To be published in the Multimedia Privacy & Security Workshop at 24th ACM Conference on Computer & Communication Security (CCS 2017)

Unwinding Ariadne's Identity Thread: Privacy Risks with Fitness Trackers and Online Social Networks

Angeliki Aktypi
Department of Computer Science
University of Oxford
angeliki.aktypi@cs.ox.ac.uk

Jason R.C. Nurse
Department of Computer Science
University of Oxford
jason.nurse@cs.ox.ac.uk

Michael Goldsmith
Department of Computer Science
University of Oxford
michael.goldsmith@cs.ox.ac.uk

ABSTRACT

The recent expansion of Internet of Things (IoT) and the growing trends towards a healthier lifestyle, have been followed by a proliferation in the use of fitness-trackers in our daily life. These wearable IoT devices combined with the extensive use by individuals of Online Social Networks (OSNs) have raised many security and privacy concerns. Individuals enrich the content of their online posts with their physical performance and attendance at sporting events, without considering the plausible risks that this may result in. This paper aims to examine the potential exposure of users' identity that is caused by information that they share online and personal data that are stored by their fitness-trackers. We approach the privacy concerns that arise by building an interactive tool. This tool models online information shared by individuals and elaborates on how they might be exposed to the unwanted leakage of further personal data. The tool also illustrates the privacy risks that arise from information that people expose, which could be exploited by malicious parties such as fraudsters, stalkers and other online and offline criminals. To understand the level of users' awareness concerning their identity exposure when engaging with such devices and online services, we also have conducted a qualitative analysis and present our findings here.

CCS CONCEPTS

• **Security and privacy → Privacy protections**; • **Information systems → Data mining**; • **Human-centered computing → Visualization toolkits**; **Empirical studies in HCI**;

KEYWORDS

Privacy; Internet of Things; Wearables; Fitness Trackers; Online Social Networks; Identity Exposure

1 INTRODUCTION

The Internet of Things (IoT) is an emerging research topic that attracts the attention of both the academic community and the industrial sector. We are on the cusp of a revolution on connectivity where the end-users can interact with a vast number of devices and platforms redefining their daily life. A total of 15.4 billion connected devices were already installed in 2015 and this is expected to continue, with an estimate of 30.7 billion and 75.4 billion connected devices by the years 2020 and 2025, respectively [33]. The newly introduced connections and recently developed capabilities, such as opening and closing a home's front-door from distance by using a smartphone, blur the boundaries between the virtual and the physical world.

We are entering a novel scientific era that departs from the existing technological status-quo and goes far beyond it, shifting the way in which we interact with devices and with each other. IoT does not only correspond to the new connections that are emerging but it is more about the launch of an ubiquitous technology. In this paradigm, data is automatically collected, generated and shared and the devices learn about consumers by observing their habits, tendencies, and preferences. Furthermore, these smart devices are constantly monitoring the environment through sensors and dynamically making decisions and changes in real time [60].

However, even if it is ultimately appealing to make these devices part of our life, convinced by their intelligence and promises for a better life, the potential flaws and vulnerabilities that perhaps accompany them are putting the end-user at a remarkable risk of cyberattacks. Several case studies from different researchers [5, 21] have discovered that a significant number of IoT devices do not use traffic encryption or strong authentication and, in addition, appear to be exposed to common vulnerabilities.

The greatest concern does not arise from the isolated study of those security breaches in each device that we use but from the accumulation and the quest for correlations between the information gathered from different resources. Two good examples are illustrated in [14, 42] where the authors analyse the digital footprint that we create through our use of portable technology devices and systems log-files. Ultimately, they could use these to infer private and social relationships between the device owners, using a range of similarity metrics.

The problem is even more salient if we also consider the way that end-users interact with their devices. Most of the time they bypass documentation, driven by their low concern for privacy or the lack of comprehension of privacy notices [39], and become bound to conditions of which they have little awareness. Although individuals value privacy and nominally mind personal data disclosure, they neither employ privacy precautions nor restrict the information they share on-line. This is what once more brings the Privacy Paradox [61] to the surface.

All the above factors attest that privacy remains one of the major concerns of IoT. Lack of supervision of personal data propagation and dissemination results in sensitive information leakages that question users' trust as far as connected IoT devices are concerned [62]. Security and especially privacy issues are stated as the Achilles heel for the IoT industry [17], establishing them as its major obstacles towards its expansion.

This paper studies the potential exposure of users' identity that is caused by information that they share online and personal data that are stored by their fitness-trackers. Our contribution is twofold. First, we develop an identity-exposure tool which seeks to

determine the leakage of information related to each user's identity. This tool is initiated by data shared both on OSNs and by wearable IoT devices, and adds further value by also presenting potential privacy risks. Hopefully, the correlated illustration of the inferred elements will help users and interested stakeholders better assess their online digital footprints. Thus, they will be more capable of making informed privacy decisions.

In many ways, we regard our work as the natural progression from related work in online identity exposure [10, 13, 25]. However, in our research we do not limit our scope to the security and privacy concerns that arise by derivations only on OSNs, but we expand it to the IoT context and especially to wearable fitness tracking devices. We decided to focus on this specific category of connected devices driven by their high popularity among users [28] and the functionalities that they can provide with a variety of sensors. We are not aware of any other work that attempts to create such a tool for assessing a user's consequential risk exposure in such domains.

Our second contribution is a reflective user-based study where we attempt to shed light on the level of users' awareness concerning their identity-exposure when engaging with wearable devices and OSNs. Additionally, we have examined the effectiveness of our tool in visualising identity exposure risks and in allowing users to gain some understanding of the flow of personal data. This data can derive from using different connected devices in the interconnected world or from engaging with OSNs.

The remainder of our paper is structured as follows. Section 2 reviews the literature concerning previous related work on identities across both the online and offline domains. Section 3, then, describes our novel, identity-exposure tool that seeks to fuse all the identity attributes that can be extracted primarily from wearable IoT devices and OSNs into a comprehensive and systematic model. Section 4 continues by presenting the methodology adopted and the results received from our empirical investigation concerning users' awareness of privacy risks and tool's effectiveness of achieving our goal. Finally, in Section 5 we consider possibilities for further research steps and we conclude our work.

2 RELATED WORK

2.1 Identity exposure in OSNs

Users' difficulty following and observing the information that concerns them in cyberspace, especially when the digital and physical world converge, can lead to the exposure of their identity without their consent. A critical data resource to retrieve personal data is Online Social Networks (e.g., Facebook, Instagram, LinkedIn) where the substantial personalised data that users publish can provide deep insights into their private lives. Previous work has addressed the privacy concerns raised within OSNs related to users' identity exposure.

Krasnova et al. in their study [30] demonstrated that concerns about organizational threats (e.g., bullying, stalking) and social threats (e.g., data collection by the OSN provider, information use by third parties) constitute two underlying dimensions of the "Privacy Concerns in Online Social Networks". These construct and have an impact on users' self-presentation strategies. In particular, users tend to reduce the amount of information disclosed and become more conscious about the information they reveal as a response to their concerns regarding organizational and social threats, respectively.

