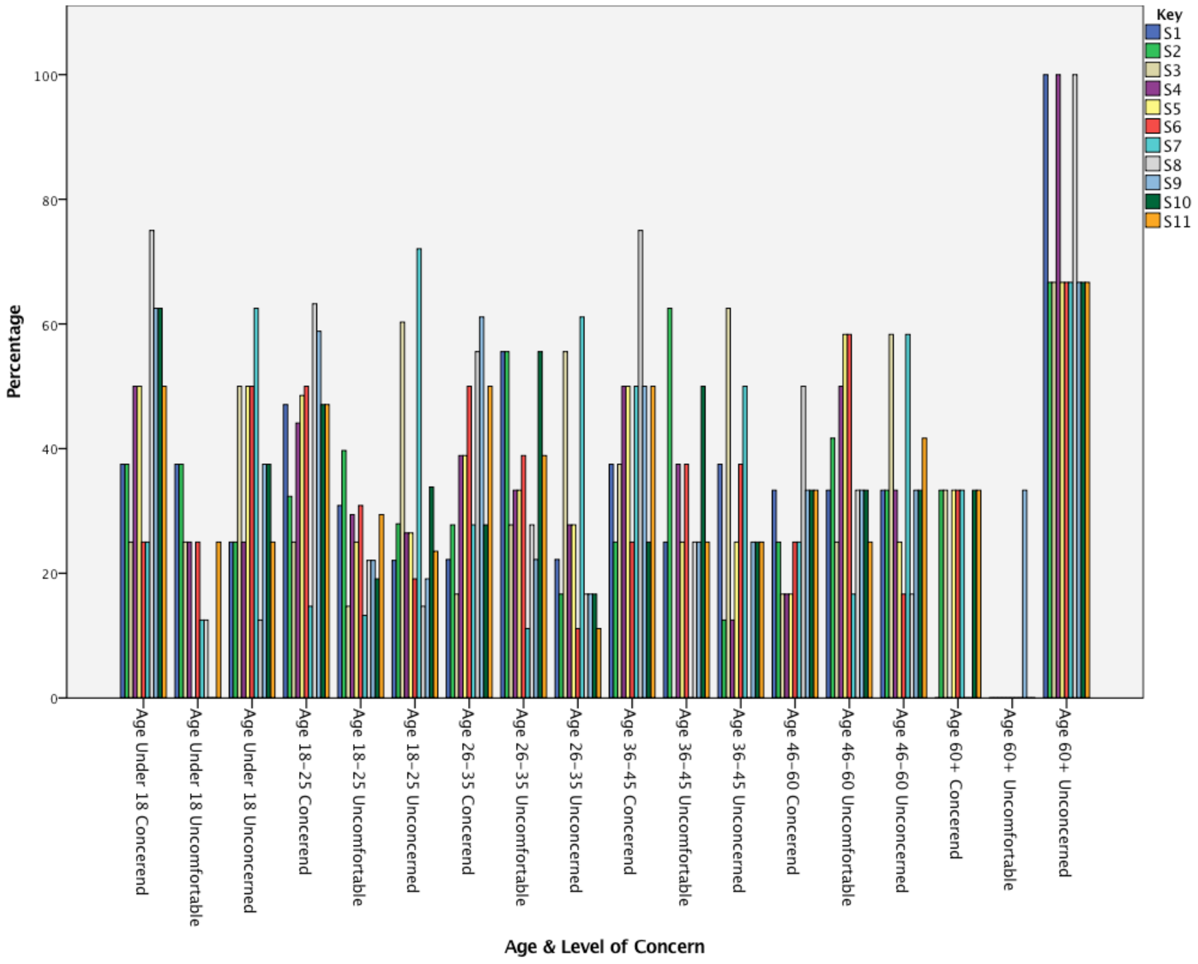
This graph shows with whom participants would be willing to share various types of data with and is compared against gender.

Figure 31- Participants Sharing Behaviour, Compared Against Wearable Usage



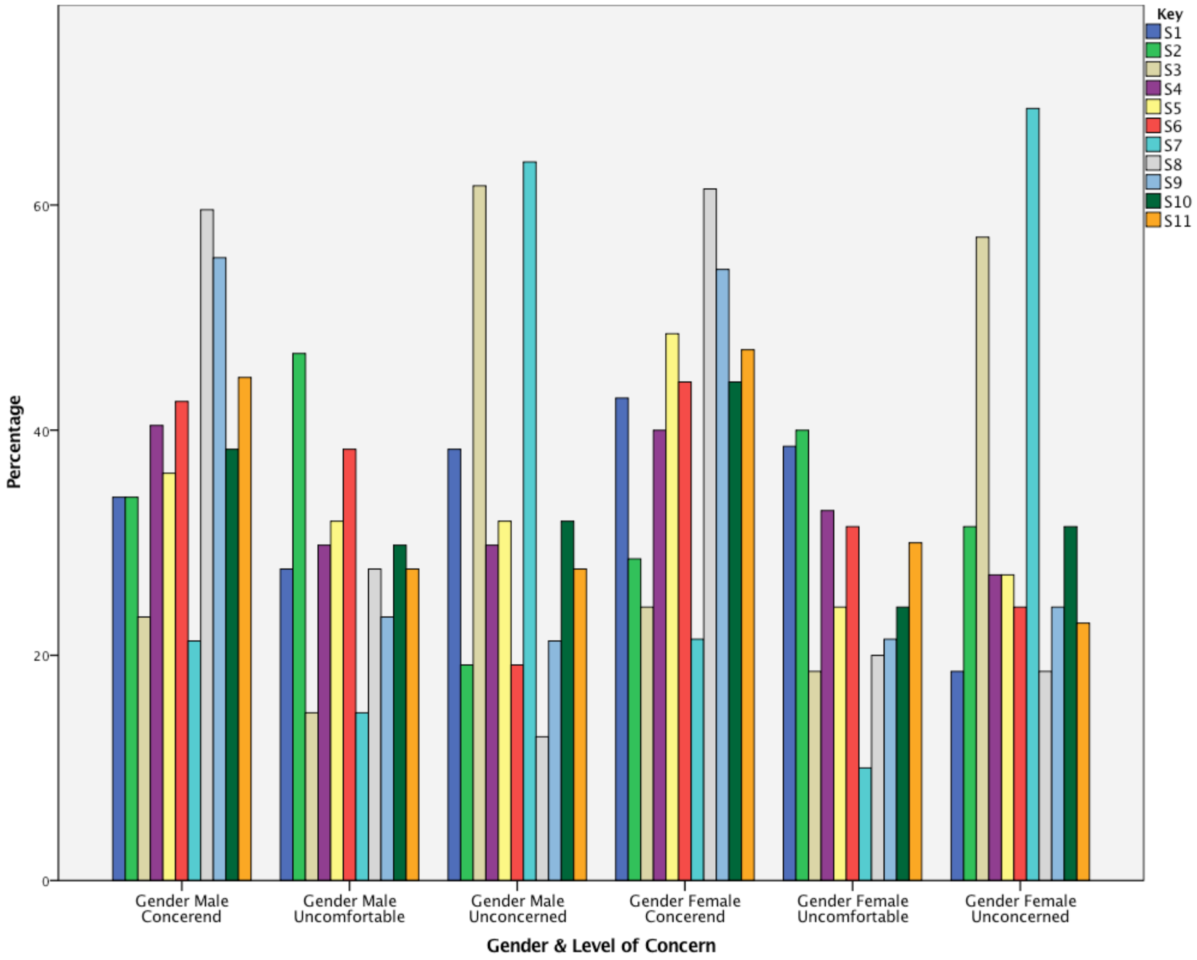
This graph shows with whom participants would be willing to share various types of data with and is compared against wearable usage.

