A STUDY ON SITUATIONAL AWARENESS SECURITY AND PRIVACY OF WEARABLE HEALTH MONITORING DEVICES

Xavier Bellekens[1], Kamila Nieradzinska[2], Alexandra Bellekens[3], Preetila Seeam[4], Andrew Hamilton[2], Amar Seeam[5]

[1] Abertay Dundee University, United Kingdom, Scotland
[2] University of Strathclyde, United Kingdom, Scotland
[3] Université Catholique de Louvain, Belgium
[4] Aberystwyth University, Mauritius
[5] Middlesex University, Mauritius

ABSTRACT

Situational Awareness provides a user centric approach to security and privacy. The human factor is often recognised as the weakest link in security, therefore situational perception and risk awareness play a leading role in the adoption and implementation of security mechanisms. In this study we assess the understanding of security and privacy of users in possession of wearable devices. The findings demonstrate privacy complacency, as the majority of users trust the application and the wearable device manufacturer. Moreover the survey findings demonstrate a lack of understanding of security and privacy by the sample population. Finally the theoretical implications of the findings are discussed.

Keyword: Situational Awareness, eHealth, Wearables, Security, Privacy,

1 INTRODUCTION

The intrinsic convenience of wearable devices such as dedicated health monitors, fitness bands and smart watches has accelerated the market for personal health monitoring, wearable gamification and the mobile market. It is estimated that 102 million fitness tracking units will be shipped by the end of 2016, an increase of 29 percent over late 2015, that 213 million wearable monitoring devices will be shipped by 2020 (Musil, 2016) and that 13.45 million remote cardiac monitoring units will be in use by 2018 (Statista, 2016).

Whilst wearable technologies have allowed users to monitor their every move, physical condition, predict their physical activities and much more, Wang *et al.* have demonstrated the dangers of wearable technologies. Through their study, they demonstrated that fitness trackers and smart watches could also reveal the PIN code by using the embedded accelerometer to derive the hand movement over a keypad (Wang *et al.*, 2016).

Wearable technology is also becoming part of our economy backbone by allowing smart payments (Apple, 2016), a digital technology that is becoming a critical resource used daily. With the growing dependency on complex architectures, the need for situational awareness has become primordial. Essentially, understanding the context, the environment, the threats, and being able to predict problems has become fundamental. Endsley defines situational awareness as "*the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.*" (M.R. Endsley, 1998.; Mica R. Endsley, 1995). This definition will be central in the development of this study.

This paper contributes to the field of cyber-situational awareness as follows: A comprehensive analysis of the cyber-security and privacy awareness of participants from different countries and backgrounds with regards to health monitoring devices is presented. A discussion of discuss the understanding of cyber-security and privacy of the participants is detailed, highlighting the grey area between both security and privacy terms and their implication in real life, and finally conclusions of the results obtained are provided.

Overall the results indicate a poor understanding and comprehension of security and privacy, not only confined to wearable devices. The population also demonstrated a lack of threat perception and meaning.

The study calls for an additional effort to provide tighter regulation for sensitive data gathered by health monitoring devices, adequate information sharing and data restriction as well as providing means to increase the security and privacy awareness of users, and manufacturers by creating a user privacy centric methodology.

The remainder of this paper is organised as follows; Section 2 provides an overview of related work. Section 3 describes the methodology used in the study, the data collection and the demographics of the sample population. Section 4 provides a descriptive statistics analysis of the results obtained through the survey, whilst Section 5 highlights the limitation of the survey. Finally Section 6 presents the discussion and conclusion.

2 RELATED WORK

Situational awareness and wearable devices have been well studied in literature. However, the majority of the relevant work has been focusing on the technical aspects of security and privacy rather than providing a user centric analysis.

In light of cyber-security and privacy on health devices Raychaudhuri *et al.* highlighted the challenges of electronic data privacy and eHealth privacy. The research outcomes provided a survey of published work describing the challenges encountered by medical and technical professionals in order to implement a modular framework. The authors also presented different solutions preserving the privacy of users. The survey was focused on the surveillance of infectious diseases such as HIV. The authors highlighted the complexity of privacy and security when monitoring health due to the multiple technologies and policies involved.

Di Pietro *et al.* provided an overview of the security and privacy issues related to handheld and wearable wireless devices. Their study highlighted the challenges to provide security and privacy to monitoring health devices and discussed two possible scenarios in order to increase the security and privacy of the devices. The study highlighted the complexity of implementing these solutions and called for better solution in the future (Di Pietro & Mancini, 2003).

Similarly to this study, Lakkaraju *et al.* presented a tool called NVisionIP allowing the improvement of the situational awareness of security analysts and security researchers facing data breaches. The tool focuses on the visualization of class-B networks and presents potential attacks in a visual fashion for clear identification (Lakkaraju *et al.*, 2004).

Moreover a study conducted in (Burghardt *et al.* , 2009) presented results on the user preferences for privacy mechanism in location based devices. The authors demonstrated a lack of user awareness towards the possible preferences. The authors provided the participants with different privacy policies and studied their "informedness" / awareness as well as quantified the mental effort required in order to increase the situational awareness of the participants. The studies demonstrated that users often have privacy concerns but were unable to understand the privacy settings due to a lack of usability and clear instructions.

3 METHODOLOGY

To assess the security and privacy awareness of wearable devices, a survey was conducted from October 2015 to February 2016. This section describes the survey methodology and the gathering of data. Details about the survey are also provided in order to ensure the validity and significance of the results presented. The survey was presented to the participants as "cyber security and privacy" survey, defining the context of the questions beforehand.

3.1 Data Collection and Demographics

The questionnaire used for in this study was designed for a web-based English interview of the participants. A representative sample (N=273) of users using wearable devices to monitor their health has been used.

Participants from different backgrounds were selected. The students are represented through three different Universities in three different countries (Belgium, United Kingdom, and Mauritius). Moreover the questionnaire was also available for Amazon Mechanical Turk where participants based in the United States were asked to answer the questions in 15 minutes and offered a $2 reward upon completion.

The MTurk participants were master workers screened by Amazon. This ensures the reliability of their answers. The results provided by the master workers were analysed separately and all incomplete or random questionnaires were discarded and the offending MTurk worker reported to Amazon.

The professional participants have been working for at least one year in the field of telecommunications, information technology, web development or information security & privacy.

The data collection methodology satisfies the randomness and reliability of answers as the participants were approached at random through the Amazon MTurk service and the students and professional participants were selected at random and asked if they wished to participate in the survey.

