

Assessing User Privacy Concerns in the Wearable Tech Industry

Paulovics, Agnes¹

Abstract: Wearable technologies, such as smart watches and fitness trackers, are devices worn on the body that connect to the internet and gather data. They provide valuable real-time insights into an individual's health and lifestyle, which highlights the importance of data security and ownership.

This study examines how much trust users have in the privacy aspects of wearable technology and what data security concerns they have. The study began with a detailed examination of the market for wearables, e-textiles, and smart textiles, explaining their technical specifics and differences. The research findings showed that data security is a significant consideration for at least 25% of wearables users when making a purchase. Furthermore, a comparison of perceptions across countries revealed that Hungarians are at least 10% more likely than the Swiss to believe that data collected by wearables is stored securely.

Keywords: *wearables, smart textiles, data security, data ownership*

JEL Codes: *M14, I15, I18*

Introduction

Digitalization is a part of humans' daily lives. Health data can nowadays be collected unnoticed with smart garments, e-textiles, and wearables thus providing a deep insight into humans' vital data and health status. These devices can record heart rate (BPM), heart rate variability (HRV), electrocardiogram (ECG), acceleration, GPS, respiration rate, and many others.

¹ PAULOVICS, Agnes PhD-Student [PhD-hallgató]

(<https://orcid.org/0009-0004-3092-1406>)

University of Sopron István Széchenyi Economics and Management Doctoral School
[Soproni Egyetem Széchenyi István Gazdálkodás- és Szervezéstudományi Doktori Iskola]

(agnes@agnespaulovics.com)

However, recording a large amount of sensitive information comes with some drawbacks and challenges. It is often not clearly communicated how the data is processed and whether it is used for monetary purposes.

With advancing technology, devices like e-textiles constantly collect vast amounts of personal data. The European Union's GDPR defines personal data as any information relating to an identifiable individual, including location, online identifiers, and even physical or cultural attributes (*What Is GDPR, the EU's New Data Protection Law?*, 2018). When e-textiles connect to user accounts, they access data from both the device and user's account. Without proper anonymization, this data can be misused, from targeted advertising to serious crimes like identity theft. Therefore, users must understand how their data is used, stored, and shared, enabling them to manage their data and make informed decisions about technology use.

The researcher, currently residing in Switzerland, has had the opportunity to establish a network of personal contacts in both Switzerland and Hungary. Through her interactions, an impression has been formed that suggests a heightened emphasis on data sovereignty in Switzerland compared to Hungary. Moreover, there is a discernible increase in the overall concern for data security. This research aims to investigate and corroborate these preliminary observations.

Three hypotheses are formulated at the beginning of the research:

- Hypothesis 1:* A significant proportion of wearable users consider data security as an important factor when buying a product.
- Hypothesis 2:* Owners fear the loss and theft of data at different levels depending on the type of the data.
- Hypothesis 3:* Hungarians are more likely than the Swiss to consider the storage of wearable data as secure.

Literature Review

The field of e-textiles, smart textiles, and wearable technology is continuously growing. These technologies blend textiles with electronic properties bringing novel solutions to the industry both visually and functionally. The revenues from wearables and smart textiles grow year by year. This development indicates that these technologies have a promising future (Singha et al., 2019).

The definitions of e-textiles, smart clothing, and wearable technology often seem confusing, and distinguishing between their functionalities is complicated.

E-textiles, or electronic textiles, incorporate digital components such as conductive fibers into traditional fabric. This technology allows them to perform simple electronic functions like lighting up or heating.

Smart textiles take this a step further. These are fabrics that not only integrate electronic components but also can respond to environmental stimuli. For example, a smart textile might react to changes in temperature, mechanical stress, or biological signals like heart rate.

Wearable technologies, often referred to as “wearables”, are devices designed to be worn on the body. These can range from smart watches to fitness trackers and often have capabilities that allow them to connect to the internet, collect data, and even process and transmit this data for various uses. While many wearable devices make use of e-textiles or smart textiles in their design, it’s not a requirement – some, like a smartwatch, contain advanced digital functions but do not use a textile component.

Each term represents a different level of the fusion between digital technology and items designed to be worn, providing new possibilities for data collection, health monitoring, and user convenience (*Figure 1*).