In Creese et al. [13], the authors present a novel data-reachability matrix that facilitates the assessment of personal information that is either directly shared online by users or inferred from their correlation. It has also been argued that the functional locations (i.e., home, work, leisure and transport) of human activities can be traced with relatively high accuracy by low density geo-location data from tweets while using visual or textual representations; in which case the former techniques perform better than the latter ones [32].

An innovative system that provides tailor-made feedback about online identity exposure, has been designed by Emanuel et al. [16]. In that instance, those authors have considered the work in [25], which refers to a mathematical model that investigates individuals superidentities. The concept of superidentities focuses attention on the aftermath of the combination of measures across online and offline contexts so that identity in one domain can be cross-referenced with identity in the other.

As the digital horizon is continuing to expand and big data analysis and machine learning techniques are becoming more mature, the level of granularity of each user' digital footprint is more prominent. It has been proven [41] that it is not only possible to intercept elements for a person's identity from online material but it is also feasible to distinguish between real and fake online identities based on how normal (or "natural") their persona appears.

In view of everything that has been mentioned so far, it is suggested that our presence on OSN leaves enough trails to reveal our true physical identity. Under certain circumstances the ability to track identity elements with high accuracy can be proven to be beneficial. A good example is the application of such a methodology by law enforcement where police analysts undertake the task of analysing and processing data throughout the criminal investigation [12]. However, concerns arise when these monitoring capabilities are used either by the government for surveillance of citizens [7] or by adversaries in cyberspace for attacking online users [35].

2.2 Security and privacy issues in the IoT

The ubiquity and dominance of technology in our lives has been accompanied by many security and privacy challenges that are raising concerns related to users' identity exposure even higher. Pervasive computing devices that allow identity and context information to be gathered, stored and exchanged easily are rapidly emerging. Under this regime, personal privacy might be sacrificed to a greater extent than ever before. However, as argued in [65], users tend to have different privacy preferences and to apply divergent mitigation techniques to preserve their identity, quite often not related to one another. On top of that, the demanding task of managing and processing the immense volume of data that is generated causes doubt towards potential data leakages of personal information. As demonstrated in [52], it is feasible that personal data can leak from a Smart Home environment that uses encrypted communications, by performing information leakage attacks and applying machine learning techniques.

Prior studies [44] have reported that users are "extremely" or "somewhat" worried about the exposure of their personal data, suggesting that privacy concerns could be a significant barrier to the growth of the IoT. In [24], the authors have tried to integrate the user in the data-propagation chain between different connected devices in order to address the lack of transparency of IoT applications. They implement a trust-feedback toolkit that evaluates trust perception of end-users in simulated and real IoT systems. In such a way industrial developers of IoT technologies could be informed about users' security and privacy preferences and ensure their trust and acceptance.

Researchers in [6] identifying users' privacy concerns have tried to gain initial insights into users' perceptions of data transactions around the BitBarista connected coffee-machine. The study emphasises that increasing transparency of data transactions helps towards gaining users' trust. In addition, it corroborates users' discomfort and anxiety around data gathering that is interwoven with their conception of IoT systems. Furthermore, it has been shown [54] that users' decisions about whether to disclose contextual information (current location, activity and social surrounding) are affected not only by the sensitivity of the disclosed information itself, but also by the purpose for collecting the data.

2.3 Security and privacy issues in wearable IoT

The rapidly emerging trend of "sensor mania" in the IoT ecosystem [57] is raising more privacy concerns. Nowadays, users perform a more refined 24/7 monitoring of their activities, performances and preferences taking advantage of a proliferation of wearable IoT devices such as sport trackers and smart-watches. In [6], the authors draw attention to this newly introduced trend of "quantified self" where people are tracking every facet of their lives with the aid of technology, establishing it as remarkable source of personal data leakages.

The neglected security aspect on the design of those connected devices [3, 49] facilitates the processing and collection of personal information elevating higher the risk of exposing users' identity data without their consent. The privacy risks emanate from both the way that these huge amounts of personal data are transmitted though different platforms; and the way that they are collected and stored by the organisations that host them.

In many cases the wearable fitness tracking devices are used in conjunction with a base-station or a smartphone application and a cloud distribution or a web server, introducing many attack vectors on the communication between the parties involved. In [48, 64] the authors evaluate the security and privacy properties of Fitbit, a fitness-tracker which also has online social network access and propose means to eliminate the vulnerabilities identified. A similar security assessment is also presented in [11], where nine fitness wristbands, along with the corresponding Android applications, were monitored in live operation. The results obtained from the analysis revealed that there is abundant room for further progress in securing wearable devices, as authentication and encryption mechanisms are implemented poorly or not at all.

Unfortunately, as previously stated, privacy concerns do not arise only from technical security breaches of the wearable devices and their communication with cooperative third parties. The data produced is regularly handled and hosted on the servers of fitness companies, so users are subjected to their applied administration privacy policy. It is worth mentioning that wearable devices may not be covered by Health Insurance Portability and Accountability Act (HIPAA) Rules. Consequently, consumers may be providing consent for their health data to be used by non-HIPAA-covered entities without knowing exactly how their data will be collected, protected, and used [19]. The study demonstrated in [34] and its preliminary technical report [47] analyse a variety of applications as to whether they are compliant with their terms and conditions or not. It reveals that Runkeeper was sending users' personal data to third parties when it was not in use, without their consent. In addition, the analysis also finds that from the Runkeeper's privacy policy declaration it was unclear whether the application deletes personal data routinely or when the users request it or delete their account.

All of the above-mentioned security breaches have set the scene for a range of potential privacy risks. In [23] the authors have examined the privacy and security properties of eight of the most popular fitness-trackers. They identify their security vulnerabilities and elaborate the risks they introduce to the users. A more recently released study [40] focuses on the current digital health marketing practices that take advantage of the "connected-health" system that is formed by wearables, and threaten the privacy of consumer health information. It also offers suggestions on how different sectors such as the government and the industry can work together to propose adequate federal laws to safeguard personal health information data collected by wearables.

The goal of our study is to address the privacy issues that arise when users engage with both the IoT domain by using wearable IoT devices in particular, and OSNs. The research tests the hypothesis that the significant personal information that is stored on the wearable IoT devices and shared on OSNs, can infer other personal characteristics related to users' identity. Hence, we have built an interactive tool that describes users' identity exposure by combining online data from these two sources and identifies potential risks that users might face. To understand the level of users' awareness concerning the leakage of their private information and to draw conclusions about the effectiveness of our tool, we have subsequently conducted a qualitative analysis. Throughout this user-based study we performed interviews with eight participants and in the following sections we elaborate on our findings.