3.2 Demographics

Table 1 provides a summary of the participant's background, age and gender.

TABLE 1 PARTICIPANTS

	Students	MTurk	Professionals
Participants	**110**	**148**	**15**
Male	**72%**	**51%**	**86.7%**
Female	**28%**	**49%**	**13.3%**
Age Range	**17-36**	**21-69**	**24-53**

All the participants were asked the same questions regarding privacy and security of wearables devices independently of their understanding of security and privacy, information technology (IT) knowledge or their possession of one or more wearable device.

TABLE 2 INFORMATION TECHNOLOGY KNOWLEDGE OF THE PARTICIPANTS AND POSSESSION OF WEARABLE DEVICES.

	Students	MTurk	Professionnals
IT Experience	**76%**	**59%**	**100%**
One or more Wearable	**53%**	**46%**	**24%**

The sample population in this survey demonstrates that 130 users possessed one or more wearable device. 93.7% users reported that they were not security savvy users, 20.51% reported that they had close to no experience in IT, whilst 74.35% reported moderate IT skills and 5.12% reported excellent IT skills. Table 2 shows the IT experience of the participants as well as the percentage of users possessing one or more wearable devices.

TABLE 3 EDUCATION

	High School	Undergraduate (Bachelor)	Graduate (Master)	PhD/MD/DSc
Education level	**4.39 %**	**73.99%**	**18.31%**	**3.29%**

Amongst the participants 100% were aware of computer malware and viruses, however, only 63% had been confronted by malicious software in the past on a personal or work computer. Finally, 29.6% of the users possessing one or more wearable device admitted having misplaced their device in the past.

4 DESCRIPTIVE STATISTICS

This section describes the findings obtained through the survey. The results are presented as a percentage, summarising the responses and results gathered. Through this section we highlight the lack of security and privacy awareness of the participants. The findings are compared to different theories in the discussion section.

4.1 Cyber-Security and Privacy Awareness

The security and privacy awareness of the participants was gauged by providing them with different scenarios. The participants were asked to classify them as being a potential security or privacy threat or neither. As shown in Figure 1, 100% of the participants classified all the scenarios as either a security or a privacy threat.

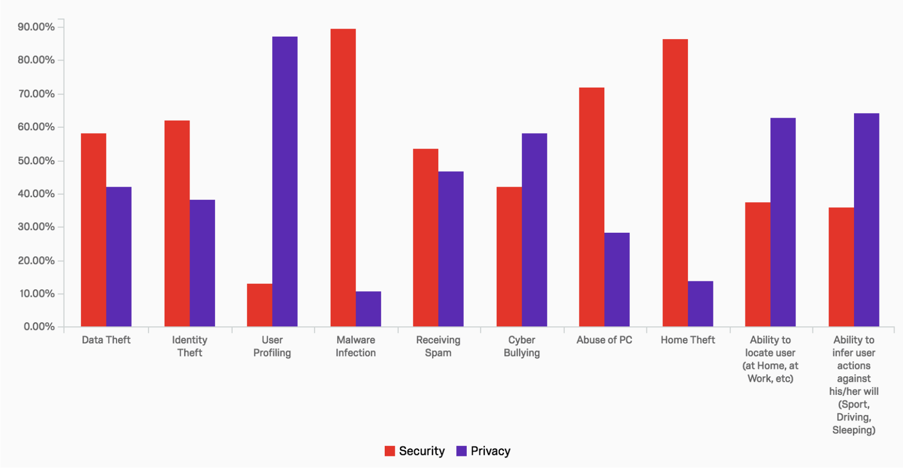


FIGURE 1 SECURITY AND PRIVACY EVALUATION

One of the most persistent findings in this survey is that the users are unaware of the boundaries between security and privacy, highlighting a grey area. More specifically *"data theft"* is classified by only 41.98% as a privacy threat. This is similar to the results obtained for the classification of "*identity theft*" where 38.18% of the users classified it as a privacy concern. This finding coincides with previous research in the field demonstrating the close relation between security and privacy in the mind of the public (Belanche *et al.*, 2012) (Gefen *et al.*, 2003).

The results also reveal the overlapping of the cyber and physical world, by demonstrating that 86% of the participants classified *"home theft"* as a security problem. These observations concur with prior research where the boundary between both worlds is vague in the mind of participants. It is speculated that these results are due to the large number of ubiquitous physical objects connected sending private data and interacting between both the cyber and physical worlds at any given point in time.

4.2 Threat Likelihood

The participants were asked to rate different threats by likelihood. The scenario threats described in the survey have been chosen, as they were part of official press and news reports or academic publications.

The majority of users (64.11%) demonstrated a lack of awareness in the presence or absence of cyber bullying. More specifically only 6.11% of the sample population was aware of cyber bullying risk and rated the threat as extremely likely.

These findings correspond to results obtained by prior research in the field of digital privacy, highlighting the poor awareness of the public in cyber bullying and threats faced by children and adults when publicly posting wearable data on social networks (Luxton *et al.* 2012) (Wang *et al.* 2012).