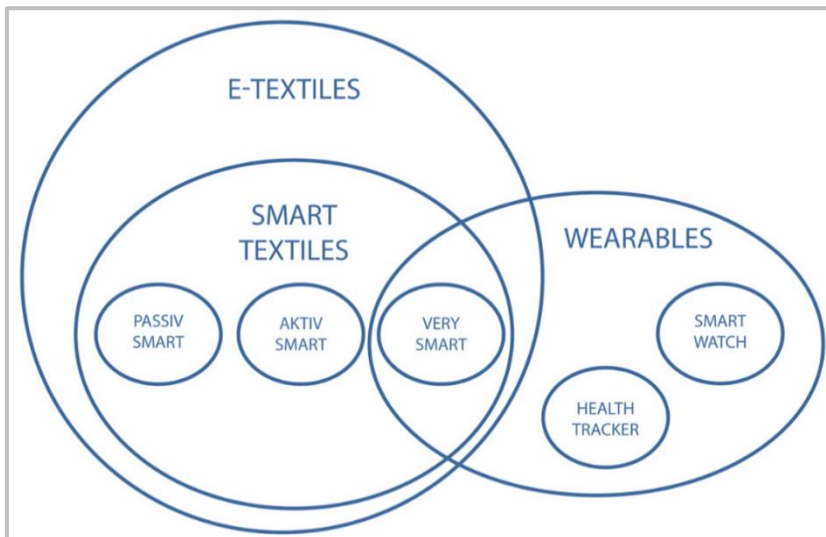


Figure 1 An overview of the relationships between e-textiles, smart clothing, and wearable technology

Source: Own visualization

As it can be seen on the self-created visualization in *Figure 1*, e-textiles is a large area, of which the group of smart textiles is entirely part, but wearables are partly included in e-textiles, as well. *Figure 1* should serve as an orientation when reading the definitions.

E-Textiles

E-textile is used as an abbreviation for electronic textile or electronically integrated textile (Maxey, 2019). Electronic textiles “*are, or are part of, electronic components that create systems capable of sensing, heating, lighting or transmitting data*” (Wilson & Teverovsky, 2012:156).

E-textiles are produced of printed electronics, conductive inks, or conductive threads. Both smart clothing and wearable technology can be produced of e-textiles.

E-textile is a circuit that is constructed into a textile, or it is designed to be integrated into a textile. E-textiles can be produced in two different ways: embedded or laminated. Embedded systems are woven or knitted into the garment. Laminated e-textiles mean that circuitry is manufactured on a non-textile substrate that gets added to a textile with sewing or bonding (Maxey, 2019).

E-textiles can serve two different goals. On the one hand, these textiles can be developed for aesthetic reasons. Conventional textiles are equipped with new electronic features, such as LEDs, glass fibers, electrically conductive threads, and electroluminescent film, to develop a new kind of textile. There are solutions where the LEDs light up when the wearer moves, or textiles that react to their immediate surroundings and mimic the colors of the environment. Additionally, touch, voice, and motion sensors can be integrated into the clothing; thus, it can change its shape and color, or make sounds, as well (Kennedy & Stoehrer, 2014). E-textiles are not necessarily smart, can do just simple tasks and can operate without a software, smartphone, or application (Orlando, 2019).

Smart textiles

On the other hand, e-textiles can be developed for performance reasons. These textiles are often called smart textiles and employ conduction yarns and sensors to collect data or provide experience. Smart textiles can perceive stimuli from the surroundings and respond to them, adjusting to them by embedding functions in the texture of the textiles (Tao, 2001). The applied technologies can be e.g., heating pads, vibrating pads, speak-

ers, motion sensors, or wireless connection. These textiles can be controlled with external devices or navigated with inbuilt regulators (Saha, 2020). The aim of these smart textiles is to collect data about vital measurements, heat, light, movement, and other local conditions (Nichols, 2020).

Existing synonyms for e-textiles are e-textile system and soft circuit. In some cases, the terms smart textile, functional fabric, smart fabric, ultra-flexible circuit, and technical textiles are used as synonyms, as well (Maxey, 2019). Smart clothing is finding usage in healthcare, sports, lifestyle, space exploration, public safety, and military (Scataglini et al., 2019).

As smart textiles represent a new and unknown technology, several factors must contribute to success. For the successful commercialization of smart garments, it is necessary to offer high functionalities and wearability as well as to develop the users' acceptance (Knight et al., 2002). Gilsoo (2009) complements this statement with highlighting the importance of even more factors by adding usability, monitoring duration, maintainability, and connectivity to the list of necessary factors.

In this context, researchers understand the successful measurement of vital information and the ability to monitor the health status under functionalities (Scataglini et al., 2019:1). Wearability stands for the easiness of putting the garment on and taking it off. Moreover, the fit, freedom of movement, and comfort belong to wearability, as well. User acceptance is the factor that depends on the wearers' cognitive comfort and their overall wellbeing during wearing smart garment (Knight et al., 2002). Therefore, it is of major importance to build up trust in the technology and to ensure customers about the safety of smart garments. Usability can be described as the *“extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use”* (ISO 9241-11. Ergonomic Requirements for Office Work with Visual Display Terminals, 1998:2). Monitoring duration means how long the batteries can absorb and transmit the information without running out of power. Maintainability indicates how long the smart garments can be used without replacement and whether repairs are possible. Finally, connectivity refers to the connection between the sensors and the electrical parts as well as to the interaction between the smart clothes and the outside world (Scataglini et al., 2019).