Figure 32 - Participants Level of Concern, Compared Against Age



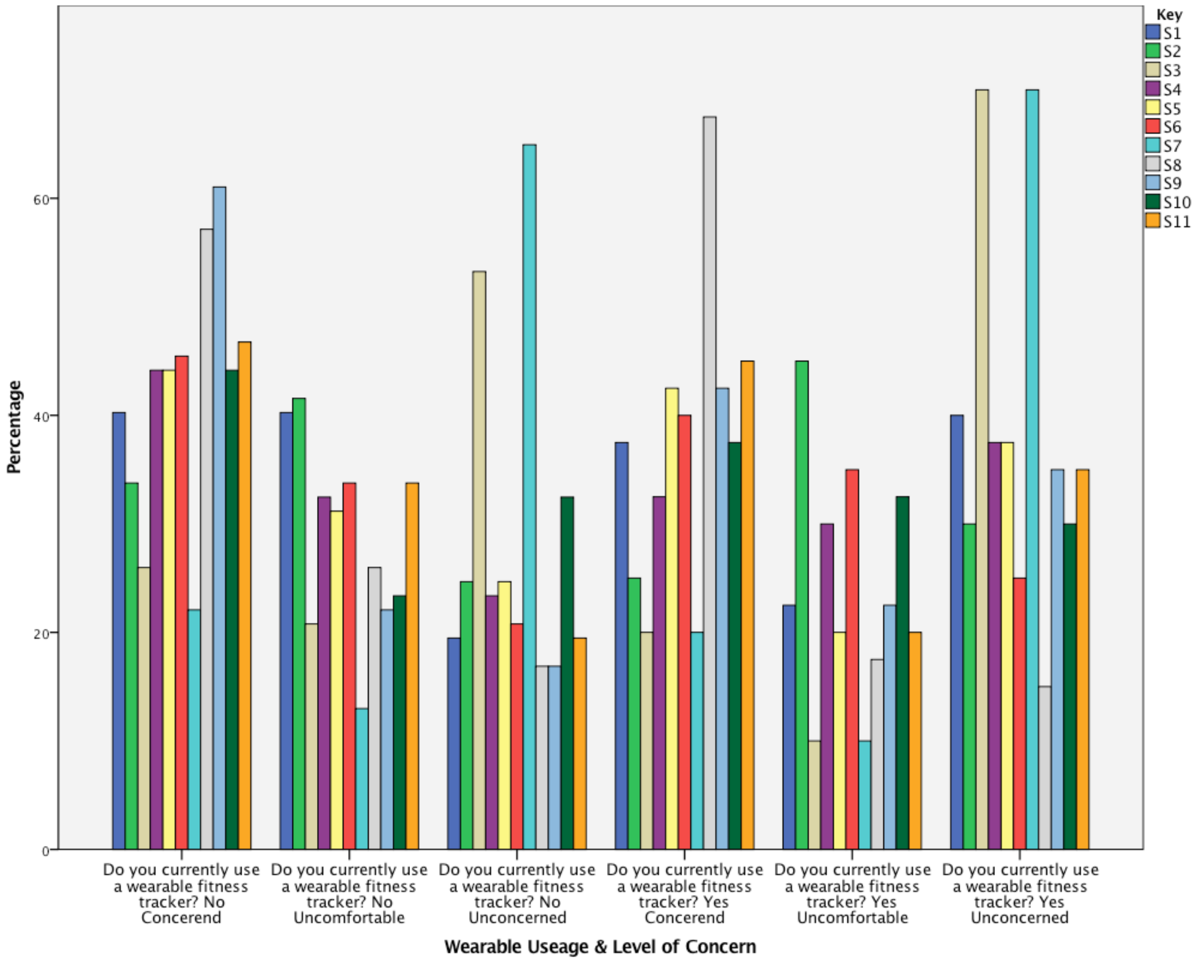
This graph shows participants level of concern in relation to 11 statements and is compared against age.

Figure 33 - Participants Level of Concern, Compared Against Gender



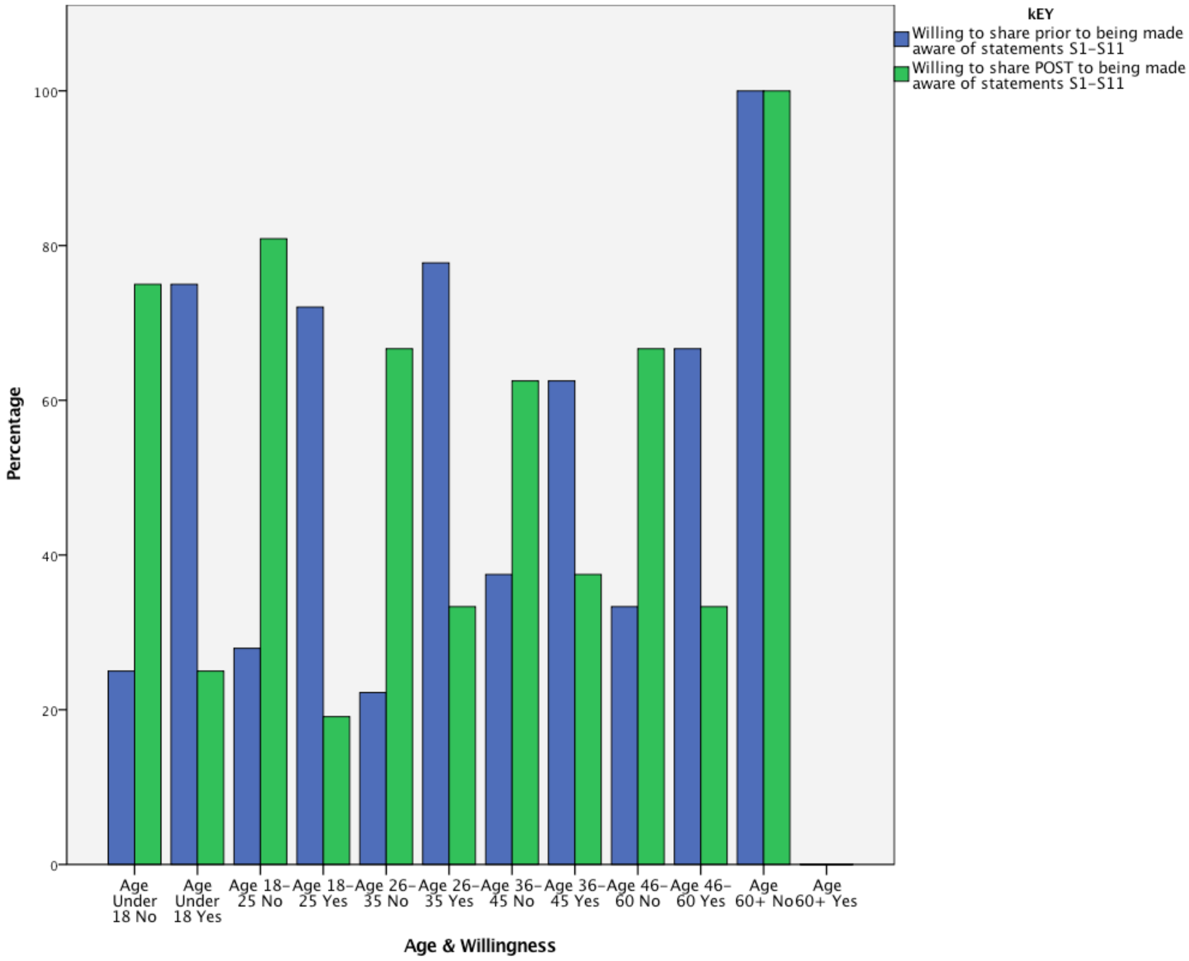
This graph shows participants level of concern in relation to 11 statements and is compared against gender.