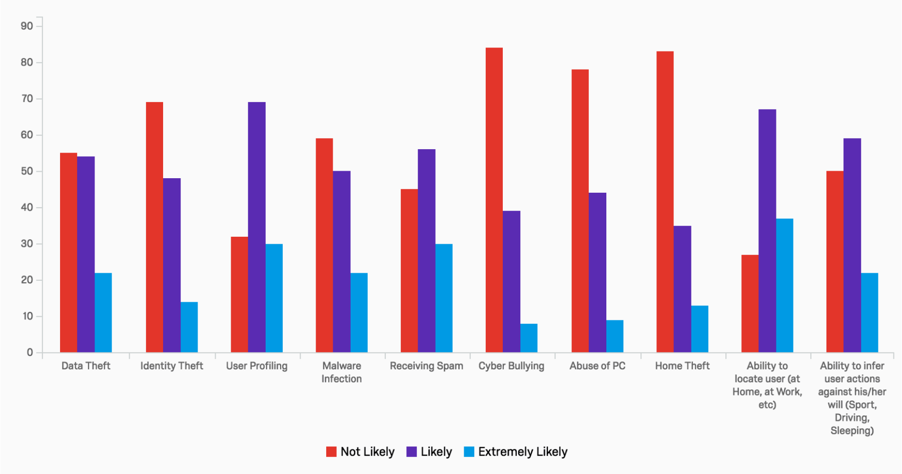


FIGURE 2 THREAT LIKELIHOOD

The participants also underestimate the risk of home theft with 63% being unaware of public data being monitored by thieves on social media in order to infer patterns in sport activities such as dates, times, and duration. Prior results were detailed by (Friedland & Choi, 2011) and (Gan & Jenkins, 2015) demonstrating the risk of sharing private data on social media, with or without consent. These risks were highlighted in prior studies demonstrating poor understanding of "*privacy settings*" by social network users. Madejski *et al.* highlighted that Facebook provided privacy policies based on data type rather than on context. A contradiction with real world scenarios, where context is more important than the type of data shared. In our study, we observed similar behavior from the participants. In real life, participants would not sharing their position publicly. However they are willing to share their location through Facebook posts without amending the privacy settings as the data type of the post feels un-important (Lewis *et al.*, 2008) (Madejski *et al.*, 2011). The sample population was also unaware of risk inferred by geo-location data gathered through a wearable device, or possible exploitation of data obtained through data leaks. Another interesting finding highlighted by our survey is that 97.06% of the participants had never heard of any case of burglary based on social media data or wearable data being shared despites numerous cases being advertised in the news, and by authorities on television and radio shows.

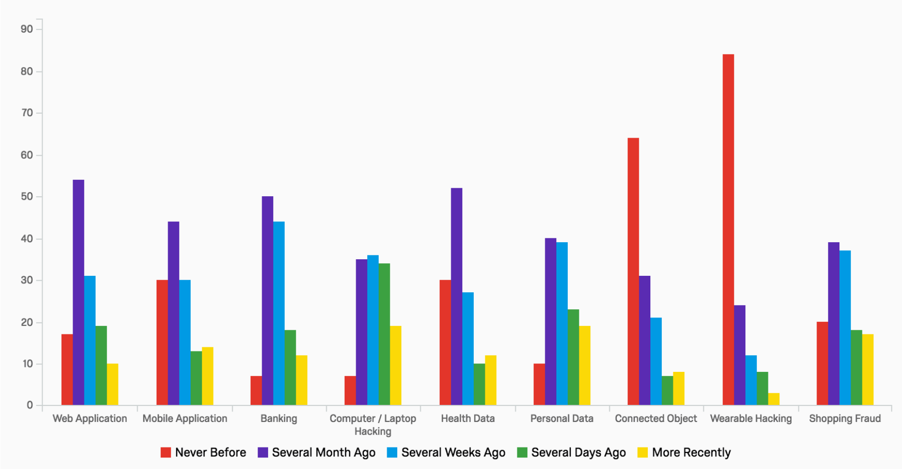


FIGURE 3 THREAT AWARENESS

The sample population was asked to rate their awareness of cyber-security and privacy flaws reported through the_media such as newspapers, the internet or television. 17.94% of the population reported having never heard of web application security flaws, while 74.7% of the population had never heard of wearable security and privacy flaws, and reported not being aware of any security concerns related to wearable devices. 63.7% of the users also reported having never heard of security breaches of internet connected objects such as IP Cameras and baby monitors.

Moreover, 73.2% of the sample population were unaware of the presence or absence of security mechanisms for wearable devices. 95.2% admitted assuming that companies providing the devices and gathering data had an explicit data privacy policy in place. Finally 89% admitted having never read the privacy policies or the amendments made by the company providing the services. These findings indicate that the users regard the wearable device and the company as inherently trusted, regardless of the security and privacy policies in place.

4.4 Risk and Occurrence

The participants were asked to analyse different threats and provide a risk rating as well as a likelihood of occurrence of the threat against one of their wearable devices or wearable accounts in a near future. This rating is based on the participants understanding of security, privacy and threat awareness to wearable devices such as described by Endlsey in (Mica R. Endsley, 1995). The participants rated the threat occurrences from “no risk” to “high risk”.

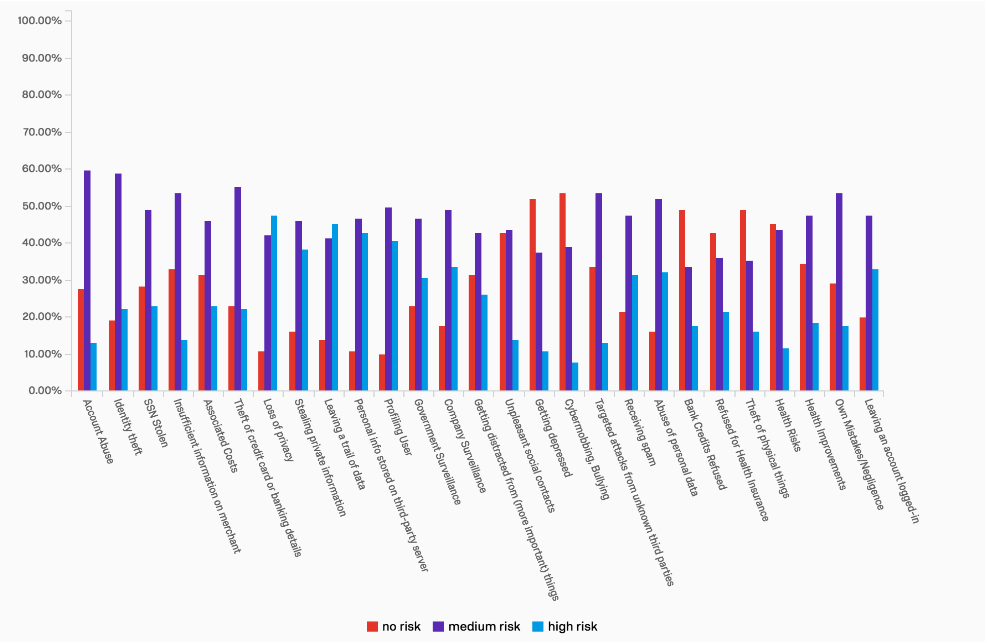


FIGURE 4 RISK EVALUATION AND RATINGS

The results presented by this question reinforced the results obtained in prior questions and strengthened our prior observation. 58.97% believed there was a medium risk their own account would be abused, while 27.83% of the population believed their account was safe. As demonstrated in Figure 4 a majority of participants (60.04%) believed they could not be subject to cyber bullying whilst sharing data on social networks. Moreover 50.91% of the participants believed they would never be refused a mortgage or a credit based on their health data, despite monitoring their health on a daily basis. The survey also demonstrated contradictions between the users, as 48.71% of the population indicated the loss of privacy as a high risk in the near future. This contradiction has been highlighted in (Levin *et al.*, 2008) in relation to social network. Levin *et al.* describe this as “*Network Privacy*”. The Network Privacy describes the accessibility of data. In their work on online social network Levin *et al.* demonstrate that users are concerned about the extent of the dissemination of their personal data, as well as “who knows what”, but are not concerned about posting salacious pictures of themselves. In our study users believe that the “Network Privacy” is limited to themselves (when not sharing the data online) or to their friends when