Intelligent clothing can be divided into three categories based on their smartness. First, there are the passive smart systems, which are merely

able to sense the environment. Second, the active smart systems cannot solely perceive the surroundings but respond to them, as well. Third, the very smart systems are the most advanced, which can change according to the conditions (Stoppa & Chiolerio, 2014; Scataglini et al., 2020).

Wearables

A wearable is a “*device for electrocardiography signal collection and heart rate monitoring*” (Lin et al., 2018:1). However, the “*wearable technology found in modern fashion garments are no longer just smart sensors but have evolved into being part of a complex ecosystem comprising sustainable and innovative apparel, aiming for a cleaner industry and a healthier lifestyle*” (Arnault, 2018:18). These garments constantly monitor and observe their surroundings thus gathering valuable and sensitive data (Ziccardi, 2020). The wearables are able to collect physiological signals (i.e., BPM, ECG, respiration, and body temperature), performance indicators (i.e., posture, aerodynamics, and movements), and environmental aspects (i.e., temperature and humidity) (Scataglini et al., 2020). Wearables merge the textiles with technology through the incorporation of conductive fibers (Sundaram et al., 2019), sensors, processors, communication equipment, displays, or input devices (Sonderegger, 2013) thus creating solutions that are both fashionable, functional, and comfortable (Sen et al., 2015). On the one hand, conductive fibers can be natural fibers, such as ferrous alloys, nickel, stainless steel, titanium, aluminium, or copper. On the other hand, they can be threaded conductive fibers, such as conductive metal or carbon powders (Scataglini et al., 2020).

The wearables open new perspectives for marketing possibilities. On the one hand, the wearers can be very precisely controlled thanks to the GPS tracking; thus, their behavior can be analyzed throughout the day. For example, their behavior can be monitored while they are shopping. On the other hand, the profiling can be much more accurate as it might contain the clients’ sensitive characteristics, as well (Ziccardi, 2020).

Privacy and security issues of e-textiles, smart garments, and wearables

One of the specialties of smart garments and wearables is the fact that the wearers do not recognize that they are monitored during the whole day (Ziccardi, 2020). Due to the close cooperation with the body, those clothes that have the ability to interact with the body and act autonomously might collect much more information and have access to sensitive data, too. For

these products, it appears important to investigate the legal aspects (Katyál, 2014) as they can be seen as “*potentially dangerous technologies for human beings*” (Ziccardi, 2020:6).

Ziccardi (2020) highlights the importance of privacy by design. According to this approach, during the development phasis, cybersecurity measures should be implemented, and protection should be incorporated as soon as designing the products. The scholar emphasizes that “*privacy and security, in conclusion, are at the hearth of wearable technologies*” (Ziccardi, 2020:7). To reduce the potential for damage associated with data breach, the use of anonymous data and the encryption of information are essential, as well (Ziccardi, 2020).

Methodology

The introduction and literature review of current research paper have already given an insight into the wearables, smart textiles, and e-textiles sector. The next part of the research includes studying the view of wearable owners on data security aspects.

The aim of this study is to collect and analyze the wearable users’ behavior and preferences. To examine the hypotheses, quantitative research is conducted, where the answers are measured on a Likert scale. The participants of the survey could decide if they agree or disagree and to what extent they agree or disagree with the provided selection criteria. Additionally, the survey uses yes-or-no questions to collect the participants’ attitude.

The quantitative survey is distributed through personal contacts and social media posts. All together 115 people participate in the survey. Four respondents do not own wearables; thus, their answers are not included in this research. Therefore, the total number of the participants is 111.

Both men and women are represented as participants in the survey. 45.95% of the respondents are women, while 54.05% of the participants are men (*Figure 2*).

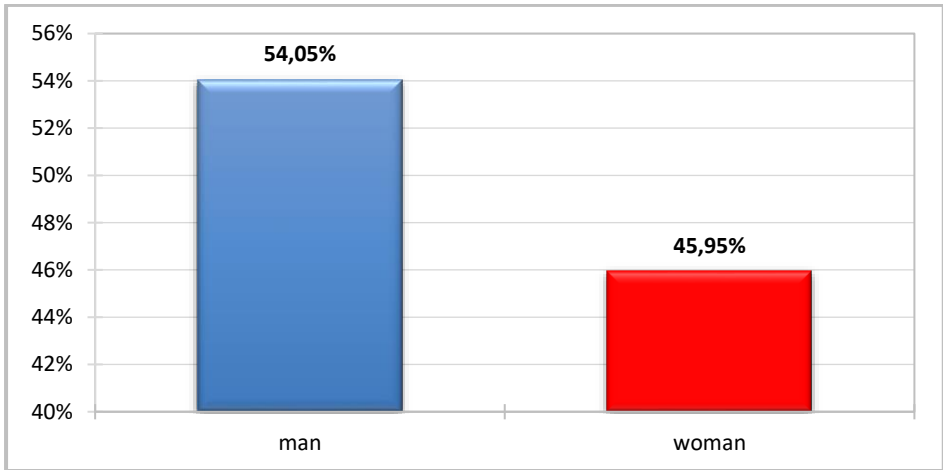


Figure 2 The gender distribution of the survey participants

Data source: Own questionnaire

Furthermore, the countries of residence show differences among the participants. 41 of the 111 survey respondents are from Switzerland, 41 participants live in Hungary, 12 people are from Germany, seven respondents live in Austria, and 10 participants are from other countries (*Figure 3*).