Figure 34 - Participants Level of Concern, Compared Against Wearable Usage



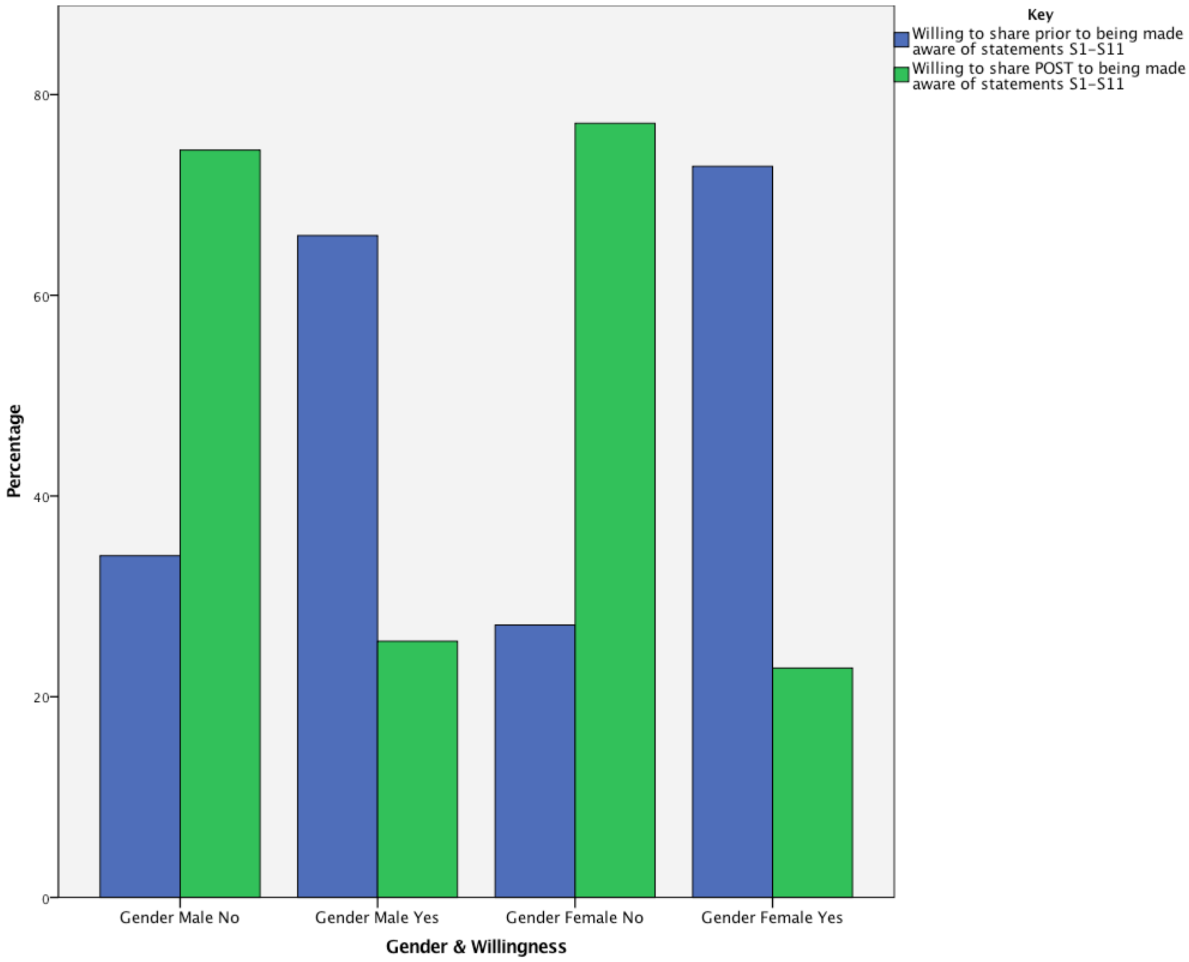
This graph shows participants level of concern in relation to 11 statements and is compared against wearable usage.

Figure 35 – Participants Willingness to Share For an Incentive, Compared Against Age



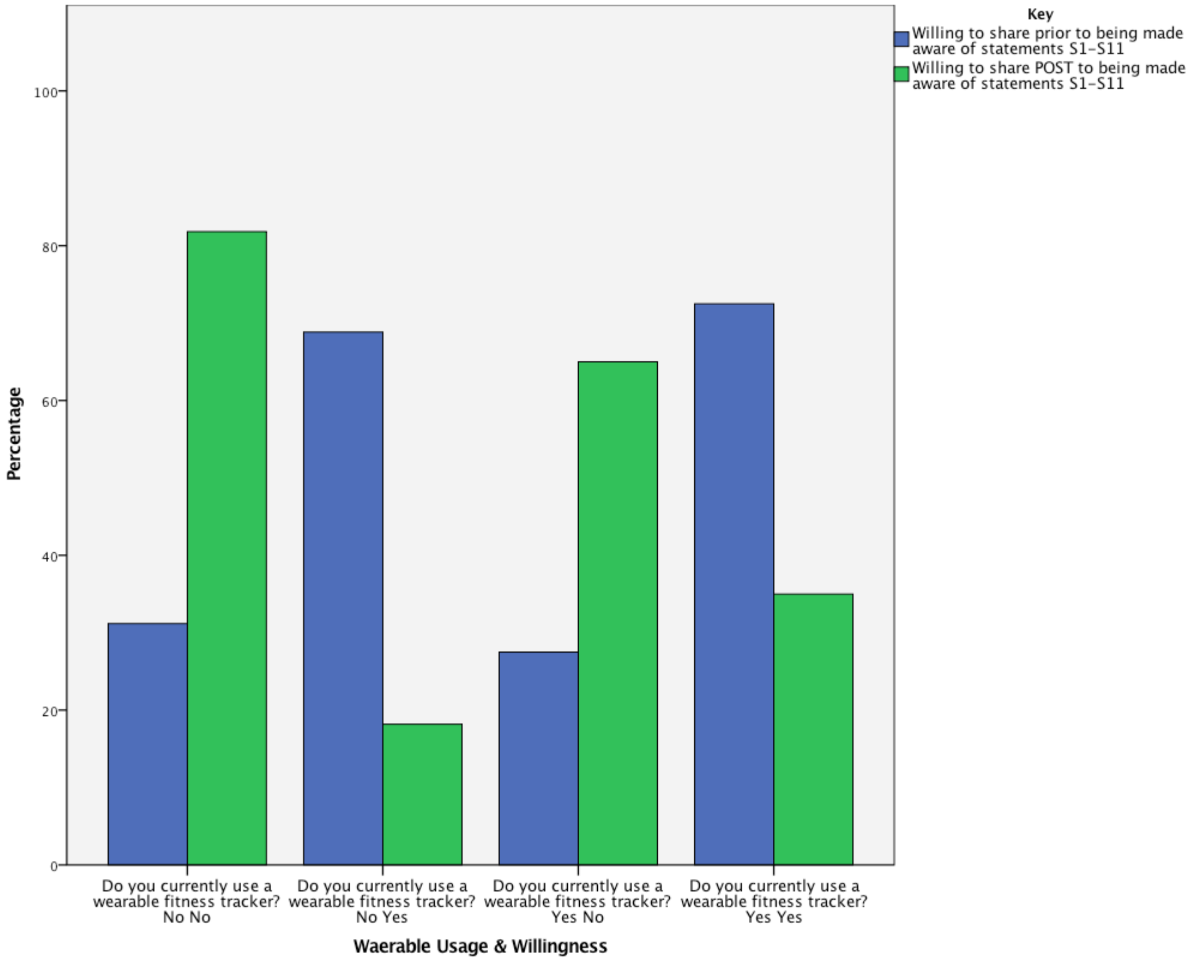
This graph shows participants willingness to share data with an employer (both before statements s1-s11 and after) and is compared against age.

Figure 36 - Participants Willingness to Share For an Incentive, Compared Against Gender