sharing data on social network. The study demonstrated that the sample population believed wearable manufacturers had privacy policies in place in Figure 4, hence our sample population believes knowing the extent of the dissemination of the data they share, despite not having read the privacy policies established by the service manufacturer or service provider. The contradiction between their fear of loss of privacy and their belief in the fact they would not be refused a mortgage based on their health data in a near future could reflect a lack of understanding of privacy and a delusional understanding of "Network Privacy" as described in (Levin *et al.*, 2008).
The results obtained also demonstrated that self-negligence is not considered as a risk by the majority of the users with only 18.68% of users considering it as a major risk in the future and over 33% of users assessing their negligence as a minor risk.

4.5 Threat Severity

The participants where asked to rate the severity of different types of threats based on personal experience and their awareness of information technology security. For each threat the participants where to give a note between 1 and 10. A rating of 1 represents a low severity threat while a ratings of 10 represents the highest threat severity, hence the most impactful.

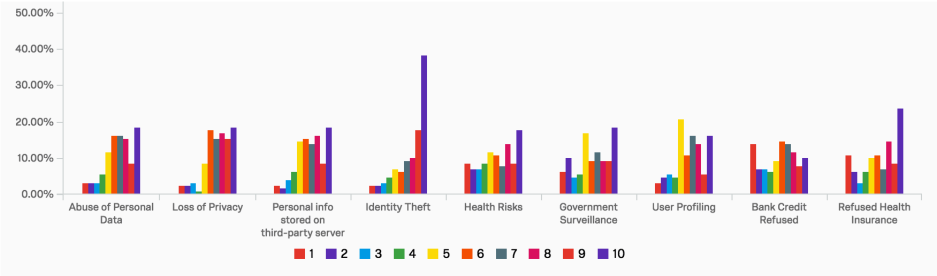


FIGURE 5 THREAT SEVERITY

Figure 5 shows the results obtained through the threat severity question. 38.82% of the sample population identified "Identity Threat" as most impactful threat demonstrating concerns of privacy, while only 19.94% of the population rated personal and health data storage on a third party server as highly impactful. This behavior demonstrates the confidence of the users in the service paid for. This behavior is described in (Thomas & Menon, 2007) and defined as a price expectation. Users demonstrate a security and privacy expectation through the price of the device regardless of the technical components of the service offered. As highlighted in prior question users are reluctant to believe that their health data can or could be used against them in a near future when applying for a mortgage or a credit (Peppet, 2013). Moreover Singer *et al.* advocate in (Singer *et al.*, 2015) for a clear communication to the users on data collected and data being shared with third party, as this is often not clear. Following this study, Heembrock discussed further the risks of wearable technologies in the work place as well as possible third party data sharing and possible re-examination of insurance policies by employers based on data provide by the wearable devices in (Heembrock, 2015). The results provided in Figure 5 demonstrate the misconception and misunderstanding of the situational awareness risks inherent to the use of health monitoring devices by the users.

5 LIMITATIONS

One possible limitation to this study is the sample size of N=273 as well as the population demographics. It may be that awareness differs greatly from country-to-country, as well as continent-to-continent. With only 28 % female participants this study is biased towards male participants. A number of questions were based on self-reported statistics. For example the users were asked to report on their ICT security and privacy expertise. The results were derived from academic sources such as College or University or from industrial sources such as security certifications (Cisco Certified Network Associate (CCNA), EC-Council Certified Ethical Hacker (CEH), etc). This survey did not validate the background of the participants or their level of education. A possible limitation of this survey is that the Amazon MTurck have been paid $2, there may be some bias as studies have demonstrated that paid groups would bias their answers based on the amount of money or attracting a specific demographic as described in (Laurie & Lynn, 2009). However, there were no major statistical differences between the 3 groups.

Another possible limitation of this survey is that both wearable devices and professional health monitoring devices were assessed, such as connected heart and tension monitors. This made the survey cross-platform; hence the survey may be biased due to a high heterogeneity. The policies of each manufacturer and services provider (storage, data collection) are different. Moreover, different devices might have different sharing opportunities (Facebook, Twitter, or their own social network). The security controls of each of the devices might also be different increasing or decreasing the situational awareness of users using a particular type of device or brand. A final possible limitation of this survey is the age bias with a majority of participants being aged between [22-34]. Nevertheless this survey did not focused on the aforementioned details. It however focused on the security and situational awareness of the participants towards wearable health devices, their security and privacy adoption, and understanding, as well as their potential to identify current and future threats. The survey demonstrated the participant's lack of security and privacy understanding, hence highlighted the lack of security and privacy awareness or the ability to detect potential threats due to data sharing, data collection via mobile phone applications, social networks, service providers and, as per Ensley's definition, a poor perception of the different elements in the environment of wearable devices.

6 DISCUSSION AND CONCLUSIONS

The security model adopted for wearable devices delegates the security and privacy directly to the users, allowing them to make critical decisions on the data being shared with the public. However, the study demonstrated that users have an implicit idea of control, which is not true in the majority of cases. While a number of participants demonstrated security and privacy concerns towards data sharing and data storage, this survey demonstrated that the participants often overestimated their choice for each device and underestimated potential threats. This phenomenon has previously been described by Ross et al. and is known as the fundamental attribution error (Ross, 1977). Due to possible cognitive dissonance the survey demonstrate that the sample population often consider their choice of wearable device as the best one on the market, hence as the most secure. This could be classified as an effort justification paradigm, where the users believe they are immune to threats due to their own choices, ignoring external factors (Festinger, 1957, 1964). Furthermore, the participants demonstrated an unrealistic optimism towards future threats, this has been previously described in (Shepperd et al., 2015; Weinstein et al., 1984). Participants misevaluate security and privacy risks linked to wearable devices, data sharing, data mining and data storage by third parties. Following Endlsey's definition of awareness, the participants were unable to perceive current security and privacy threats nor where they able to predict and protect their current situation by improving their security and privacy awareness due to a lack of knowledge, educational resources, and details provided by the service providers or manufacturer on the data collected, shared, and stored.