3 IDENTITY-EXPOSURE TOOL

In order to examine users' potential identity exposure, we have designed and developed an interactive tool. The tool is initiated by data that is stored by wearables (entered by the user or calculated by the device based on the user's information and activity) and information that is posted on OSNs. We choose to combine these two different domains motivated by the great amount of private data that are communicated through them and that can be used as information sources for identity data leakages. Our main thought was that despite the increased attention that has been given to the security and privacy aspect within OSNs following their established presence in our lives, security is still neglected within the newly evolving IoT domain. To narrow the scope of our study

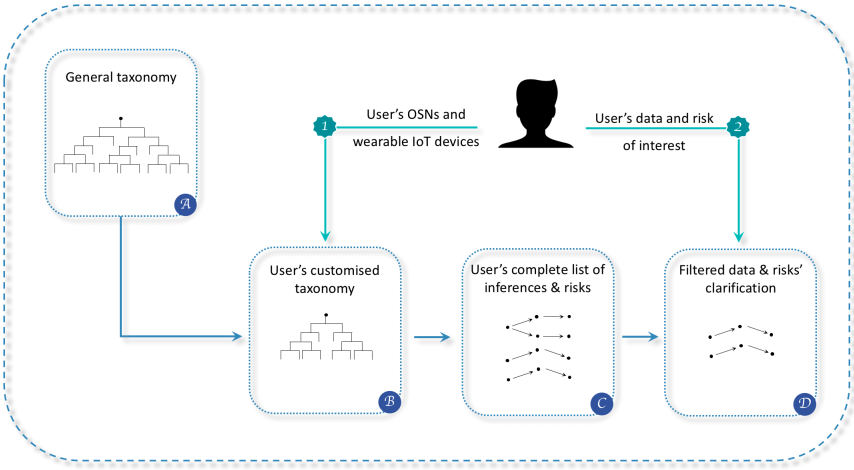

Figure 1: The workflow of our identity-exposure tool

we have chosen to focus on wearable devices driven by the highly confidential and identity-related personal data that those devices are handling.

In the past, previous work [13] has investigated how data may be aggregated across OSNs to highlight additional risks. For our study, we consider the incorporation of both the private information posted on users' OSN profiles and the personal data stored on their wearable IoT devices. We assume that this data-mining could be available to malicious parties for exploitation. Such an event could occur via security breaches or due to the users' choice to share publicly their posts on OSNs. Another possibility could be users unknowingly or knowingly consenting to companies' privacy terms and conditions that allow them to trade their information to third parties.

3.1 Overview of the Tool

Our tool is completely agnostic of any OSN or IoT device, therefore meaning that any specific wearable device can be added and used. Its usage is demonstrated in the workflow in Figure 1. Users interact directly with the tool by providing input at two different moments. In the core of the tool there is a general taxonomy, illustrated in tool's component A (see Figure 1) that functions as a retrieval database. This general taxonomy contains the identity attributes that users might be expected to share (e.g., name, location) based on the OSNs that they participate in and the wearables they use. We delineate its main features and describe the process that we follow for its definition in the following subsection 3.2.

As an initial step in the tool, users are expected to tailor the identity attributes to their context by specifying the different OSNs in which they are members and the wearables, in particular fitness-trackers, that are in their possession. The tool automatically customises the general taxonomy based on users' choices and builds a personalised one, depicted in tool's component B (see Figure 1). Based on the customised taxonomy the tool later allows visualisation of the risks faced by the user, an illustration which can be seen in component C that is built around three different axes. We elaborate further on these in the subsection 3.3. The second interaction point and the last illustration, depicted in component D, are optional. Their goal is to help the user to navigate across the different risks in a more efficient way and understand them better. This is also explained further in that subsection.

3.2 Taxonomy

The initial step of our study was the creation of a taxonomy to categorise all the available identity attributes that can be collected from the OSNs and IoT, in particular wearable IoT domains. This classification allows us to determine the digital traits that can be leveraged to yield a more detailed picture about an online user's identity.

To define our taxonomy, we used a grounded theory (GT) approach. Originating in the field of sociology, GT has become a popular research method through which new frameworks, models and theories can be developed by a process of data-gathering, categorisation and coding, followed by various comparative and theoretical analyses of findings [63]. As a research method, it is highly appreciated for its proximity to the data as well as its ability to identify and group themes [53]. To this end, we use it for our study, although the construction of a taxonomy is not one of its typical applications.

For our research, we have studied various academic publications relevant to identity exposure through the use of OSNs (e.g., [13, 25, 32]). We have also examined several industry-based reports and media articles concerning the privacy risks caused by the use of wearable and similar IoT devices (e.g., [6, 20, 34, 51]). Finally, in order to reflect the already existing perils, we have paid considerable attention on studying the capabilities of the state-of-the-art wearable devices and fitness-trackers applications that are currently available to the end-users in the market (for instance, [18, 46, 56]).

Hence, we have created a taxonomy that demonstrates the elements that compose the digital footprint generated for an individual while engaging with different aspects of the digital world, both the OSNs and the wearable IoT devices. Figure 2 illustrates the two subnodes of the central digital footprint node on which our study is focused. In more detail, the resulting hierarchy contains three

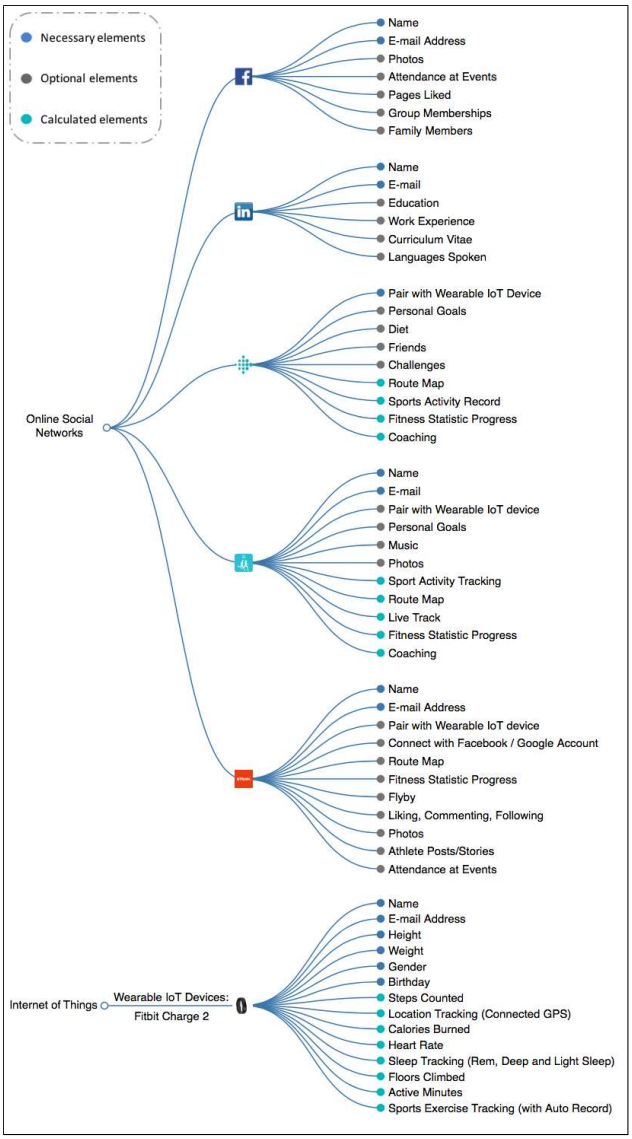

Figure 2: An example of a user's customised taxonomy

distinct levels, with the top-level representing the two domains of OSNs and IoT on which our study is focused, and the level below showing a subdivision within each domain. For the OSNs domain we have identified different networks of which the user might be a member, using their official logos for their visual representation, whereas for the IoT domain we have highlighted different groups of connected devices. Finally, the last elements of the hierarchy are the actual identity attributes that can explicitly be captured, for example the birthday, height, steps counted and heart-rate within the wearable "space".