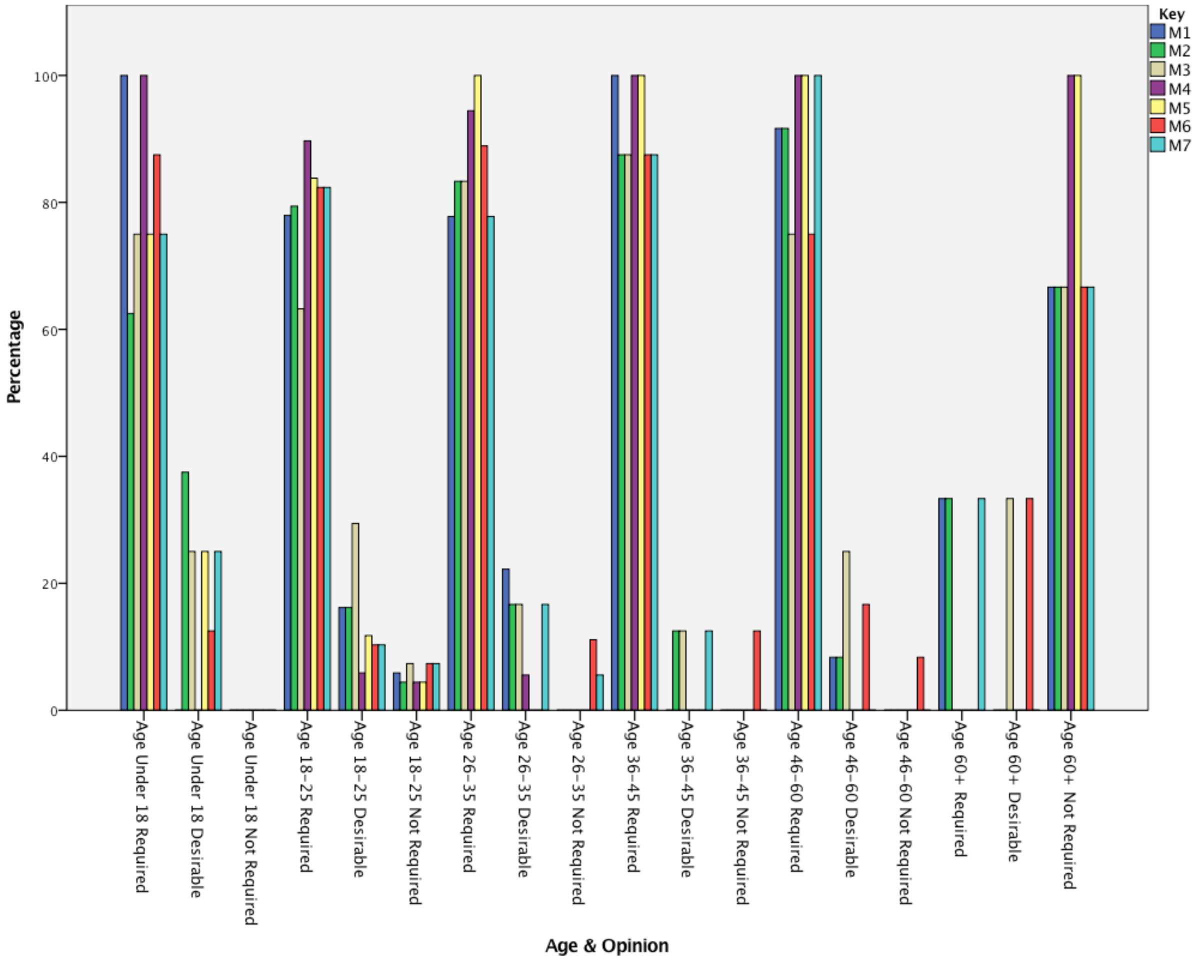
This graph shows participants willingness to share data with an employer (both before statements S1-S11 and after) and is compared against gender.

Figure 37 - Participants Willingness to Share For an Incentive, Compared Against Wearable Usage



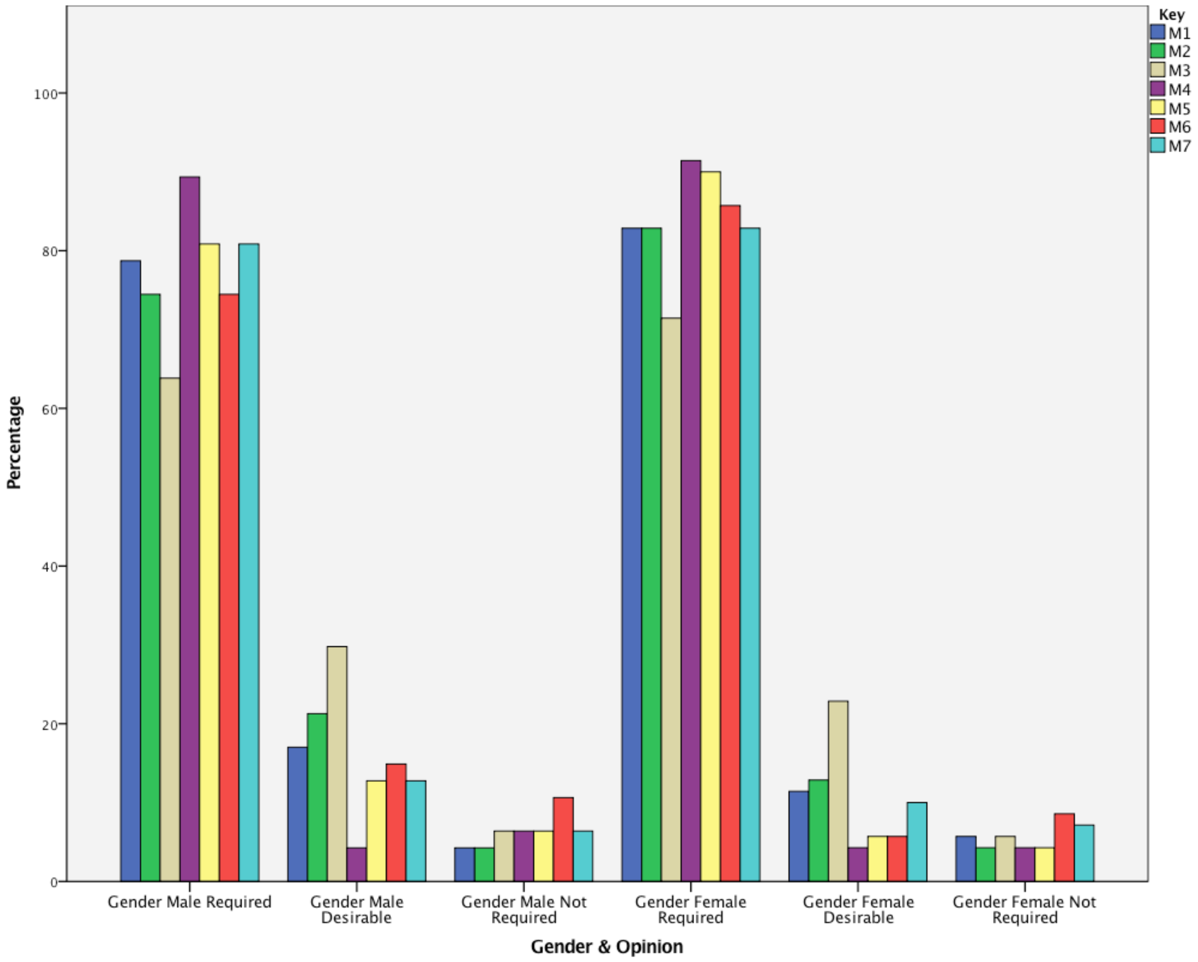
This graph shows participants willingness to share data with an employer (both before statements s1-s11 and after) and is compared against wearable usage.

Figure 38 - Participants Opinion for Protecting Their Privacy, Compared Against Age.