Our results also indicated an asymmetry in the answers, as users indicated using antivirus software on their computer, however did not demonstrate concern on the security of their wearable devices. As explained in (Harris, 2016), wearable devices have their own operating system and are therefore potentially subject to malware, data loss, etc.

In this paper it has been shown that users are not aware of security and privacy threats against health monitoring devices and that the prevalence of an implicit idea of control is considerably higher than estimated. This survey also demonstrated that users are not aware of the data collection, the data processing, and the data storage process and that the users are unable to formally identify where the data is being stored.

Consideration should be given to increase the awareness of the users on the potential threats of sharing data publicly as well as on the data collection and the data storage implied by the wearable health monitoring devices. It should now be clear that increasing the privacy and security of the devices may reduce the usability of sharing platform such as social networks.

Another consideration to improve the situation is to strengthen the regulation on data collection and data storage as well as through user education as suggest previously in (Bellekens et al., 2016). More specifically in the case of situational awareness for wearable health devices, this study calls for an additional effort to provide a user-centric situational awareness framework, allowing the users to increase their awareness of potential threats.

The focuse of this paper was on an overall measure of situational awareness in the context of eHealth and its relationship to demographics and awareness. It is now crucial to define the relationship factors between the attackers and the users in order to create a user-centric situational awareness framework in order to gain a fine grained understanding of the perceived environment and the strategies employed by attackers.

7 CONFLICT OF INTERESTS

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

8 ACKNOWLEDGEMENTS

The authors are grateful to Quentin Franssen for his participation, advices and his comments on earlier versions of the manuscript and to all the participants for their time and collaboration.

9 REFERENCES

Apple. (2016). Set up Apple Pay on your iPhone, iPad, Apple Watch, or Mac. Retrieved September 18, 2016, from https://support.apple.com/en-gb/HT204506

Belanche, D., Casaló, L. V., & Guinalíu, M. (2012). How to make online public services trustworthy. *Electronic Government, an International Journal*, *9*(3), 291. http://doi.org/10.1504/EG.2012.048004

Bellekens, X., Hamilton, A., Seeam, P., Nieradzinska, K., Franssen, Q., & Seeam, A. (2016). Pervasive eHealth services a security and privacy risk awareness survey. In *2016 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2016*. http://doi.org/10.1109/CyberSA.2016.7503293

Burghardt, T., Buchmann, E., Müller, J., & Böhm, K. (2009). Understanding User Preferences and Awareness: Privacy Mechanisms in Location-Based Services. In R. Meersman, T. Dillon, & P. Herrero (Eds.), *On the Move to Meaningful Internet Systems: OTM 2009: Confederated International Conferences, CoopIS, DOA, IS, and ODBASE 2009, Vilamoura, Portugal, November 1-6, 2009, Proceedings, Part I* (pp. 304–321). inbook, Berlin, Heidelberg: Springer Berlin Heidelberg. http://doi.org/10.1007/978-3-642-05148-7_21

Di Pietro, R., & Mancini, L. V. (2003). Security and privacy issues of handheld and wearable wireless devices. *Communications of the ACM*, *46*(9), 74–79. http://doi.org/10.1145/903893.903897

Endsley, M. R. (1995). Measurement of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 65–84. http://doi.org/10.1518/001872095779049499

Endsley, M. R. (1998). Situation awareness global assessment technique (SAGAT). In *Proceedings of the IEEE 1988 National Aerospace and Electronics Conference* (pp. 789–795). IEEE.

http://doi.org/10.1109/NAECON.1988.195097

Festinger, L. (1957). Cognitive dissonance theory. *1989) Primary Prevention of HIV/AIDS: Psychological Approaches. Newbury Park, California, Sage Publications*. article.

Festinger, L. (1964). *Conflict, decision, and dissonance* (Vol. 3). book, Stanford University Press.

Friedland, G., & Choi, J. (2011). Semantic Computing and Privacy: a Case Study Using Inferred Geo-Location. *International Journal of Semantic Computing*, *5*(1), 79–93. http://doi.org/10.1142/S1793351X11001171

Gan, D., & Jenkins, L. (2015). Social Networking Privacy—Who's Stalking You? *Future Internet*, *7*(1), 67–93. http://doi.org/10.3390/fi7010067

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Inexperience and experience with online stores: The importance of tam and trust. *IEEE Transactions on Engineering Management*, *50*(3), 307–321. http://doi.org/10.1109/TEM.2003.817277

Harris, J. (2016). Is Security a Concern for Wearables? Retrieved from https://www.mwrinfosecurity.com/our-thinking/is-security-a-concern-for-wearables/

Heembrock, M. (2015). The risks of wearable tech in the workplace. *Risk Management*, *62*(1), 10–12. article.

Lakkaraju, K., Yurcik, W., & Lee, A. J. (2004). NVisionIP: Netflow Visualizations of System State for Security Situational Awareness. In *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security* (pp. 65–72). inproceedings, New York, NY, USA: ACM. http://doi.org/10.1145/1029208.1029219

Laurie, H., & Lynn, P. (2009). The use of respondent incentives on longitudinal surveys. *Methodology of Longitudinal Surveys*, 205–233. article.

Levin, Avner. Abril, P. S. (2008). Two Notions of Privacy Online. *Vand. J. Ent. & Tech. L.*, *11*(January 2009), 1001.

Lewis, K., Kaufman, J., & Christakis, N. (2008). The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. *Journal of Computer-Mediated Communication*, *14*(1), 79–100. http://doi.org/10.1111/j.1083-6101.2008.01432.x

Luxton, D. D., June, J. D., & Fairall, J. M. (2012). Social media and suicide: A public health perspective. *American Journal of Public Health*, *102*(SUPPL. 2), 195–200. http://doi.org/10.2105/AJPH.2011.300608

Madejski, M., & Bellovin, S. M. (2011). The Failure of Online Social Network Privacy Settings. *Methodology*, *10*(CUCS-010-11), 1–20. Retrieved from http://posterous.com/getfile/files.posterous.com/shaundakin/EISP1ZG5eaIRJIePuVK1vwdumGImwnqJm4pZrdA1s6Dl4mukj9gBWqnxhOh6/ColumbiaPrivacycucs-010-11.pdf

Musil, S. (n.d.). Wearables market expected to hit 213 million units shipped in 2020. Retrieved September 16, 2016, from https://www.cnet.com/news/wearables-market-expected-to-hit-213-million-units-shipped-in-2020/

Peppet, S. R. (2013). Regulating the Internet of Things : First Steps Toward Managing Discrimination , Privacy , Security , and Consent.