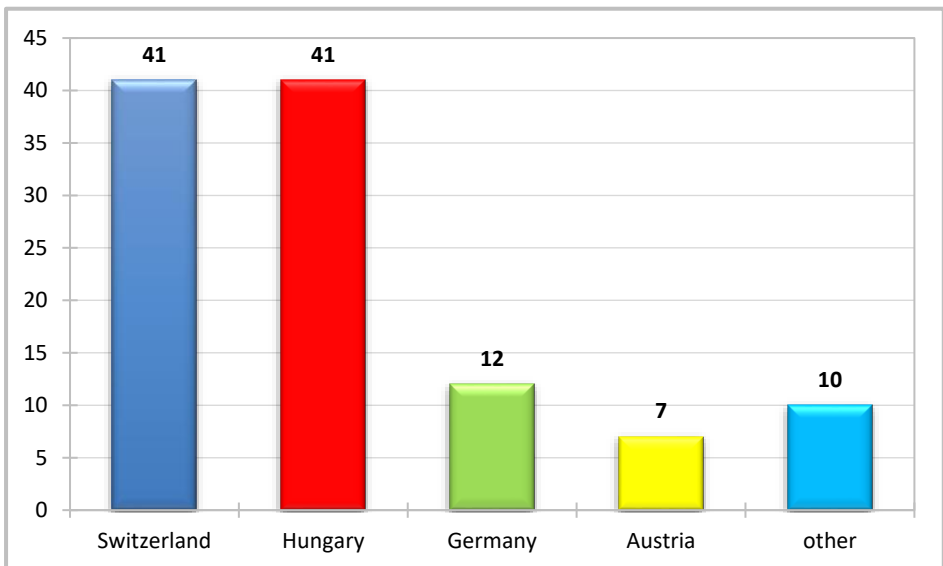


Figure 3 The participants' countries of residence

Data source: Own questionnaire

The survey participants' age distribution is similar to the wearable owners' age distribution in the survey of eMarketer Editors (2018). In the 2018 survey, most wearable users are between the ages of 25-34 followed by the groups of 35-44 and 18-24. Comparing these survey participants' ages, it is visible that in current research, most people are from the age group of 25-36, as well. The order of the groups 35-44 and 18-24 is slightly different, but these two groups are the second and third highly represented ones in this survey, too (*Figure 4*).

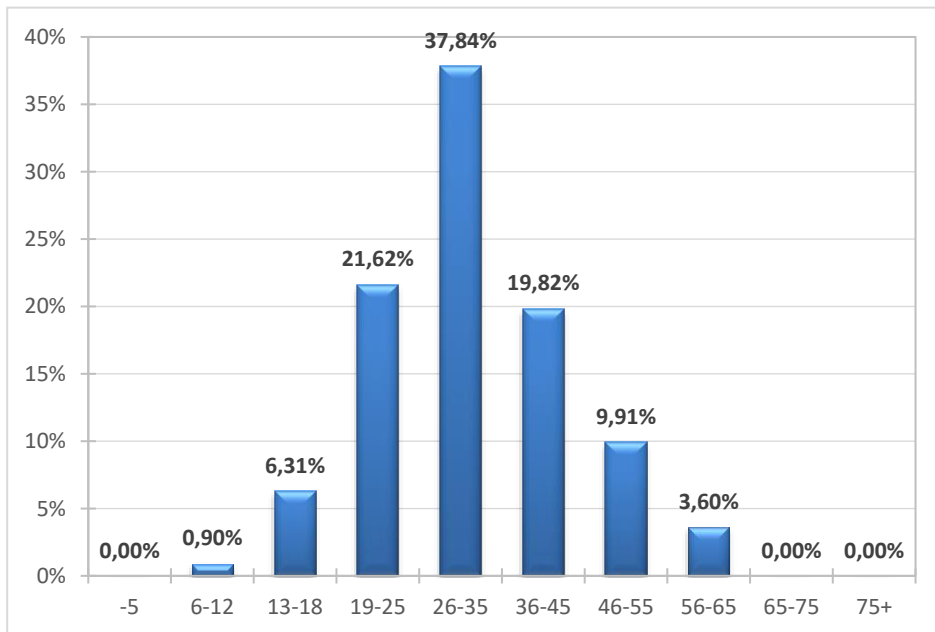


Figure 4 The survey participants' age distribution

Data source: Own questionnaire

Considering the length of possessing a wearable, it can be seen that a lot of respondents, over 30% of the survey participants, have been owning a wearable for over two years. This group is followed by 27.93% of the participants stating that they bought a wearable within the last one year. 20.72% declare that they have been owning their wearables for a half year, and 17.12% have been using the technology for two years.