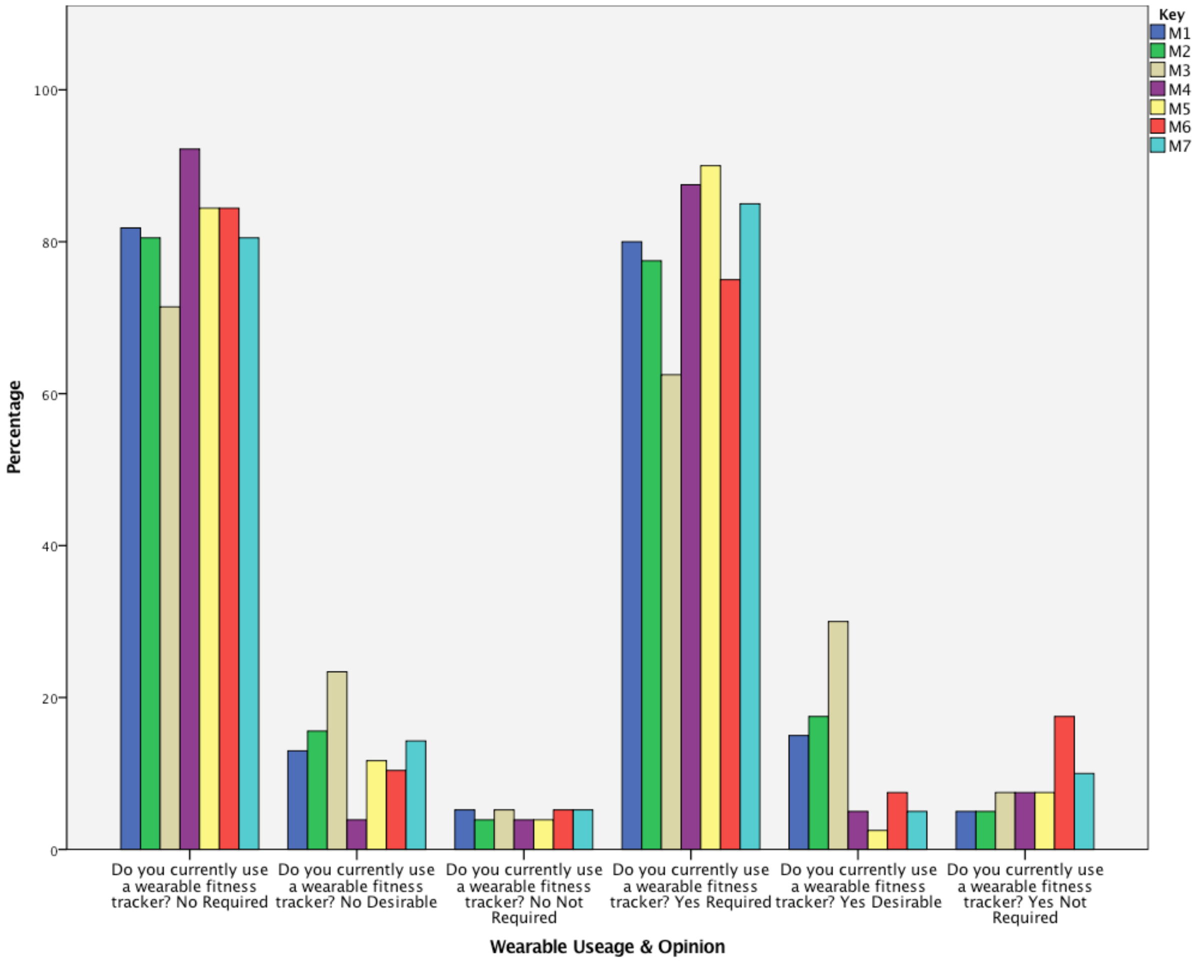
This graph shows participants opinion in relation to 7 statements for protecting their privacy and is compared against age.

Figure 39 - Participants Opinion for Protecting Their Privacy, Compared Against Gender



This graph shows participants opinion in relation to 7 statements for protecting their privacy and is compared against gender.

Figure 40 - Participants Opinion for Protecting Their Privacy, Compared Against Wearable Usage



This graph shows participants opinion in relation to 7 statements for protecting their privacy and is compared against wearable usage.

Appendix H – Interviews

Name: James King

Interview time: 5:00pm

Interview Date: 19th April 2016

James is 21 years old. He is a full time student and a frequent goer of the gym. James has previously done a placement year in which he was rewarded for the number of steps he took with a gift voucher.

> *I am familiar with wearable technology in a general sense, I know that you can get wristbands, watches and all sorts. I am also aware of what can be collected but did not know that fitness trackers had the ability to monitor sleep, but can see that being useful in regards to improving health.*
>
> *I would only be willing to share with an employer if I felt the trade-off was worth it, for example a monetary bonus or discount of some sort.*
>
> *Wasn't aware of most of these, obviously was aware that health can be improved and the monitoring of activity (as I have participated in a scheme which did so). The facts relating to sleep alarm me, especially if closely monitoring it. For example, I wouldn't like my employer to know the time I went to bed or being wrongly judged for lack of sleep, it's effectively surveillance.*
>
> *More so than before but regardless I still stand by my point, it would ultimately depend on what is in it for me. However, since being informed of possible inferences it would now depend on what they asked me to give away, I wouldn't mind activity during work hours but wouldn't be keen on sleep or weight being monitored.*
>
> *Employers should be explicit in what types of data they are collecting and allowed to view (I don't think it's their job to tell me about the possibilities but rather just what they are making use of, I can discover from the manufacturer what the device collects). Aggregate data is good but could also hinder trends that are needed for showing eligibility for rewards. Privacy policies are essential for me, they should state what employees are parting with alongside how it is anonymised (as well as how they protect the data). They should also outline what the data is primarily being used for and what*

it can potentially be used for. However, whilst it should protect the employee it should also protect the employer. Circumstances can change, I think it's a good idea to let employees opt out, it is not a responsibility but rather a bonus activity so shouldn't be forced. Appropriate security I presume will validate data gathered and thus validate eligibility for incentives, so yes this is required. Health officials should only have visibility if there is consent, this could actually help the health of employees by providing qualified professionals who can make sense of the data without compromising privacy.

I think these recommendations are good, be careful to take into consideration employee demographic and background, this will likely effect the likelihood of participation in the scheme. The rewards should be targeted at all employees and not entice everyone, for example not always monetary.

Name: **Charlotte Osling**

Interview time: **8:00pm**

Interview Date: **26th April 2016**

Charlotte is 21 years old and works full time for a leading banking firm. She attends the gym regularly and is very keen on getting involved in voluntary activities (she recently done BBC Children in Need and DIY SOS with her work).

I am somewhat familiar with the concept, my boyfriend is addicted to his Apple Watch and this has meant I never hear the end of it

I would be willing to share all my information, although I wouldn't share my weight with anyone but friends.

I am happy to share information with my employer for an incentive, I'm not sure about my weight or sleep though – how would this even benefit them!?

Wow that is incredible, I wasn't aware of these possibilities and certainly am shocked to be informed, to say I wasn't concerned would be a lie. I understand this can be used to improve employee health as my boyfriend's health has improved since using his Apple Watch but the rest are news to me!

I don't think I would actually. I think it would ultimately depend on if I was protected and was in the driving seat in regards to what they can do with my data. I'm not so much as fussed about what they give me in return.

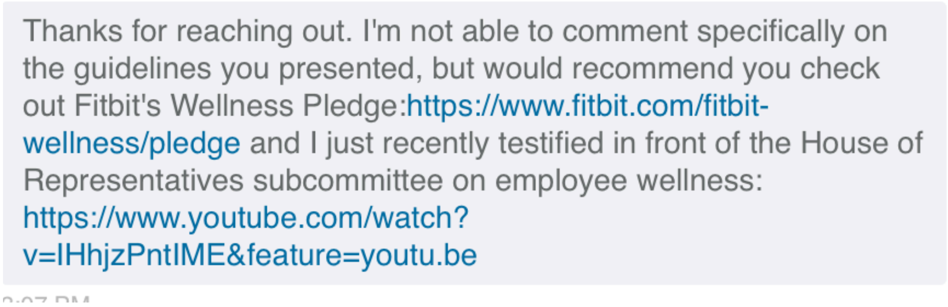
Being honest and telling me what can be done with my data is one part, actually protecting it is another, so yes this is needed, but it is not as important as other things. Aggregate data seems like this is protecting me but still allowing the employer to do as you suggested, decrease their health care costs and things. Work hours shouldn't matter if its aggregate data ****Informed Charlotte than sometimes individual activity data can be used to get rewards**** *, in that case then yes I think that what I am doing outside of work is not works business unless I am tarnishing their brand, the amount of steps I do is surveillance not tarnishing them! Privacy policy is good; it will protect the employee. Probably would be a good thing for the employer too as they would presumably have protection as well. I think it needs to include how users are protected essentially, laws and to what extent my data can be used by the employer. Like anything you do voluntary it should be able to be stopped at any point in time. I think that it should not be mandatory and ultimately up to the employee. If they do chose to quit then there is no reason to keep their data, it should always be owned by the employee. Security goes over my head as I am not technical, but if it plays a part in protecting me then of course I agree it should be included, regardless of cost. Not sure that tying a work related activity with health officials is a good thing, if it would help then I think this should be a completely separate activity in which the employer cannot see anything.*

Overall yes I think this would help protect users. The key is the privacy policy!