Ross, L. (1977). The intuitive psychologist and his shortcomings: Distortions in the attribution process. *Advances in Experimental Social Psychology*, *10*, 173–220. article.

Shepperd, J. A., Waters, E. A., Weinstein, N. D., & Klein, W. M. P. (2015). A Primer on Unrealistic Optimism. *Current Directions in Psychological Science* , *24*(3), 232–237. JOUR. http://doi.org/10.1177/0963721414568341

Singer, R. W., & Perry, A. J. (2015). Wearables: The Well-Dressed Privacy Policy. *Intellectual Property & Technology Law Journal*, *27*(7), 24. article.

Statista. (2016). Facts and statistics on Wearable Technology. Retrieved September 16, 2016, from https://www.statista.com/topics/1556/wearable-technology/

Thomas, M., & Menon, G. (2007). When Internal Reference Prices and Price Expectations Diverge: The Role of Confidence. *Journal of Marketing Research*, *44*(3), 401–409. http://doi.org/10.1509/jmkr.44.3.401

Wang, B. J., Ph, D., Iannotti, R. J., & Ph, D. (2012). Bullying Among U . S . Adolescents, *19*(September), 3–6.

Wang, C., Guo, X., Wang, Y., Chen, Y., & Liu, B. (2016). Friend or Foe?Your Wearable Devices Reveal Your Personal PIN. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security - ASIA CCS '16* (pp. 189–200). New York, New York, USA: ACM Press. http://doi.org/10.1145/2897845.2897847

Weinstein, N. D. (1984). Why it won't happen to me: perceptions of risk factors and susceptibility. *Health Psychology*, *3*(5), 431.

10 APPENDIX

Q1 Age: How old are you?

Q2 Gender: What is your gender?
Male
Female
Other

Q3 Education: What is your education level?
High School
Undergraduate (BSc, BSc (Hons))
Graduate (MSc)
Post-graduate (PhD, MD)

Q4 IT Expertise: What is your level of Expertise?
Excellent
Good
Moderate
Low

Q5 How many health monitoring devices do you possess?
None
One or more

Q6 Have you ever misplaced your wearable device or smartphone?
Yes
No

Q7 Should health data be subject to regulations?
Yes
No
I do not know

Q8 Have you heard of regulations regarding connected health sensors, wearable or eHealth services?
Yes
No

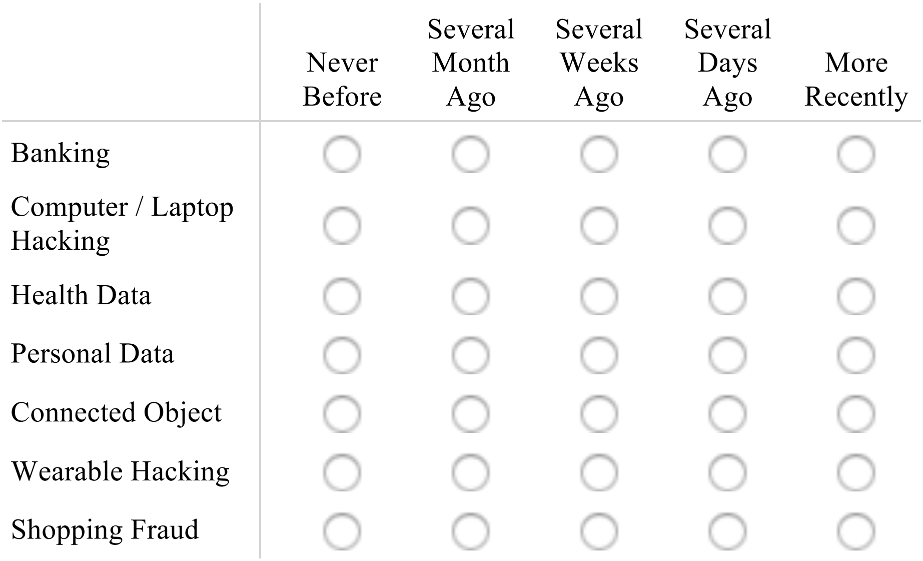
Q9 The following question is divided in two parts, in the first part, evaluate each threat and categorize them as a Security or Privacy threat or neither of them. In the second part evaluate (by ranking) the

likelihood of occurrence of each threat. Answer both questions based on your own experience.

	Not Likely	Likely	Extremely Likely	Security	Privacy		Neither
Data Theft	○	○	○	○		○	○
Identity Theft	○	○	○	○		○	○
User Profiling	○	○	○	○		○	○
Malware Infection	○	○	○	○		○	○
Receiving Spam	○	○	○	○		○	○
Cyber Bullying	○	○	○	○		○	○
Abuse of PC	○	○	○	○		○	○
Home Theft	○	○	○	○		○	○
Ability to locate user (at Home, at Work, etc)	○	○	○	○		○	○
Ability to infer user actions against his/her will (Sport, Driving, Sleeping)							

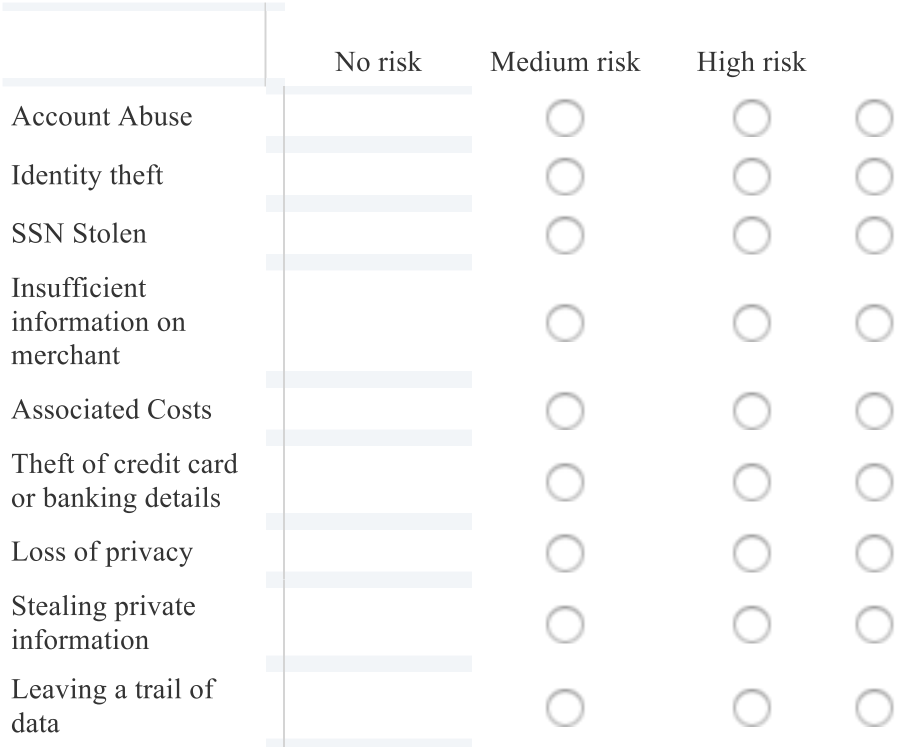
Q10 When is the last time you have heard about security or privacy fraud through a popular media such as the Internet, the radio, television or newspaper?