The application of GT helped us identify the newly emerging trend of OSNs specifically dedicated to athletes. Fitness applications (e.g., Strava, Runkeeper) and online dashboard platforms designed by the fitness-trackers companies and dedicated to the community of their customers (e.g., Polar Flow, Suunto Movescount), exceed self-tracking and personal analytics functionalities. The additional capabilities that they are providing, interaction with other users, uploading of photos, sharing personal posts to name but a few are imitating the ones commonly encountered on OSN. The conceptual interpretation of such competences leads us to initially develop and then refine our taxonomy categorising them under the group of OSNs, even though they are part of the "quantified self" system.

One important aspect of the taxonomy is the fact that it allows control of fidelity around the elements of identity by using different illustrations. Thus, steel-blue filled circles have been used to indicate the elements that are explicitly necessary for the creation of an online account or the use of a wearable. Furthermore, dark-grey filled circles have been used to illustrate data that are optional and therefore each user decides whether they are going to be entered or used. Finally, turquoise filled circles are used for showing elements that are measured by the wearables or the platforms based on the input data and users' activity.

3.3 Inferences and Risks

Simply having a set of identity attributes is not enough to give rise to causes for concerns about identity exposure. As outlined above, the main motivational question was what kind of previously unknown elements of identity could be communicated either directly or through correlation from a wide range of input. In particular, we have focused both on the isolated and the aggregative study of the several identity attributes that are shared within the domain of wearable IoT devices and OSNs. Also, our parallel objective was to investigate the kind of privacy risks that users encounter, possibly without knowing. To this end, we introduce the second core concept of our tool: the inferences and the derived risks.

We have based our postulations on already published academic and industrial research evidence and general knowledge in the field. To illustrate and communicate our findings to the user we have used a visualisation depicted in Figure 3. As we can observe it is divided into three main columns: the first one contains the identity attributes that are specified by the user's customised taxonomy. Those identity attributes are used individually or in conjunction with others (indicated with aggregation symbols) to infer other identity characteristics of the user, thus forming the second column of the illustration. Finally, the risks that are a broader consideration of all the identity attributes that might be gathered or used by someone else to potentially invade the privacy of a person constitute the third column of the illustration. Sequences of arrows indicate how the surveyed data point(s) can be projected to reach inferences and exploited for significant risks to arise.

To facilitate navigation, a search auto-complete widget has been added to filter the identity attributes that are of most interest to the user. All of the identified risks related to the attributes are displayed on a provided list. The user can select a risk and ask for clarification of it. Then, emerging popup windows will provide more information concerning the risk and its potential mitigation techniques. In Figure 4, an example of filtered data and of a risk clarification based on a user's request is portrayed.

To give an example of the inferences made and the risks identified, we now consider a few of them and subsequently present

Figure 3: Excerpt of identified inferences and risks

them in detail. In order not to detract from the overall discussion of the tool we keep this presentation brief, hence the inferences and risks outlined in this section capture only a subset of the overall ones demonstrated by our tool. It should be noted that the value of the tool is in the approach, not specifically the values with which it is populated.

The first risk, identified in Figure 3, is that of *financial loss due to home burglary*, especially targeting high-income neighbourhoods. The possibility to map the route of a run can easily expose someone's home address as normally it will be the starting and ending point of the distance covered. The disclosure of a user's home location can be even more precise if the data from the wearable's altimeter sensor were used that could reveal the floor where someone lives. Furthermore, users' past sporting activity could divulge their behavioural patterns, particularly the time slots when they are away from home. Thus, potential thieves would have all the information they might need to perform their criminal actions without the fear of exposing themselves. Social media have already been identified as a great source of careless public exposure of personal data to criminals [27]. The combination of the publicly accessible data on OSNs with the data obtained by fitness-trackers can make the available information more precise and raise the level of the privacy threat that their users encounter.

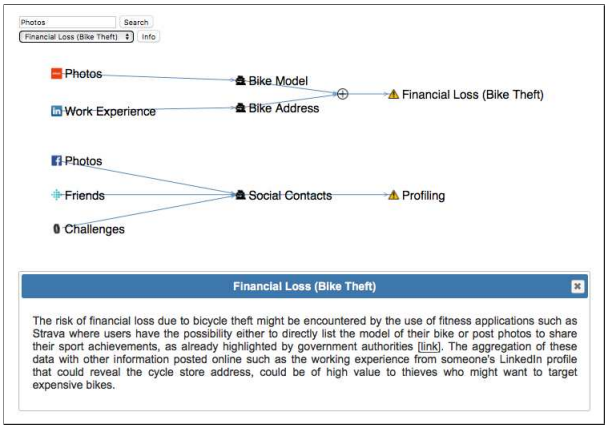

Figure 4: An example of filtered data and the clarification of a risk based on a user's request

In addition, another risk that we described is the one of *stalking*. Fitness social application platforms provide users with the ability to observe their activity surroundings with multiple functionalities offered on them. For example, Strava "Flyby" and Runkeeper "Live Track" features enable users to identify other individuals they crossed paths with on their activity and broadcast live their route, respectively. It is the constant broadcasting of users' presence that makes those fears reported in [38], realistic since someone can easily trace the whereabouts of another person.

Furthermore, the risk of *profiling* is significantly high with all the personal data that are stored and communicated. Attendance at sports events or participation in sport challenges together with friend lists allow intuitions about users' health condition and social contacts. Furthermore, new companies such as BioBeats [8] have begun to appear in the market providing predictive insights into individual's health and well-being by tracking data from wearable and smartphone sensors. In particular, they are using users' heart-rate variability (HRV), that is, a measure of how variable heart-rate is over time, as an indicator of stress, potentially revealing something of users' mental health [4].