Just a very small percentage, 3.6% of the participants say that they bought their smartwatch or wearable just one month ago (*Figure 5*).

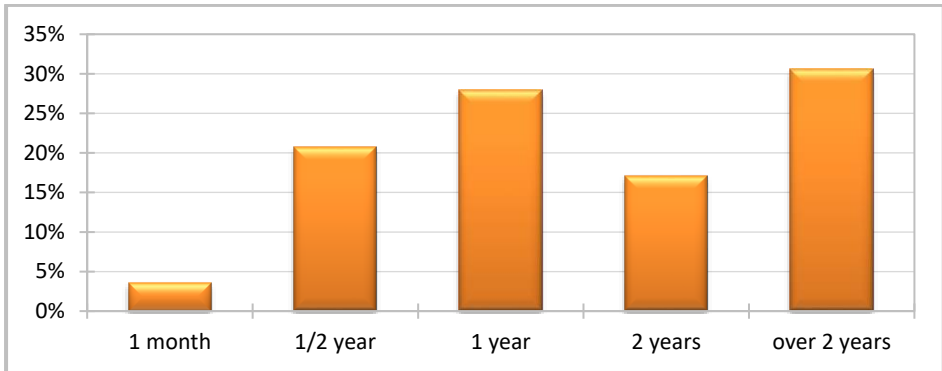


Figure 5 The duration regarding the possession of wearables

Data source: Own questionnaire

Research findings

Hypothesis 1: A significant proportion of wearable users consider data security as an important factor when buying a product.

Hypothesis 1 suggests that data security is considered as an important factor by a significant proportion of wearable users when purchasing a product. A significant proportion was quantified as 25% for the purpose of this analysis.

A one-sample z-test was applied to validate this hypothesis as the data set was independent and composed of at least 30 participants. The analysis was performed at a significance level of $\alpha=0.05$, allowing a confidence level of 95% if the null hypothesis could be successfully rejected.

The survey results indicated that 36 out of 111 participants consider data protection as an important factor when buying a wearable. This leads to a proportion of $P=36/111=0.324324$.

The calculated z-score ($z_0=1.808$) exceeded the critical value ($z_{crit}=1.6449$), leading to the rejection of the null hypothesis. Consequently, with 95% confidence, it can be concluded that the proportion of consumers who regard data protection as important during the purchasing process of wearables is at least 25%. Therefore, Hypothesis 1 is supported.

Figure 6 below illustrates the importance of various factors in purchasing wearables. It becomes evident that quality, technical functions, and app integrations are key aspects for wearable buyers. Contrarily, the

weight and novelty level are considered important by a maximum of 14% of the respondents (*Figure 6*).

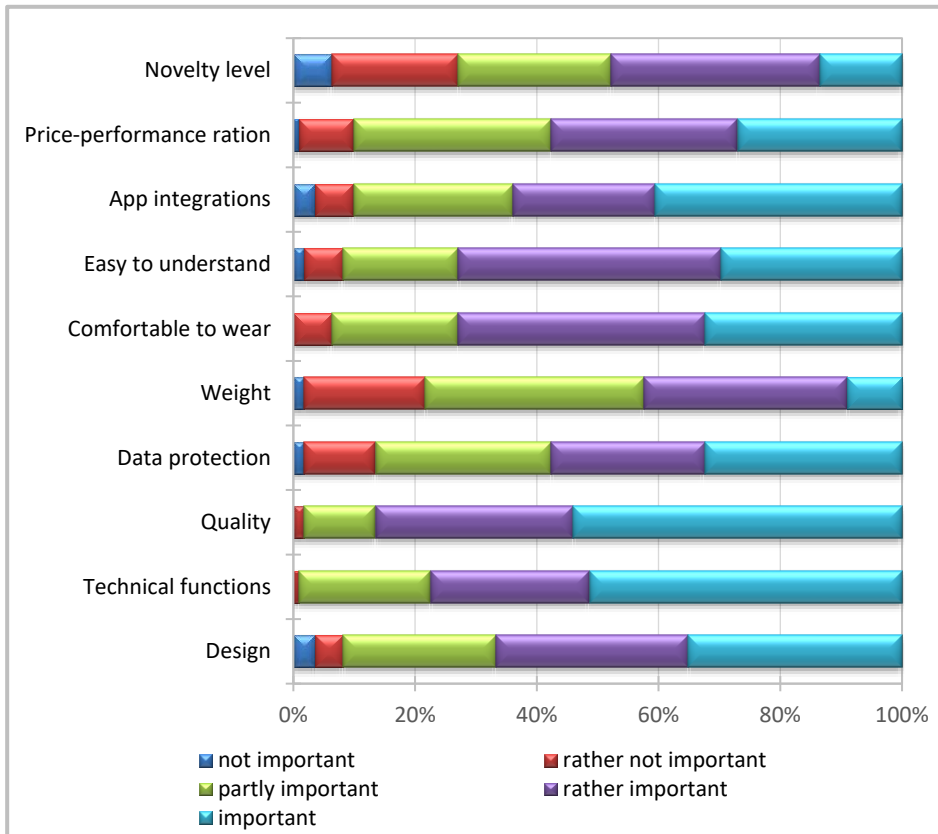


Figure 6 The importance of various factors in purchasing wearables

Data source: Own questionnaire

Hypothesis 2: Owners fear the loss and theft of data at different levels depending on the type of the data.