	Never Before	Several Month Ago	Several Weeks Ago	Several Days Ago	More Recently
Web Application	○	○	○	○	○
Mobile Application	○	○	○	○	○

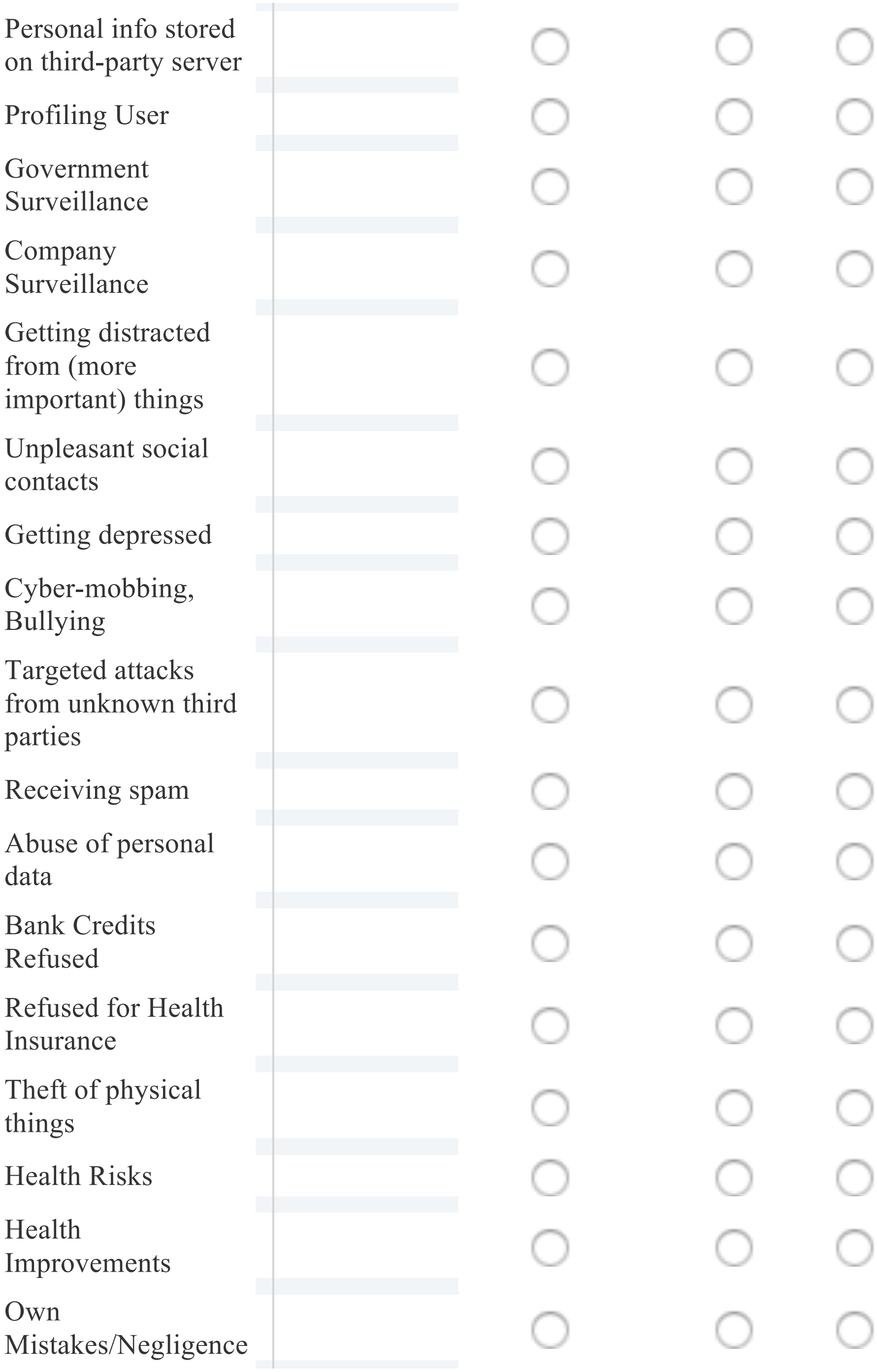


	Never Before	Several Month Ago	Several Weeks Ago	Several Days Ago	More Recently
Banking	○	○	○	○	○
Computer / Laptop Hacking	○	○	○	○	○
Health Data	○	○	○	○	○
Personal Data	○	○	○	○	○
Connected Object	○	○	○	○	○
Wearable Hacking	○	○	○	○	○
Shopping Fraud	○	○	○	○	○

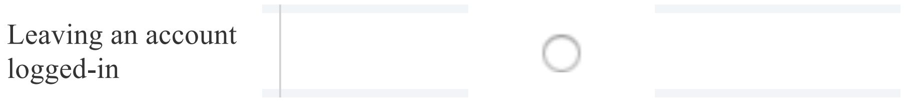
Q10 Evaluate the risk and likelihood of occurrence of each threat against your own wearable device, wearable service provider, or wearable data storage provider in a near future?