Regarding the work sector, the risks are significant for some employees in case their wearable's data leak to their future or present employers. It has been reported that obesity-related illnesses cost American businesses $73.1 billion per year in medical expenses and lost productivity [40]. In addition, many debates have been made about pregnancy and hiring discrimination due to employers' intention to avoid maternity leave [15]. Thus one might argue that in the future, wearables and the data that they collect may affect *applicants' acceptance for advertised job positions*. This data may be gathered from a wearable in two example cases. For instance, a wearable may calculate a user's body mass index (BMI) based on weight and height and that data may be used to infer or diagnose obesity [45]. Or, the wearable may predict pregnancy likelihood

based on the reality that resting heart-rates are increased by 30-50% in pregnant women [22].

It has been already reported [37] that companies around the world are analysing applicants' profile on OSNs. This is an act that it is in accordance with the law in the US and in most of the EU member states under certain circumstances. Hence, the enrichment of a user's personal profile with information gathered by their wearable is enabling the human resources sector to obtain more information with higher precision concerning applicants or employees lives.

Also, the list of personal goals and the sport performances logs can raise privacy concerns by revealing personal interests and the health condition of an individual. As stated in [40], these factors can lead to *manipulative marketing* as some individuals will be offered bargains or discounts, whereas others might be given less favourable treatment as they may have a low lifetime-revenue potential. Also, users may experience increased yearly premiums for their health insurance in case the prospect of suffering from an illness is characterised considerably high. IoT devices in general, and in particular wearable fitness-trackers, might be used for providing *insights for insurance companies* that are trying to create more detailed risk profiles of their clients based on their behaviour [43, 51].

Special programmes that offer clients significant discounts for purchasing expensive wearables and rewards for tracking their activity have already made their appearance in the market [58]. However, there has been no holistic, detailed approach to the circumstance as only the positive rewarding consequences have been underlined and no attention has been paid to the negative ones. The reality is that discounts can quickly become surcharges following clients' daily routine and companies' risk-averse policy.

Finally, we have underlined the important risk of *identity theft*. Researchers have underlined the possibility to infer the social security number (SSN) from individuals' personal information, that is, their date and state of birth, in particular [1]. Furthermore, studies [59] suggest that personally identifiable information can be used for targeted online password guessing as users tend to utilise this kind of information for the creation of their credentials.

This completes our brief description of the tool and how it could support users. As we observed different identity attributes known a priori can lead to similar derivations, while there is also the case of multiple attributes being necessary to produce just one inferred element. Certainly, the greater the number of target identity attributes required to reach an inferred element and the greater the uncertainty of their entry by the user is, the less probability for a risk to rise exists. Conversely, more reliable derivatives are produced when an inferred element can be reached from multiple sources, where alternative choices can be used in the absence of another or as a confirmation or comparative measure.

4 USER-BASED STUDY

The development of our tool was followed by an initial user-based study. The purpose of this study was to test the utility of the tool. Firstly, we examined users' awareness of how their identity might be exposed when they engage with wearable IoT devices and OSNs. This allowed us to understand their basic knowledge before engaging with the tool. Secondly, we introduced participants to the tool and asked for their opinions on how useful it could be at gaining a better understanding of the privacy risks. In this section, we present the methodology that we have applied and the findings from this work.

4.1 Methodology

Our empirical data stems from the thematic analysis of semi-structured interviews with a sample of eight participants. Interviewees were recruited individually though invitations, flyers, advertisements on social media and by word-of-mouth. There were no criteria for inclusion other than that all the participants were expected to be owners of wearable IoT devices which were used regularly, either for their work or for their pleasure and convenience. They were also expected to have some social media presence, given that we were looking to correlate data from social media and wearables in our tool. The main motivation was to investigate the general public's awareness of online privacy risks, hence for our sample we excluded people with background in security that could introduce a bias in our results.

Our sample contained four females and four males ranged in age from 25 to 40, the majority of whom were based in the UK. Their educational backgrounds varied from first degree to doctorate and their occupations included postgraduate students, data scientists and university officials. As dictated by our selection criteria, all of them were using various types of fitness-trackers such as Fitbit Charge 2, Polar V800, Polar M400, Apple Watch (1st and 2nd generation) and Suunto Ambit, which provided a diverse set of user experiences.

A Central University Research Ethics Committee approval was obtained prior to the beginning of data collection. All the interviews were conducted during June 2017 and performed in person or over Skype. They lasted between 30 and 45 minutes and they were audio-recorded with the participants' permission. In the course of the study sessions participants elaborated on their risk perception while using their fitness-tracker and their apprehension of the "quantified self" system, in general. They also listed the personal information that they are happy to share on OSNs or store on their wearable IoT device, or else deliberately hide, stating the reason that explains their decision. Reflecting on their responses and utilising our identity tool, we presented them with the potential risks that they may be subject to by using their wearable, and we observed their emotional reactions. Finally, we discussed the countermeasures that they were willing to take soon after realising the possibility of their identity being exposed and their privacy being compromised.

To analyse our data, we employed a thematic analysis approach [9]. This qualitative analytic method when simplified, consists of identifying codes and introducing themes among the collected data. Codes help to the categorisation of the gathered sample into meaningful groups by highlighting interesting semantic or latent content. Subsequently, themes are acting as umbrella terms for certain codes [50] by capturing important meaning within the data in relation to the research question. The following subsection reports our identified themes.

4.2 Findings and Discussion

Prior to our discussion, the majority of participants had paid little attention to the risks that might occur as a result of the usage of their wearable device. We found that several different factors have given them confidence that their privacy is not at risk. One of them was the options available on online sites that provide them with the possibility to preserve their privacy by selecting with whom they share their data. Another factor was the explicit questions throughout the signing up process that ask for their consent in order for their data to be shared with third parties. Also, the trust that such device companies have built throughout the years in the market appeared to have the same impact. Interestingly, one participant reported that the amount of data collected from these devices is insignificant compared to the immense volume of data that are produced for each individual in our big data era. This in some ways suggests that this risk vector might be of minor importance to some. He stated:

> *There is just a massive amount of data out there and the information that would come from my device would be just a drop in the ocean.*

A minority of the participants indicated that they have connected their wearables with other OSNs such as Facebook or linked them with other fitness applications such as Strava. From their responses it was deduced that they tend to separate their fitness activity from their online social life. As for wearable dashboard sites that offer OSN features, interviewees mentioned that they use them mainly to keep a record of their physical performance and not to interact with other users. In that sense, two participants expressed the desire for software that could be installed locally on their personal computers and help them analyse their fitness data. This would be instead of them being obliged to use the online dashboard site that is provided by the company of their wearable. As noted by one of the two:

> *I would have preferred the software to be just on my laptop because I just put the data on this website so as to have a record of the exercise I have done, for example. I do not really care about sharing this kind of stuff which is the reason why I am not on Strava.*

A recurrent theme in the interviews was the participants' attitude that their health data are less valuable than their financial details to cyber criminals. In addition, the interviewees argued that it seemed very difficult their information to reach third parties that could use it for harm in case of a security breach. An apt quote was:

> *In my mind I think, well if you had my bank information what damage could you do to me? You could steal my money. If you had my health information data, let's say, if you knew my heart rate, what could you do to me? It seems there is less risk in this occasion.*

In reality however, it is reported [55] that the physical fitness information that is stored on wearables is worth ten times that of a credit card on the black market. The personal nature of this kind of data, increase both their value and the magnitude of their exchange between different illegal parties [36].