Hypothesis 2 posits that the degree of apprehension concerning data loss and theft among device owners varies according to the type of data.

An initial evaluation of survey respondents' concerns about various types of data theft indicates a pronounced level of anxiety associated with the potential theft of passwords or financial information. GPS location and address information also elicited considerable concern. Conversely, the potential theft of data such as daily step count, age, fitness level, heart

rate, and name seemed to cause minimal distress among participants, based on the “very much” rating.

The figure below, labeled as *Figure 7*, illustrates the distribution of these fears about data loss and theft.

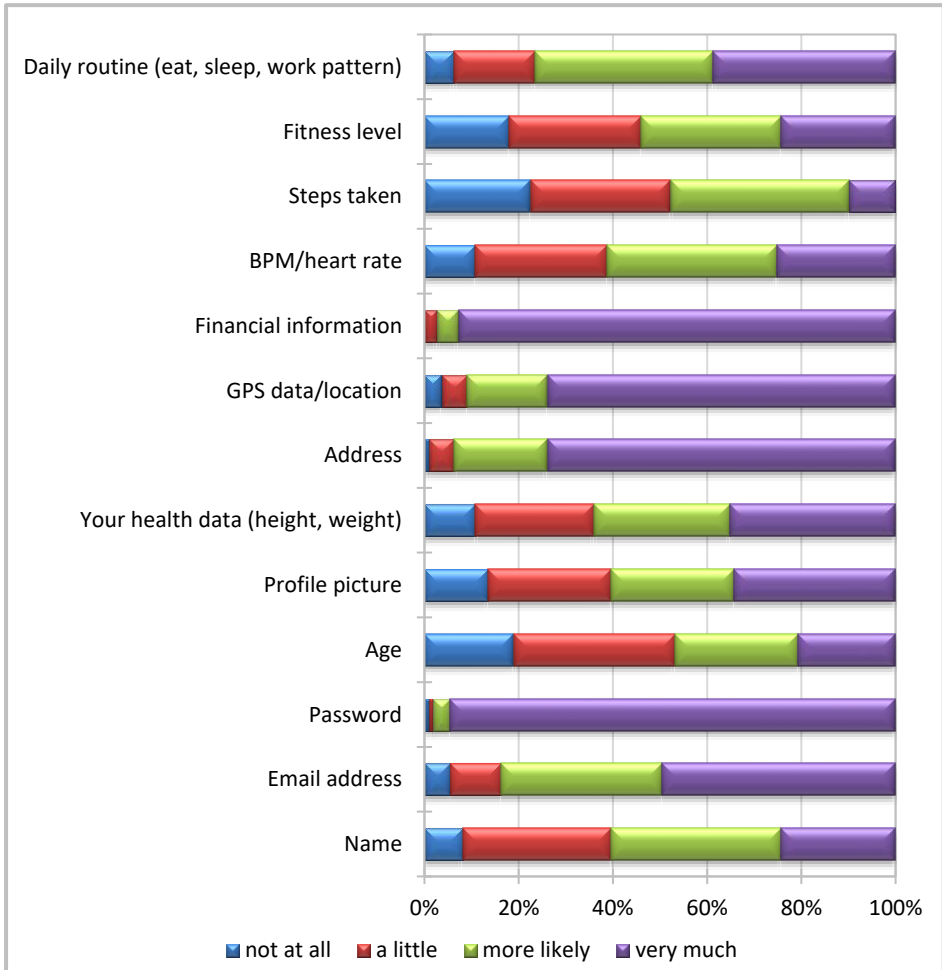


Figure 7 The distribution of fear of loss and theft of data

Data source: Own questionnaire

To further explore this hypothesis, an Analysis of Variance (ANOVA) was conducted to detect any significant group differences among four selected types of data: financial information, password, GPS location, and address.

The null hypothesis (H0) was set as no difference among the mean levels of concern across these data types, whereas the alternative hypothesis (H1) proposed that at least one mean differs from the others. This analysis was performed at a significance level of $\alpha=0.05$, implying a 95% confidence level if the null hypothesis could be rejected (*Table 1*).