	No risk	Medium risk	High risk	
Account Abuse		○	○	○
Identity theft		○	○	○
SSN Stolen		○	○	○
Insufficient information on merchant		○	○	○
Associated Costs		○	○	○
Theft of credit card or banking details		○	○	○
Loss of privacy		○	○	○
Stealing private information		○	○	○
Leaving a trail of data		○	○	○

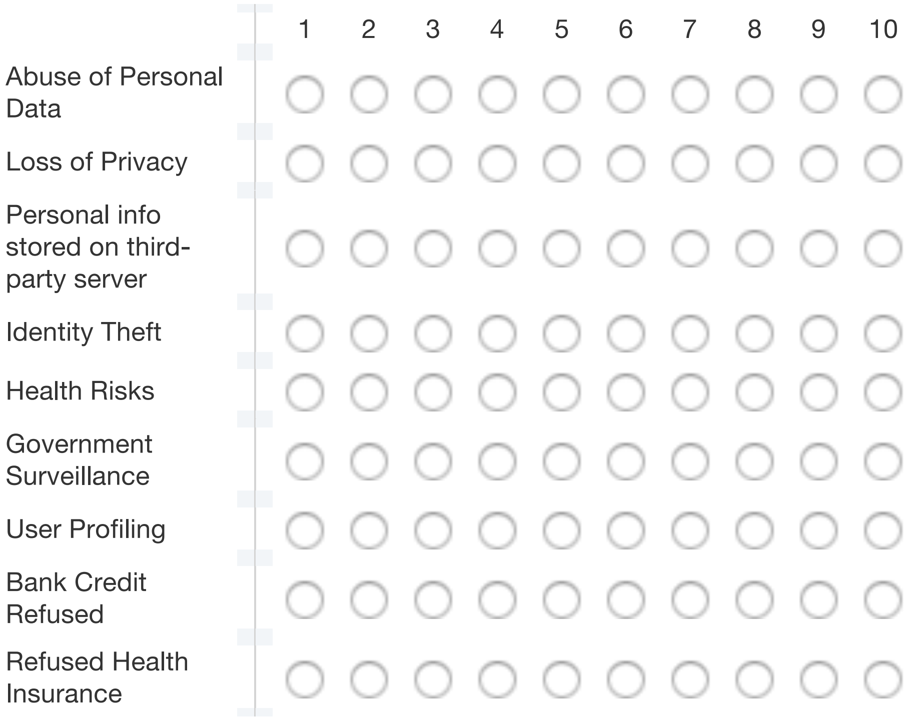


Personal info stored on third-party server	○	○	○
Profiling User	○	○	○
Government Surveillance	○	○	○
Company Surveillance	○	○	○
Getting distracted from (more important) things	○	○	○
Unpleasant social contacts	○	○	○
Getting depressed	○	○	○
Cyber-mobbing, Bullying	○	○	○
Targeted attacks from unknown third parties	○	○	○
Receiving spam	○	○	○
Abuse of personal data	○	○	○
Bank Credits Refused	○	○	○
Refused for Health Insurance	○	○	○
Theft of physical things	○	○	○
Health Risks	○	○	○
Health Improvements	○	○	○
Own Mistakes/Negligence	○	○	○



Leaving an account logged-in		○	

Q11 Rate the security and privacy threats against wearable devices by severity, based on your personal experience (1 being the lowest and 10 being the highest).



	1	2	3	4	5	6	7	8	9	10
Abuse of Personal Data	○	○	○	○	○	○	○	○	○	○
Loss of Privacy	○	○	○	○	○	○	○	○	○	○
Personal info stored on third-party server	○	○	○	○	○	○	○	○	○	○
Identity Theft	○	○	○	○	○	○	○	○	○	○
Health Risks	○	○	○	○	○	○	○	○	○	○
Government Surveillance	○	○	○	○	○	○	○	○	○	○
User Profiling	○	○	○	○	○	○	○	○	○	○
Bank Credit Refused	○	○	○	○	○	○	○	○	○	○
Refused Health Insurance	○	○	○	○	○	○	○	○	○	○

Q12 Are you concerned about the privacy of your data?

Yes
No

Q13 Are you currently using an anti-virus software on your computer?

Yes
No

Q14 Do you consider security and privacy essential to health monitoring devices?

Yes
No

Biographical notes:

Xavier Bellekens received the Bachelor Degree from Henam in Belgium; the Masters degree in Ethical Hacking and Computer Security from the University of Abertay Dundee and the PhD in Electronic and Electrical Engineering from the University of Strathclyde in Glasgow in 2010, 2012 and 2016 respectively. He is currently a lecturer in Security and Privacy at the University of Abertay Dundee. His current research interests include deep learning for cyber-security, situational awareness, autonomous distributed networks, the Internet of Things and critical infrastructure protection.

Kamila Nieradzinska received her MEng degree in mechanical engineering from Wroclaw University of Technology, Poland in 2008 and in the same year was awarded her BSc in Building Services and Engineering from Glasgow Caledonian University, Scotland. Currently she is working towards her PhD at the University of Strathclyde, Glasgow; her research interests include renewable energy integration, critical infrastructure protection, the Internet of Things, as well as security and privacy.

Alexandra Bellekens is currently working towards a Masters Degree in organizational psychology at the Université Catholoque de Louvain in Belgium. Her research interests include social psychology, human resources, situational awareness and testing

Preetila Seeam is a lecturer in Business and Management at Aberystwyth University (Mauritius Branch Campus). She received her BSc in Management and MSc in Human Resource Studies from the University of Mauritius in 2008 and 2010 respectively. Her current research interests include knowledge management, knowledge sharing cultures and organisational behaviours.

Andrew Hamilton is a researcher at the University of Strathclyde. His projects include the development of novel aerospace manufacturing technology through sensor technology and the optimisation of continuous pharmaceutical manufacturing through 3D modeling of crystalline structures. He received his Ph.D in 2015 for his work into the development of condition monitoring systems for offshore wind turbine gearboxes. He graduated with an MEng in Civil Engineering in 2009 with a focus on the sustainable design of timber frame structures.

Amar Seeam is a computer science lecturer at Middlesex University (Mauritius Branch Campus), where he coordinates Internet of Things related research activities. He received his PhD in 2015 for his work on the validation of building simulation tools for predictive control applications and gained his MSc in System Level Integration in 2005 both at the University of Edinburgh. Previously he graduated with a BEng in Mechanical Engineering and MSc in Information Technology (Systems) from the University of Glasgow, in 2003 and 2004, respectively. His current research interests include next generation network architectures for the Internet of Things, IPv6 deployment strategies, eHeatlh, smart cities, building simulation, intelligent buildings, distributed wireless sensor networks and historical computing.