An important issue that emerged from the analytic process was interviewees' inability to associate themselves with the risk that might occur in cyberspace, given that they were not aware of similar incidents that have happened to people they knew. This can be related to the ineffective information that is communicated by security incident notification mechanisms [29], that leave the victims of data breaches among the last ones to learn about incidents affecting them. This oblivious approach diminishes the attention that users are paying to protect their privacy in cyberspace as they believe that incidents like these are targeting special users and not users such as themselves. A participant stated:

> *I feel the risk is small, we always talk about the possibility of these security breaches to happen but I do not know anyone who has ever experienced something like that.*

Almost two-thirds of the participants stated that the way their data are stored and whether companies take actions to maintain anonymity or not, is unclear to them. In addition, over half of those interviewed highlighted that they were feeling a little lost concerning the massive amount of measurements that are happening in the background simultaneously. They also expressed concerns that there might be more data collected than they are aware of. Something like that could be possible either by the use of unlisted sensors on the devices [26] or by the application of data-mining techniques where other information could be accurately inferred by data provided initially, such as in our tool. This is summarised:

> *There are so many parameters and things that you just get overwhelmed by the amount of what the wearable can do and measure.*

Of the study population, the minority of participants reported that they have skimmed through the privacy terms and conditions when signing up their device. Several issues were identified as the main reasons that dissuade them from devoting the time needed to read the provided documentation. The participants appeared to be negatively influenced by the use of unfriendly language with many legal terms and the lack of consideration of how private all this collected information is. Furthermore, this proves already documented issues [31] in relation to the great effort that users have to make to interpret the privacy policies on different websites and define if they are in accordance with their privacy preferences. One participant expressed this concern as follows:

> *No, I did not read the terms and conditions, it's in legalese anyway so you are not really expected to read it unless you hire a lawyer who will go through these sixty pages or whatever, it's not practical really.*

A number of the participants stated that the considerable amount of money that needs to be spent on purchasing such devices is also crucial. Hence, this significant investment leaves little space to decline the use of the device or return it due to concerns that occur after reading the privacy policies. Finally, the majority of the participants commented that they would feel more secure in case the privacy terms and conditions were the outcome of the collaboration between the government and the wearables companies. They suggested that in such a case the document delivered would be more trustworthy as criminal liability will be attributed whenever users' privacy would somehow be violated.

Concerning the data on their wearables, all the interviewees reported that they have entered their age/birthday, height, weight and gender as those are prerequisites for other data to be calculated by the device such as the calories that they have burnt. The fact that they wanted the resulted measurements to be as accurate as possible made them not to lie about the information they provided. Some of the participants reported that they also added optional information such as their daily diet, led by their enthusiasm to make the most out of all the built-in capabilities of their tracker. Similarly, others stated that they have entered more detailed information related to their health status, like allergies for example, in order to instruct other people on how to help them in case an anaphylactic shock occurs to them. They noted:

> *Well, you are buying the device for tracking stuff so the tricky thing about that is that if you don't insert the appropriate information you are not going to have accurate measurements.*

When participants were presented with their respective risks that we identified with the aid of our tool, they found the risks presented as credible and intriguing. We observed that the participants who claimed to mind their privacy and have considered the first level of extracted risks such as the one of *stalking*. However, they were indeed surprised with the more complexly inferred ones such as the possibility of extracting their Social Security Number from their birthday and their birthplace [1]. Even the interviewees who were somewhat sceptical about the actual risks (because they argued that these risks existed in the past prior to the era of IoT) recognised that the technology made the ease of these attacks considerably higher. One participant stated:

> *I had a rough idea, I knew it to a certain extent but I had not put much thought to the deep network of the risks and how these risks can really escalate when you connect one risk to another.*

Our tool received positive feedback by the overwhelming majority of the participants and they stated that they would continue to use it, and suggest it to others, if it was publicly available. We found that even the individuals who were considering that there might be risks while engaging with wearables did not have a clear picture of the risks involved. They reported that our tool with its illustration where the user can observe the data propagation and how this can be maliciously used, made the unspecified risks more tangible. They also stated that it seemed interesting to have a tool that interprets information and shows risks caused by multiple different online sources instead of only one. As summarised by a participant:

> *This tool tells you that if you share this information, this is where it can go and what else could be inferred from that. Seeing this sort of network is quite interesting.*

In addition, they reported that both the tool illustration and the mitigation techniques proposed for each risk could be helpful for the users. Thus, they could still store their data on their wearable but also be more conscious about what they do, both by specifying who can have access to them or by reviewing the information they share on other sites. Hence, they could achieve their privacy without exposing their identity while benefiting from all the functionalities of their devices.

5 CONCLUSION AND FUTURE WORK

In this paper, we have presented our identity-exposure tool that seeks to determine the leakage of information related to users' identity resulting from their engagement with wearable IoT devices, in particular fitness-trackers and OSNs, in parallel. We have demonstrated that the plausible risks are essential and must be taken into consideration when users interact with such devices and engage with OSNs. The qualitative analysis that we performed showed that users' awareness, concerning the risks encountered, can be characterised as low and that the usage of an interactive tool such as the one we have developed could help them identify the risks better and adopt proposed mitigation techniques to safeguard their privacy.

We consider this work somewhat to be an initial step of a broader study that tries to identify and raise awareness about the privacy issues arising in the emerging IoT era. As a following step, we are planning to enrich our tool by identifying further inferences for the data points already presented. We are also working towards expanding the scope of the tool with a view to incorporating information from other IoT domains such as Building & Home Automation and Smart Cities, which are also expected to host significant private data of the users.

As already presented, the tool is currently stating the postulations that are identified by us, or proposed in the literature, in order to assess individuals' online digital footprints. Our ultimate objective is to integrate the different techniques into the tool, so that the inferred elements can be calculated automatically. Thus, an inference categorisation could be introduced based on the accuracy and ease of their extraction. Also, in such a way we could examine the deterioration of quality caused by error propagation in derivations that demand multi-level chain of extractions. These live demonstrations are expected to help users attest better the risks encountered and regain control of their data [20]. It is important that this enhanced identity-exposure tool is going to be used responsibly as we acknowledge the related privacy risks that arise from its use.

For now the tool can be launched locally on a user's computer. On-going work is aiming at enabling its access through the web and developing a mobile application that users could use on their mobile phone. As a result, the tool will be able to be reached by a greater range of people allowing us to launch user-based studies on a larger group of individuals. We are also particularly keen on exploring how other interested stakeholders perceive our tool, the risks it identifies and the correlated illustration of the inferred elements. Hence, we are considering conducting interviews with executives from companies that provide wearables in the market. We are positive that our tool could help them to be better informed about the potential risks that their devices can possibly cause and take countermeasures against them, acquiring thus the trust of their customers.