Amy McDonough, VP & GM, Fitbit Wellness:

Amy's response:

Figure 41 - Amy's Response



Thanks for reaching out. I'm not able to comment specifically on the guidelines you presented, but would recommend you check out Fitbit's Wellness Pledge:https://www.fitbit.com/fitbit-wellness/pledge and I just recently testified in front of the House of Representatives subcommittee on employee wellness: https://www.youtube.com/watch?v=lHhjzPntIME&feature=youtu.be

2:07 PM

Amy's House of Representatives speech:

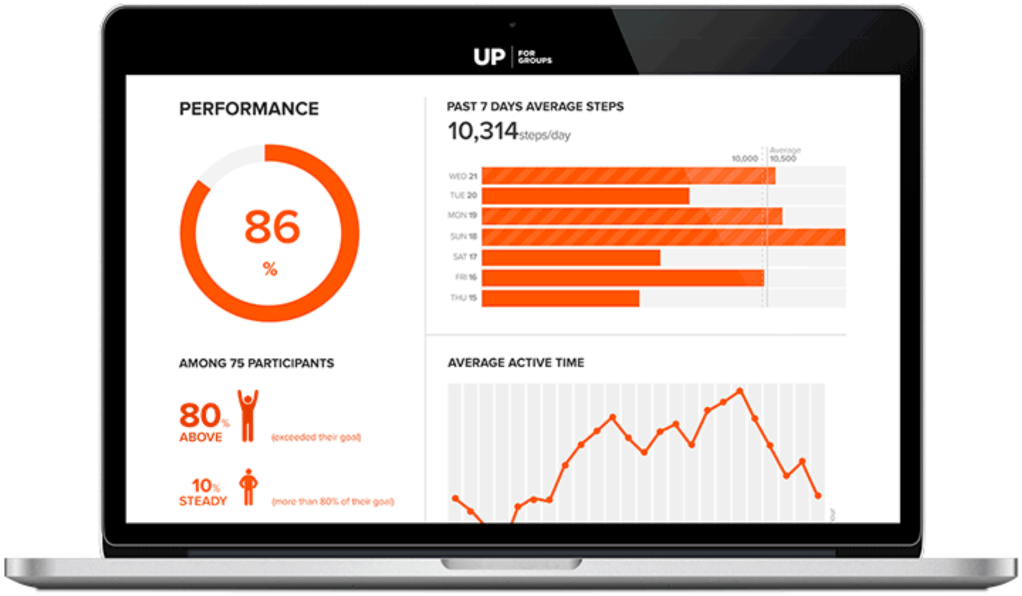
1. Corporate Wellness was born in 2010, this was in response to market need.
2. The right tools, data and guidance can empower people to take charge of their health and fitness, community is also key to fostering healthy behaviour.
3. Fitbit have a specific vision of wellness, one that addresses the needs of companies and those that power them (employers).
    a. However, the main goal is to provide opportunities for individuals to improve their health and wellness.
4. Fitbit iterate that wellness should always be **inclusive, voluntary** and **protect the privacy** of the people it aims to serve.
5. Results from corporate wellness are significant:
    a. Indiana University Health (The most comprehensive health system) Fitbit wellness customer for 2 years, 40% of participants decreased BMI. 60% of those with diabetes also decreased A1C levels.
    b. BP – reduced health care spend by 3.5%, employee's health risk declined 11.1% over a year, if involved with health management plan.
6. Better people orientated technology enables stronger results:
    a. Focus on engaging people first, incentivising them, by rewarding community driven experiences using wearable devices.
7. Companies traditionally worry about investing in wellness due to worrying about participation rates:
    a. Typical wellness programs show average 24% participation rate.

    b. Fitbit participation rates vary from company to company, but are often higher – sometimes more than 80%.

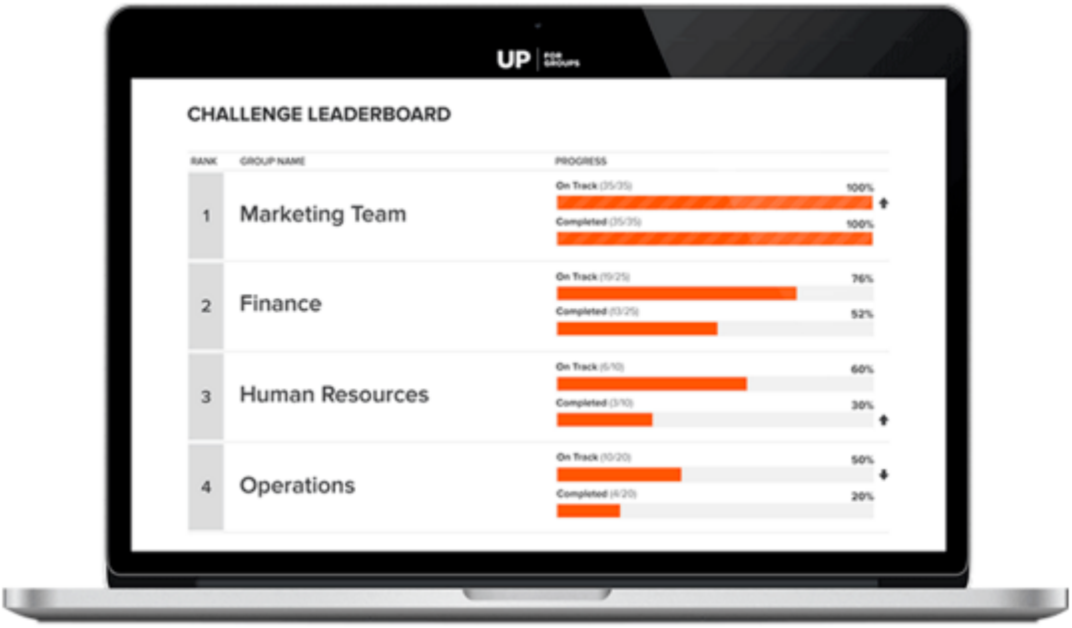
8. Ultimately these programs increase health and fitness, subsequently reducing health care costs and increasing productivity.
9. Employers are uniquely positioned to improve population health in the workplace by fostering wellness incentives which are fun, voluntary, but also protect the privacy of the people they aim to serve.
10. Seen a shift from heath officials focusing on diet and exercise, to sleep, mental health and financial wellness and stress management.
11. Wellness programs aim to help people live healthier, happier and more active lives.
    a. Inherent in this mission is the need to implement data security and privacy policies.
12. As leader – Fitbit committed to projecting user data and the health information tools people turn to for help are used properly. They believe:
    a. Participation should always be voluntary
    b. Should be given choice to opt in
    c. No penalties from saying no
    d. Employers should make employees understanding how their data will be used
13. Regulations not always clear, confusion has left some employers on side-lines. Fitbit are supportive of efforts to clarify and streamline the applicable laws and regulations that govern the structure of wellness programs.

This speech has highlighted several connections in the proposed recommendations. Especially, points 12 a-d, which have all been included as fundamental requirements. Point 11 also touches on security, this has been addressed as requirements and whilst Fitbit has room for improvement (SSL Pinning and LE Privacy), this shows their intention to improve and shift towards better protection of user's data. Amy also highlight's the benefits all parties can expect to see, as a result of participating in wellness programs, some of which are incredible. Touches on health officials using data in new and innovative ways, including focusing on mental health. This is in alignments with the proposed recommendation of supplying health officials with user's data. Also highlights the power and responsibility employers have in ensuring that their staff are healthy. Point 13 serves as justification for the inclusion of recommendations in this report. A consolidated, user derived set of recommendations will serve as a baseline for streamlining a structure which inherently includes the appropriate regulations and laws.

Appendix I – Jawbone Compliance Analysis

R1.1	Jawbone are **compliant.** Jawbone display data in an aggregate form and activity data in an individual form (only once an individual has opted in[23], as explained in Jawbones introductory blog post) *Figure 42 - Jawbone Aggregate Interface (ROSENTHAL, 2014)*  UP FOR GROUPS PERFORMANCE 86 % PAST 7 DAYS AVERAGE STEPS 10,314 steps/day 10,000 Average 10,500 WED 21 TUE 20 MON 19 SUN 18 SAT 17 FRI 16 THU 15 AMONG 75 PARTICIPANTS 80% ABOVE (exceeded their goal) 10% STEADY (more than 80% of their goal) AVERAGE ACTIVE TIME
R1.1.1	Jawbone are **compliant,** Jawbone provide the user with the option to 'opt in' prior to distribution of devices.
R1.1.2	Jawbone are **compliant,** Jawbone allow for the individual tracking of Activity data, with consent, as explained in their introductory blog post[1].
R.1.1.3	Jawbone are **not compliant.** Jawbone currently allow for the tracking outside of work hours (Saturday/Sunday), be it aggregated or individual (see Figure 42 above)
R1.1.4	Jawbone are **compliant**. Jawbone currently provide the option to revoke third party access.
R1.1.5	Jawbone are **Not compliant.** Jawbone currently provide the option to track individual sleep timings, with consent, but do not provide the ability to track employee's BMI or weight. Jawbone allow for the displaying of weight, BMI and sleep timings on individual's profiles (as per one's experiment this can lead to third-parties getting visibility of data without consent, providing profile set to 'public' or "friends and family").