Table 1 ANOVA Calculation

SUMMARY						
Group	Count	Sum	Average	Variance		
Password	111	435	3.918918919	0.147911548		
Address	111	407	3.666666667	0.387878788		
GPS data/location	111	401	3.612612613	0.566748567		
Financial information	111	433	3.900900901	0.144635545		
ANOVA						
Source of Variation	SS	df	MS	F	P-value	F crit
Between the groups	8.288288288	3	2.762762763	8.860870327	1.03035E-05	2.625176998
Within the groups	137.1891892	440	0.311793612			
Total	145.4774775	443				

Source: Own questionnaire

ANOVA computations yielded a p-value of approximately 1.03×10^{-5} , which is below the $\alpha=0.05$ threshold, thereby rejecting the null hypothesis. This result supports the alternative hypothesis, indicating that the degree of concern about data theft varies depending on the type of data. This conclusion aligns with the F statistic obtained from the analysis, which exceeded the critical value.

Hence, Hypothesis 2 is substantiated. It should be noted, however, that while this analysis establishes the existence of significant differences, further post-hoc tests may be necessary to pinpoint precisely which types of data differ significantly in terms of the concern they generate among device owners.

Hypothesis 3: Hungarians are more likely than the Swiss to consider the storage of wearable data as secure.

Hypothesis 3 postulates that Hungarian respondents are more likely than their Swiss counterparts to perceive the storage of wearable data as secure. In statistical terms, this posits that the proportion of Hungarians

expressing confidence in data security significantly exceeds the corresponding proportion among Swiss respondents.

A two-sample z-test was employed for this analysis. This method was chosen as the samples were independent, and each consisted of more than 30 observations. The analysis was conducted at a significance level of $\alpha=0.02$, providing a confidence level of 98%.

The results revealed a larger proportion of Hungarian respondents ($p_1=23/41=0.56098$) expressing agreement (either “rather agreeing” or “totally agreeing”) that data from their smartwatch or wearable is securely stored compared to Swiss respondents ($p_2=10/41=0.24390$).

The computed z-score for this comparison ($z_0=2.12$) exceeded the critical value ($z_{crit}=2.05$). Therefore, the null hypothesis was rejected at a confidence level of 98%. This confirms the initial hypothesis that a significantly higher proportion of Hungarian respondents believe in the security of wearable data compared to Swiss respondents.

The quantification of the difference is not provided here; however, these findings have important implications for understanding regional variations in the perceptions of wearable data security.

Conclusion

The terms e-textiles, smart textiles and wearable technology are often used interchangeably, although all three should be used in their own specific fields. The wearables are able to collect physiological signals, performance indicators, and environmental aspects, which are all private related data. The market of wearable devices is growing rapidly, which raises the question of who owns the data and how it should be processed.

Thus the current research work addresses the wearable users’ data security concerns. Three hypotheses are formulated and investigated based on a quantitative survey. Based on the results, I can conclude that all hypothesis can be accepted, and I formulate the following theses:

Thesis 1: A significant proportion of wearable users consider data security as an important factor when buying a product.

Among wearable users, at least 25% consider data security as an important factor when buying a product. Based on the statement “important”, the most important characteristics for wearable buyers are the followings: quality, technical functions, and app integrations.

Thesis 2: Owners fear the loss and theft of data at different levels depending on the type of the data.

Owners fear the loss and theft of data at different levels depending on the type of the stolen data. Participants indicate that they would be very worried if their password, financial information, GPS location, or address were stolen. On the other hand, they would be merely slightly bothered if their daily step count, age, fitness level, BPM, and name were hijacked.

Thesis 3: Hungarians are more likely than the Swiss to consider the storage of wearable data as secure.

An interesting finding of the research is that Hungarians trust the companies managing their data more than the survey participants from Switzerland. Significantly higher proportion of Hungarian respondents believe in the security of wearable data compared to Swiss respondents.

A limitation of the study is the low number of participants in the survey. 111 individuals participate in the questionnaire, which with high probability don't represent the population.

Bibliography

- Arnault, L. (2018, October). The Only Thing That Buyers Want from Wearable Technology Fashion. Retrieved: September 29, 2022, from <https://www.fibre2fashion.com/industry-article/8157/the-only-thing-that-buyers-want-from-wearable-technology-fashion>
- eMarketer Editors. (2018, December 13). Who's Driving Wearables Adoption? – EMarketer Trends, Forecasts & Statistics. Retrieved: October 6, 2022, from <https://www.insiderintelligence.com/content/older-americans-drive-growth-of-wearables>
- GDPR.EU. (2018, November 7). What is GDPR, the EU's new data protection law? GDPR.Eu. Retrieved: 22. June 2022, from <https://gdpr.eu/what-is-gdpr/>
- Gilsoo, C. (2009). Smart Clothing: Technology and Applications. CRC Press, ISBN: 9781420088526. Retrieved: 17. September 2022, from <https://www.routledge.com/Smart-Clothing-Technology-and-Applications/Cho/p/book/9781420088526>
- ISO 9241-11. (1998). Ergonomic requirements for office work with visual display terminals (Guidance on usability (VDTs)-Part 11), ISO.
- Katyal, N. (2014). Disruptive technologies and the law. *The Georgetown law journal*, 102:1685–1689. Retrieved: 17. September 2022, from <https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2901&context=facpub>