Finally, ongoing work is also focusing on surveying the ethical considerations that are caused by the possibility of deducing successfully significant information about users' identity in this new

heavily connected world. Among the issues that are under investigation are the discrimination effects of users' decision to remain unconnected and the questions raised from the existence of such accumulated superabundant information that may be used either by the government or by companies to place individuals under surveillance [2].

ACKNOWLEDGMENTS

We would wish to thank the UK EPSRC who have funded this research through a partial PhD studentship in Cyber Security for EU Candidates.

REFERENCES

[1] Alessandro Acquisti and Ralph Gross. 2009. Predicting social security numbers from public data. *Proceedings of the National academy of sciences* 106, 27 (2009), 10975–10980.
[2] Samantha Adams, Nadezhda Purtova, and Ronald Leenes. 2016. Under Observation: The Interplay Between eHealth and Surveillance. (2016).
[3] Orlando Arias, Jacob Wurm, Khoa Hoang, and Yier Jin. 2015. Privacy and security in internet of things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems* 1, 2 (2015), 99–109.
[4] American Psychological Association et al. 2012. Stress in America: Our health at risk. *Washington DC, American Psychological Association* (2012).
[5] Mario Ballano Barcena and Candid Wueest. 2015. Insecurity in the Internet of Things. *Security Response, Symantec* (2015).
[6] Mario Ballano Barcena, Candid Wueest, and Hon Lau. 2014. How safe is your quantified self. *Symantech: Mountain View, CA, USA* (2014).
[7] Leyla Bilge, Thorsten Strufe, Davide Balzarotti, and Engin Kirda. 2009. All your contacts are belong to us: automated identity theft attacks on social networks. In *Proceedings of the 18th international conference on World wide web*. ACM, 551–560.
[8] BioBeats. 2016. http://biobeats.com. (2016). [Online; accessed 15-July-2017].
[9] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.
[10] Sandra Carpenter, Feng Zhu, and Swapna Kolimi. 2014. Reducing online identity disclosure using warnings. *Applied ergonomics* 45, 5 (2014), 1337–1342.
[11] Dipl-Inform Eric Clausing, Michael Schiefer, Ulf Lösche, and Dipl-Ing Maik Morgenstern. 2015. Security Evaluation of nine Fitness Trackers. *The Independent IT-Security Institute* (2015).
[12] Sadie Creese, Thomas Gibson-Robinson, Michael Goldsmith, Duncan Hodges, Dee Kim, Oriana Love, Jason RC Nurse, Bill Pike, and Jean Scholtz. 2013. Tools for understanding identity. In *Technologies for Homeland Security (HST), 2013 IEEE International Conference on*. IEEE, 558–563.
[13] Sadie Creese, Michael Goldsmith, Jason RC Nurse, and Elizabeth Phillips. 2012. A data-reachability model for elucidating privacy and security risks related to the use of online social networks. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*. IEEE, 1124–1131.
[14] Mathieu Cunche, Mohamed Ali Kaafar, and Roksana Boreli. 2012. I know who you will meet this evening! linking wireless devices using wi-fi probe requests. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*. IEEE, 1–9.
[15] April L Dowler. 1980. Pregnancy and Hiring Discrimination. *W. Va. L. Rev.* 83 (1980), 537.
[16] Lia Emanuel, Chris Bevan, and Duncan Hodges. 2013. What does your profile really say about you?: privacy warning systems and self-disclosure in online social network spaces. In *CHI'13 Extended Abstracts on Human Factors in Computing Systems*. ACM, 799–804.
[17] Hewlett Packard Enterprise. 2015. Internet of things research study. *Internet of Things Research Study* (2015).
[18] Fitbit. 2017. Fitbit Charge 2. https://www.fitbit.com/uk/charge2. (2017). [Online; accessed 29-July-2017].
[19] Office for Civil Rights (OCR) and U.S. Federal Trade Commission (FTC). 2016. Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA. *U.S. Department of Health and Human Services Report* (2016).
[20] Sarah Gordon. 2017. Our personal data are precious - we must take back control. *Financial Times* (2017). https://www.ft.com/content/3278e6dc-67af-11e7-9a66-93fb352ba1fe [Online; accessed 19-July-2017].
[21] Sarthak Grover and Nick Feamster. 2016. The Internet of Unpatched Things. *Proc. FTC PrivacyCon* (2016).
[22] Haywood L. Brown. 2016. Physical Changes During Pregnancy. http://www.merckmanuals.com/home/women-s-health-issues/normal-pregnancy/physical-changes-during-pregnancy. (2016). [Online; accessed 20-Jun-2017].
[23] Andrew Hilts, Christopher Parsons, and Jeffrey Knockel. 2016. Every Step You Fake - A Comparative Analysis of Fitness Tracker Privacy and Security. *Open Effect Report* (2016).
[24] Christina Hochleitner, Cornelia Graf, Peter Wolkerstorfer, and Manfred Tscheligi. 2012. uTRUSTit–Usable Trust in the Internet of Things. In *International Conference on Trust, Privacy and Security in Digital Business*. Springer, 220–221.
[25] Duncan Hodges, Sadie Creese, and Michael Goldsmith. 2012. A model for identity in the cyber and natural universes. In *Intelligence and Security Informatics Conference (EISIC), 2012 European*. IEEE, 115–122.
[26] iFixit. 2015. Apple Watch Teardown. *iFixit* (2015). https://www.ifixit.com/Teardown/Apple+Watch+Teardown/40655?revisionid=HEAD [Online; accessed 15-July-2017].
[27] Andreas Illmer. 2016. Social Media: A hunting ground for cybercriminals. *BBC* (2016). http://www.bbc.co.uk/news/business-36854285 [Online; accessed 15-July-2017].
[28] International Data Corporation (IDC). 2017. Worldwide Quarterly Wearable Device Tracker. http://www.idc.com/getdoc.jsp?containerId=prUS42342317. (2017). [Online; accessed 30-May-2017].
[29] Erka Koivunen. 2010. "Why Wasn't I Notified?": Information Security Incident Reporting Demystified. In *Nordic Conference on Secure IT Systems*. Springer, 55–70.
[30] Hanna Krasnova, Oliver Günther, Sarah Spiekermann, and Ksenia Koroleva. 2009. Privacy concerns and identity in online social networks. *Identity in the Information Society* 2, 1 (2009), 39–63.
[31] Stephen E Levy and Carl Gutwin. 2005. Improving understanding of website privacy policies with fine-grained policy anchors. In *Proceedings of the 14th International Conference on World Wide Web*. ACM, 480–488.
[32] Ilaria Liccardi, Alfie Abdul-Rahman, and Min Chen. 2016. I know where you live: Inferring details of people's lives by visualizing publicly shared location data. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 1–12.
[33] Sam Lucero. 2016. *IoT platforms: enabling the Internet of Things*. Technical Report. IHS Technology.
[34] Finn Lutzow-Holm Myrstad, Gro Mette Moen, Mathias Stang, Siv Elin Anestad, Gyrid Giaever, Oyvind Herseth Kaldestad, and Helene Storstrom. 2016. APPFAIL Threats to Consumers in Mobile Apps. *Forbrukerradet Report* (2016).
[35] David Lyon. 2014. Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society* 1, 2 (2014), 2053951714541861.
[36] Teena Maddox. 2015. The dark side of wearables: How they're secretly jeopardizing your security and privacy. *TechRepublic* (2015). [Online; accessed 15-July-2017].
[37] Jonathan Margolis. 2017. Be careful with social media - employers are watching. *Financial Times* (2017). https://www.ft.com/content/5b8bb3b0-6aca-11e7-b9c7-15af748b60d0 [Online; accessed 18-July-2017].
[38] Jane McCallion. 2014. Fitness trackers could pose stalking risk. *PC Pro* (2014). http://www.alphr.com/fitness-trackers/24999/fitness-trackers-could-pose-stalking-risk [Online; accessed 15-July-2017].
[39] George R Milne and Mary J Culnan. 2004. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing* 18, 3 (2004), 15–29.
[40] Kathryn Montgomery, Jeff Cester, and Katharina Kopp. 2016. Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection. *Centre for Digital Democracy Report* (2016).
[41] Jason RC Nurse, Arnau Erola, Thomas Gibson-Robinson, Michael Goldsmith, and Sadie Creese. 2016. Analytics for characterising and measuring the naturalness of online personae. *Security Informatics* 5, 1 (2016), 3.
[42] Jason RC Nurse, Jess Pumphrey, Thomas Gibson-Robinson, Michael Goldsmith, and Sadie Creese. 2014. Inferring social relationships from technology-level device connections. In *Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on*. IEEE, 40–47.
[43] Parmy Olson. 2014. Wearable Tech Is Plugging Into Health Insurance. *Forbes* (2014). https://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/#660a2f1d18bd [Online; accessed 15-July-2017].
[44] Charith Perera, Rajiv Ranjan, Lizhe Wang, Samee U Khan, and Albert Y Zomaya. 2015. Big data privacy in the internet of things era. *IT Professional* 17, 3 (2015), 32–39.
[45] F Xavier Pi-Sunyer, Diane M Becker, C Bouchard, RA Carleton, GA Colditz, WH Dietz, JP Foreyt, RJ Garrison, SM Grundy, BC Hansen, et al. 1998. Clinical guidelines on the identification, evaluation, and treatment of overweight and obesity in adults. *American Journal of Clinical Nutrition* 68, 4 (1998), 899–917.
[46] Polar. 2017. Polar V800. https://www.polar.com/uk-en/products/pro/V800. (2017). [Online; accessed 29-April-2017].
[47] Antoine Pultier, Nicolas Harrand, and Petter Bae Brandtzaeg. 2016. Privacy in Mobile Apps. *SINTEF Report* (2016).
[48] Mahmudur Rahman, Bogdan Carbunar, and Madhusudan Banik. 2013. Fit and vulnerable: Attacks and defenses for a health monitoring device. *arXiv preprint*