[23] https://jawbone.com/blog/up-for-groups/ - Accessed April 13th 2016

R1.2	Jawbone are **compliant.** Jawbone currently provide the option to group information by teams, as shown below in Figure 43. *Figure 43 - Team Comparison Interface (ROSENTHAL, 2014)*  CHALLENGE LEADERBOARD RANK · GROUP NAME · PROGRESS 1 · Marketing Team · On Track (35/35) 100% · Completed (35/35) 100% 2 · Finance · On Track (19/25) 76% · Completed (13/25) 52% 3 · Human Resources · On Track (6/10) 60% · Completed (3/10) 30% 4 · Operations · On Track (10/20) 50% · Completed (4/20) 20%
R.1.2.1	Jawbone are **compliant.** Jawbone allow for the comparison against teams and the overall program, as shown above in Figure 43.
R1.3	Jawbone are **compliant.** Jawbone use percentage statistics to allow for the easy identification of how complete targets are, as shown above in Figure 43.
R1.3.1	Jawbone are **compliant.** Jawbone allow for the administrator to set goals and message participants for encouragement.
R2.1	Jawbone are currently **not compliant**. Hilt, et al., (2016) identified that the unique identifier (MAC Address) was fixed on Jawbone devices.
R2.2	Jawbone are **compliant.** Hilt, et al., (2016) identified that Jawbone use HTTPS encryption.
R2.2.1	Jawbone are currently **not compliant**. Hilt, et al., (2016) identified Jawbone did not currently use SSL pinning.
R3.1	Jawbone are currently **compliant.** Jawbone align the functionality of the system to their privacy policy. (In terms of personal profiles, user's data is only shared with friends they specifically add, then the user is given the option to make entries private.)

R3.1.1	Jawbone are currently **compliant.** Jawbone currently email participants and provide them with their Terms of Use and Privacy Policy (which govern user data), which must be accepted prior to participation.
R3.2	Jawbone are currently **not compliant.** Jawbone do not currently list the limitations of their devices and application. Jawbone state in their privacy policy[24]: *We apply organizational and technical measures to ensure access to your information is limited to persons with a need to know. Even though we have taken steps to protect your personal information, you should know that neither we nor any company can fully eliminate security risks.* This is somewhat admitting limitations of their security, although doesn't provide any examples of such limitations or risks.
R3.3	Jawbone are currently **compliant.** Jawbone currently email participants and inform them of the data they will be giving away before they consent to participating.
R3.4	Jawbone are currently **not compliant.** Jawbone are not HIPAA compliant. Jawbone also do little to state which laws govern their Terms of Use or Privacy Policy, and limit it to the law of the state of California, with no examples.
R3.5	Jawbone are currently **compliant** in informing users in their policy of whom the data will be shared with and in what state (aggregated), they also do not share data with anyone other than friends which have been explicitly requested.
R3.6	Jawbone are currently **not compliant.** Although Jawbone state they use affiliated and unaffiliated service providers (subject to confidentiality agreements), they do not provide any specific examples.
R3.7	Jawbone are currently **not compliant.** Jawbone provide no justification of how they ensure user's data cannot be identified from grouped data.
R3.8	N/A (This falls under the employer policy).
R3.9	Jawbone are currently **partially compliant.** Jawbones Terms of Use specifies that users have the right to terminate their participation at any time. However, the Terms of Use do nothing to explain if their data is removed completely, or if Jawbone can continue to use their aggregated data.
R4.1	Jawbone are currently **not compliant.**

[24] https://jawbone.com/privacy - Accessed 26th April 2016

R4.1.1	N/A
R4.1.2	N/A
R5.1	Jawbone are currently **partially compliant.** Jawbone's website does an excellent job of informing users of the sensors in the device, alongside the functionality they provide. Jawbone do not however provide users with any information regarding inferences possible from their data.
R5.2	Jawbone are currently **partially compliant.** Jawbone allow for the export of data and do so in 365 day instalments (better than Fitbit's 30 days). This feature is also free (better than Fitbit's, who charge a year subscription fee). It does not however provide data down to lower levels of granularity (e.g. minutes, hours), and only provides daily statistics.

References

ABIResearch, 2013. *Corporate Wellness is a 13 Million Unit Wearable Wireless Device Opportunity.* [Online]
Available at: https://www.abiresearch.com/press/corporate-wellness-is-a-13-million-unit-wearable-w/
[Accessed 10 April 3016].

Accenture, 2015. *Engaging the Digital Consumer in the New Connected World..* [Online]
Available at: https://www.accenture.com/us-en/insight-engaging-digital-consumer-new-connected-world.aspx.
[Accessed 9 February 2016].

Acxiom & DMA, 2015. *Data privacy: what the consumer really thinks.* [Online]
Available at: http://www.dma.org.uk/uploads/ckeditor/Data-privacy-2015-what-consumers-really-thinks_final.pdf
[Accessed 9 February 2016].

Apple, 2016. *Answers to your questions about Apple and security.* [Online]
Available at: http://www.apple.com/customer-letter/answers/
[Accessed 6 April 2016].

Ausick, P., 2016. *2016 Data Breaches Expose 1.8 Million Records.* [Online]
Available at: http://247wallst.com/technology-3/2016/03/03/2016-data-breaches-expose-1-8-million-records/
[Accessed 7 April 2016].

Austin, P., 2016. *Taking the Pulse of Fitbit's Contested Heart Rate Monitors.* [Online]
Available at: http://www.consumerreports.org/fitness-trackers/taking-the-pulse-of-fitbits-contested-heart-rate-monitors/
[Accessed 9 Fberuary 2016].

Barcena, M. B., Wueest, C. & Lau., H., 2014. *How safe is your quantified self?.* [Online]
Available at: https://www.symantec.com/content/dam/symantec/docs/white-papers/how-safe-is-your-quantified-self.pdf.
[Accessed 9 February 2016].

Bilger, M. et al., 2013. *The effect of weight loss on health, productivity, and medical expenditures among overweight employees..* [Online]
Available at: http://www.ncbi.nlm.nih.gov/pubmed/23632594
[Accessed 9 February 2016].

BURGESS, M., 2016. *FBI unlocks shooter's iPhone without Apple's help.* [Online]
Available at: http://www.wired.co.uk/news/archive/2016-03/29/apple-fbi-unlock-iphone-5c-court-order-dropped
[Accessed 6 April 2016].

Business Analyst Learning, n.d. *MoSCoW : Requirements Prioritization Technique.* [Online]
Available at: http://businessanalystlearnings.com/ba-techniques/2013/3/5/moscow-technique-requirements-prioritization
[Accessed 4 April 2016].

Checkland, 1999. *Systems Thinking, Systems Practice.* England: Wiley.

Clearswift, 2015. *Clearswift Insider Threat Index (CITI).* [Online]
Available at: https://www.clearswift.com/insider-threat.
[Accessed 9 February 2016].

Cyr, B., Horn, W., Miao, D. & Specter, M., n.d. *Security Analysis of Wearable Fitness Devices (Fitbit),* Cambridge, Massachusetts, U.S.A.: Massachusetts Institute of Technology.