- Kennedy, A., & Stoehrer, E. B. (2014). Fashion. The handbook of fashion (Fashion. Das Handbuch der Mode), Haupt Verlag.
- Knight J. F., Baber C., & Schwirtz A. (2002). The comfort assessment of wearable computers. *Sixth International Symposium on Wearable Computers (ISWC 2002)*:65–72. DOI: <https://doi.org/10.1109/ISWC.2002.1167220>
- Lin, C.-C., Yang, C.-Y., Zhou, Z., & Wu, S. (2018). Intelligent health monitoring system based on smart clothing. *International Journal of Distributed Sensor Networks*, 14. DOI: <https://doi.org/10.1177/1550147718794318>
- Loomia Technologies Inc. (2019). What's the Difference between an E-Textile, Smart Fabric, Functional Fabrics and Smart Textiles? Retrieved: August 15, 2022, from <https://www.loomia.com/blog/whats-the-difference-between-an-e-textile-smart-fabric-functional-fabrics-and-smart-textiles>
- Nichols, M. R. (2020, January 10). How Are E-Textiles & Smart Textiles Different? Retrieved: September 16, 2022, from <https://www.iiotnewshub.com/news/articles/444210-how-e-textiles-smart-textiles-different.htm>
- Orlando, J. (2019, January 14): Electronic Textiles, Wearable Technology & Smart Garments. What's the Difference? Retrieved: July 18, 2022, from <https://butler-technologies.com/electronic-textiles/>
- Saha, S. (2020, November 29): Difference Between Electronic Textiles, Smart Textiles/Garments and Wearable Technology. Retrieved: September 9, 2022, from <https://www.onlineclothingstudy.com/2020/11/difference-between-electronic-textiles.html>
- Scataglini, S., Andreoni, G., Gallant, J. (2019). Smart Clothing Design Issues in Military Applications. In: Ahram, T. (eds) Advances in Human Factors in Wearable Technologies and Game Design. AHFE 2018. Advances in Intelligent Systems and Computing, vol 795. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-94619-1_15
- Scataglini, S., Moorhead, A., & Feletti, F. (2020). A Systematic Review of Smart Clothing in Sports: Possible Applications to Extreme Sports. *Muscle Ligaments and Tendons Journal*, 10. DOI: <https://doi.org/10.32098/mltj.02.2020.19>
- Sen, S., Chakrabarty, S., Toshniwal, R., & Bhaumik, A. (2015). Design of an intelligent voice controlled home automation system. *International Journal of Computer Applications*, 121(15):975–8887. DOI: <https://doi.org/10.5120/21619-4904>
- Singha, K., Kumar, J., & Pandit, P. (2019). Recent Advancements in Wearable & Smart Textiles: An Overview. In *Materials Today: Proceedings*, 16:1518–1523. DOI: <https://doi.org/10.1016/j.matpr.2019.05.334>
- Sonderegger, A. (2013, September 8). Smart garments – The issue of usability and aesthetics. In UbiComp '13 Adjunct: Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication, 385–392. DOI: <https://doi.org/10.1145/2494091.2495969>
- Stoppa, M., & Chiolerio, A. (2014): Wearable electronics and smart textiles: A critical review. *Sensors*, 14:11957–11992. DOI: <https://doi.org/10.3390/s140711957>

- Sundaram, P. S., Basker, N., & Natrayan, L. (2019): Smart clothes with bio-sensors for ECG monitoring. *International Journal of Advanced Technology and Engineering Exploration*, 8, 298–301. ISSN: 2278-3075. Retrieved: 22. September 2022, from https://www.researchgate.net/profile/Natrayan-L/publication/331331285_Smart_clothes_with_bio-sensors_for_ECG_monitoring/links/5cb8981fa6fdcc1d499ee3ff/Smart-clothes-with-bio-sensors-for-ECG-monitoring.pdf
- Tao, X. M. (2001): Smart technology for textiles and clothing – An overview and review. *Smart Fibres, Fabrics and Clothing*, 2-3. ISBN: 0-8493-1172-1. Retrieved: 8. September 2022, from http://textilelibrary.weebly.com/uploads/1/1/7/4/11749432/smart_fibres_fabrics_and_clothing_xiaoming_tao_2001.pdf
- Wilson, P., & Teverovsky, J. (2012). New product development for e-textiles: Experiences from the forefront of a new industry. In L. Horne (Hrsg.), *New Product Development in Textiles*. Woodhead Publishing, 156–174. DOI: <https://doi.org/10.1533/9780857095190.2.156>
- Ziccardi, G. (2020). Wearable Technologies and Smart Clothes in the Fashion Business: Some Issues Concerning Cybersecurity and Data Protection. *Laws*, 9, 1–13. DOI: <https://doi.org/10.3390/laws9020012>