arXiv:1304.5672 (2013).

[49] Jakob Rieck. 2016. Attacks on Fitness Trackers Revisited: A Case-Study of Unfit Firmware Security. *arXiv preprint arXiv:1604.03313* (2016).

[50] Ramzi Rizk, Daniel Marx, Matthias Schrepfer, Janina Zimmerman, and Oliver Guenther. 2009. Media coverage of online social network privacy issues in Germany: A thematic analysis. *AMCIS 2009 Proceedings* (2009), 342.

[51] Jathan Sadowski. 2016. Alarmed by Admiral's data grab? Wait until insurers can see the contents of your fridge. *The Guardian* (2016). https://www.theguardian.com/technology/2016/nov/02/admiral-facebook-data-insurers-internet-of-things [Online; accessed 15-July-2017].

[52] Ignacio Sanchez, Riccardo Satta, Igor Nai Fovino, Gianmarco Baldini, Gary Steri, David Shaw, and Andrea Ciardulli. 2014. Privacy leakages in Smart Home wireless technologies. In *Security Technology (ICCST), 2014 International Carnahan Conference on*. IEEE, 1–6.

[53] Taylor Jackson Scott, Katie Kuksenok, Daniel Perry, Michael Brooks, Ona Anicello, and Cecilia Aragon. 2012. Adapting grounded theory to construct a taxonomy of affect in collaborative online chat. In *Proceedings of the 30th ACM international conference on Design of communication*. ACM, 197–204.

[54] Fuming Shih, Ilaria Liccardi, and Daniel Weitzner. 2015. Privacy tipping points in smartphones privacy preferences. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 807–816.

[55] Aatif Sulleyman. 2017. NHS Cyber Attack: Why Stolen Medical Information Is So Much More Valuable Than Financial Data. *Independent* (2017). [Online; accessed 15-July-2017].

[56] Suunto. 2017. Suunto Ambit. http://www.suunto.com/en-GB/Products/sports-watches/Suunto-Ambit/Suunto-Ambit-Black/. (2017). [Online; accessed 29-August-2017].

[57] Melanie Swan. 2012. Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. *Journal of Sensor and Actuator Networks* 1, 3 (2012), 217–253.

[58] Vitality. 2017. Apple Watch with Vitality health and life insurance. https://www.vitality.co.uk/rewards/partners/active-rewards/apple-watch/. (2017). [Online; accessed 15-July-2017].

[59] Ding Wang, Zijian Zhang, Ping Wang, Jeff Yan, and Xinyi Huang. 2016. Targeted online password guessing: An underestimated threat. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1242–1254.

[60] Bruce D Weinberg, George R Milne, Yana G Andonova, and Fatima M Hajjat. 2015. Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons* 58, 6 (2015), 615–624.

[61] Meredydd Williams and Jason RC Nurse. 2016. Optional data disclosure and the online privacy paradox: A UK perspective. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 186–197.

[62] Meredydd Williams, Jason RC Nurse, and Sadie Creese. 2016. The perfect storm: The privacy paradox and the Internet-of-Things. In *Availability, Reliability and Security (ARES), 2016 11th International Conference on*. IEEE, 644–652.

[63] Carla Willig. 2013. *Introducing qualitative research in psychology*. McGraw-Hill Education (UK).

[64] Wei Zhou and Selwyn Piramuthu. 2014. Security/privacy of wearable fitness tracking IoT devices. In *Information Systems and Technologies (CISTI), 2014 9th Iberian Conference on*. IEEE, 1–5.

[65] Feng Zhu, Sandra Carpenter, and Ajinkya Kulkarni. 2012. Understanding identity exposure in pervasive computing environments. *Pervasive and Mobile Computing* 8, 5 (2012), 777–794.