Desarnauts, B., 2015. *The birth of a new market.* [Online]
Available at: https://medium.com/wristly-thoughts/the-birth-of-a-new-market-2b680e5ea733#.wk6l3f1je.
[Accessed 9 February 2016].
Eddy, N., 2015. *Gartner: 21 Billion IoT Devices To Invade By 2020.* [Online]
Available at: http://www.informationweek.com/mobile/mobile-devices/gartner-21-billion-iot-devices-toinvade-by-2020/d/d-id/1323081.
[Accessed 10 April 2016].
Experian, 2016. *Data Breach Industy Forecast,* s.l.: Experian.
Furberg, R. D., 2015. *Self-generated Fitbit dataset 10.22.2011-09.20.2014.* [Online]
Available at: http://zenodo.org/record/14996#.VwYyiPkrKUk
[Accessed 9 February 2016].
Galesic, M. & Bosnjak, M., 2009. Effects of Questionnaire Length on Participation and Indicators of Response Quality in a Web Survey. *Public Opinion Quarterly,* 73(2), pp. 349-360.
Gartner, 2016. *Gartner Says Worldwide Wearable Devices Sales to Grow 18.4 Percent in 2016.* [Online]
Available at: http://www.gartner.com/newsroom/id/3198018
[Accessed 11 April 2016].
Github, 2014. *A Colloquial Definition of Big, Open, and Personal Data.* [Online]
Available at: https://github.com/theodi/data-definitions.
[Accessed 10 April 2016].
Google, 2016. *European privacy requests for search removals..* [Online]
Available at: https://www.google.com/transparencyreport/removals/europeprivacy/.
[Accessed 9 February 2016].
Hill, K., 2011. *Fitbit Moves Quickly After Users' Sex Stats Exposed..* [Online]
Available at: http://www.forbes.com/sites/kashmirhill/2011/07/05/fitbit-moves-quickly-after-users-sex-stats-exposed/#e54a4a379e73
[Accessed 9 February 2016].
Hilt, A., Parsons, D. C. & Knockel, J., 2016. *Every Step You Fake A Comparative Analysis of Fitness Tracker Privacy and Security..* [Online]
Available at: https://openeffect.ca/reports/Every_Step_You_Fake.pdf
[Accessed 9 February 2016].
IDTRC, 2016. *Data Breach Reports.* [Online]
Available at: http://www.idtheftcenter.org/2016databreaches.html
[Accessed 6 April 2016].
Jan & Brian, 2016. *end-to-end encryption.* [Online]
Available at: https://blog.whatsapp.com/10000618/end-to-end-encryption
[Accessed 6 April 2016].
Jawbone, 2016. *UP3 by jawbone | A smarter activity Tracker for A Fitter you..* [Online]
Available at: https://jawbone.com/fitness-tracker/up3.
[Accessed 9 February 2016].
Jourová, V., 2015. *Data protection Eurobarometer.* [Online]
Available at: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf
[Accessed 9 February 2016].
Karagöl, A., Özçürümez, G. & Aslı Nar, N. T., 2014. Association of body mass index with depression and alexithymia. *Anatolian Journal of Psychiatry,* 15(3), pp. 207-213.
Kaye, K., 2014. *FTC: Fitness Apps Can Help You Shred Calories and Privacy.* [Online]
Available at: http://adage.com/article/privacy-and-regulation/ftc-signals-focus-health-fitness-

data-privacy/293080/.
[Accessed 9 February 2016].
Kelly, S., 2016. *Husband Discovers Wife if Pregnant through Fitbit.* [Online]
Available at: http://mashable.com/2016/02/10/fitbit-pregnant/#e9hK_S4Vokqa.
[Accessed 9 February 2016].
LICBS & Zeno, 2014. *The Wearables Privacy Report,* London: Zeno.
Love, J., 2015. *Exclusive: Apple mines big profits from Watch band..* [Online]
Available at: http://www.reuters.com/article/us-apple-watch-idUSKBN0OY0FC20150618.
[Accessed 9 February 2016].
Maddox, T., 2015. *The dark side of wearables: How they're secretly jeopardizing your security and privacy.* [Online]
Available at: http://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/
[Accessed 9 February 2016].
Marrs, M., 2014. *7 Best Survey Tools: Create Awesome Surveys For Free!.* [Online]
Available at: http://www.wordstream.com/blog/ws/2014/11/10/best-online-survey-tools
[Accessed 9 February 2016].
Microsoft, 2016. *Microsoft Band Sensors.* [Online]
Available at: https://www.microsoft.com/microsoft-band/en-gb/support/hardware/sensors
[Accessed 24 March 2016].
O'Connor, S., 2015. *Wearables at work: the new frontier of employee surveillance..* [Online]
Available at: http://www.ft.com/cms/s/2/d7eee768-0b65-11e5-994d-00144feabdc0.html#axzz435hNkmkP.
[Accessed 9 February 2016].
Oslon, P., 2014. *Fitbit Data Now Being Used In The Courtroom..* [Online]
Available at: http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/#2cb45ba5209f.
[Accessed 9 February 2016].
Oslon, P., 2015. *Fitbit On Track To Sell Thousands More Devices Through Barclays, GoDaddy And Other Employers..* [Online]
Available at: http://www.forbes.com/sites/parmyolson/2015/10/20/fitbit-employers-barclays-godaddy-wellness/#172dbcc83baa.
[Accessed 9 February 2016].
Oslon, P., 2016. *Fitbit's Game Plan For Making Your Company Healthy..* [Online]
Available at: http://www.forbes.com/sites/parmyolson/2016/01/08/fitbit-wearables-corporate-wellness/#48f63f4d4527.
[Accessed 9 February 2016].
Outlaw, 2010. *Workers may find discrimination claims for depression easier after EAT ruling.* [Online]
Available at: http://www.out-law.com/page-11151
[Accessed 9 February 2016].
Parliament, European, 2015. *New EU rules on data protection put the citizen back in the driving seat.* [Online]
Available at: http://www.europarl.europa.eu/news/en/news-room/20151217IPR08112/New-EU-rules-on-data-protection-put-the-citizen-back-in-the-driving-seat
[Accessed 9 February 2016].
Peat, Mellis & Williams, 2002. The Importance of Pilot Studies. In: s.l.:s.n., p. Table 3.23 P123.

PWC, 2014. *The Future of Privacy.* [Online]
Available at: http://www.pewinternet.org/2014/12/18/future-of-privacy/.
[Accessed 9 February 2016].
PWC, 2014. *Wearable Technology Future is Ripe for Growth..* [Online]
Available at: http://www.pwc.com/us/en/press-releases/2014/wearable-technology-future.html.
[Accessed 9 February 2016].
PWC, 2015. *Half of people would use a workplace smartwatch – PwC research..* [Online]
Available at: http://pwc.blogs.com/press_room/2015/04/half-of-people-would-use-a-workplace-smartwatch-pwc-research.html.
[Accessed 9 February 2016].
Rahman, M., Carbunar, B. & Bani, M., 2013. *Fit and Vulnerable: Attacks and Defenses for a,* Florida International University, Miami, FL: School of Computing and Information Sciences.
Raosoft, 2016. *Sample Size Calculator.* [Online]
Available at: http://www.raosoft.com/samplesize.html
[Accessed 9 February 2016].
Rijmenam, M. v., 2016. *The Re-Identification Of Anonymous People With Big Data.* [Online]
Available at: https://datafloq.com/read/re-identifying-anonymous-people-with-big-data/228
[Accessed 6 April 2016].
ROSENTHAL, A., 2014. *JAWBONE LAUNCHES UP FOR GROUPS.* [Online]
Available at: https://jawbone.com/blog/up-for-groups/
[Accessed 13 April 2016].
Ruiz, J., 2016. *Data Privacy Day: the new EU Data Protection Regulation explained.* [Online]
Available at: https://www.openrightsgroup.org/blog/2016/data-protection-day-and-the-new-eu-regulation
[Accessed 9 February 2016].
Solicitors, Crossland Employment, 2016. *Employers' Attitude to Obese Candidates..* [Online]
Available at:
http://www.crosslandsolicitors.com/site/crossland_news/Employer_survey_obese_candidates_2015_html.
[Accessed 9 February 2016].
Taylor PHD, D. J. et al., 2015. Epidemiology of Insomnia, Depression, and Anxiety. *Sleep,* 28(11).
Willan, H. F., 2015. *New General Data Protection Regulation, December 2015..* [Online]
Available at: http://www.hfw.com/New-General-Data-Protection-Regulation-December-2015
[Accessed 9 February 2016].
Williams, B., 2005. *Soft Systems.* [Online]
Available at: http://www.bobwilliams.co.nz/Systems_Resources_files/ssm.pdf
[Accessed 9 February 2016].
Wisbey, B., 2012. *Workplace experiment: How does your sleep affect your productivity?.* [Online]
Available at: http://blog.rescuetime.com/2012/11/08/workplace-experiment-how-does-your-sleep-affect-your-productivity/.
[Accessed 9 February 2016].