sciendo

Timisoara Journal of Economics and Business TJE&B

A USER PERSPECTIVE ON THE VULNERABILITIES OF SMART WATCHES: IS SECURITY A CONCERN?

Daniela POPESCUL[1] , Mircea GEORGESCU[2]

DOI: 10.1515/tjeb-2017-0009

Nowadays, we are witnessing a serious gain in popularity of the wearable smart things. A triumphalist language referring to their benefits can be noticed in mass media, revealing the hype in their adoption. Multiple advantages are perceived by the consumers, and work as positive drivers in the wearables market. Yet, there is little awareness regarding their privacy and security – such concerns are constantly expressed by academia, but usually ignored by buyers and manufacturers. Therefore, the purpose of this paper is to provide some preliminary insights into how do the users perceive vulnerabilities as interferences, frequent disconnections, hardware and software malfunctions, improper/difficult configuration etc. of hand worn devices. The analysis was realized by means of netnography, using emag.ro, the oldest and largest ecommerce site in Romania as online source. Inspired by a similar study conducted by (Genaro Motti & Caine, 2016), we selected and reviewed 931 comments posted by the buyers of the ten most popular smart watches, in order to identify the hardware, software and connectivity problems they faced while using the devices and to assess the awareness of the buyers to security and privacy issues. Also, an overview of the privacy and security policies published by selected smart watches' manufactures was made, and some conclusion regarding the recommended future actions for wearable buyers, sellers and manufacturers were presented.

Keywords: **Wearables, Smart things, Smart watches, Wearables data privacy, Wearables security**

JEL Classification: **M15, O3**

[1] *Associate Professor PhD, "Al. I. Cuza" University of Iasi, Romania*

[2] *Professor PhD, "Al. I. Cuza" University of Iasi, Romania*

1. Introduction

Wearable technology integrates various devices with clothing and human body (Hughes, 2014), promising a seamless experience characterized by convenience, efficiency, safety and health improvement for its users. There is no effort in wearing the smart devices, which blend unobtrusively in everyday life. The benefits they are offering to individuals consist of always on/always accessible information, hands-free operation, and comfortable integration in day-to-day activities (Madakam, 2015). Regarding the wearables taxonomy, (marketsandmarkets.com, 2017) propose segmentations by product (wrist wear, headwear/eyewear, footwear, neckwear, body wear), type (smart textile, non-textile), application (consumer electronics, healthcare, enterprise & industrial), and geography. Many examples of successful implementations are available. (Emrich, 2017) and (Poladian, 2017) present the MagicBand, a $1 billion investment used by Disney theme park goers to enter rides, buy goods, enter hotel rooms and personalize the Disney experience, glasses transformed in enterprise tools by DHL and Boeing, or personal data serving as a differentiator for selling shoes. (Thierer, 2015) synthesizes some very daring uses of wearable technology, in complex procedures performed by surgeons, immediate diagnose and treatment in ambulances, firefighting, law enforcement, financial services and electoral campaigns. Also, (Tomico & Wilde, 2016) present "diverse and subtle ways" in which soft textiles engage with wearers' senses. The hype in adoption is not yet faded by privacy and security concerns, even if vulnerabilities, threats and third-party attacks were largely presented by literature. In this spirit, we consider that the assessment of users' awareness regarding the security flaws of wearables is mandatory, as a first step in the adoption of security and privacy protections by manufacturers, sellers and legislators.

2. Literature review

Wearables smart things are Web-connected miniaturized computers that have the capability to collect (usually through sensors), store, process and transmit data about the user, his/her behavior and physical surroundings. According to (Madakam, 2015), wearables execute multiple, possibly concurrent, applications, and support different degrees of mobility and customization. People own, wear, operate and configure them for various purposes, like monitoring their body functions during sport activities, sharing the collected data to friends in social networks, and accessing multimedia files or just because they feel that head-mounted, body-dressed, hand- or foot-worn electronics are fashionable and entertaining. (Bauer, Wutzke, & Bauernhanls, 2016) show that wearables are producing and communicating a wide variety of data ranging from structured data like number of steps taken, distance travelled, speed and pace, calories burnt, heart rate, skin temperature, perspiration level, hours slept, dietary information accelerometer values to unstructured voice or video recordings. They are able to detect users and the social connections between them, access user's data, infer social context according to user's network topology, preferences and features, identify social goals according to the social context and the user model, coordinate their behavior and provide a context driven output (Biamino, 2012). (De Arriba-Pérez, Caeiro-Rodríguez, & Santos-Gago, 2016) compiled their own list of sensors in wearables, ordered by the frequency of appearances: accelerometer (82%), heart rate (33%), GPS (27%), gyroscope (26%), compass (18%), microphone (17%), ambient light (11%), barometer (6%), altimeter (6%), camera (5%), thermometer (1%) etc., and warned that these sensors provide continuous data about vital signs (e.g., heart rate, skin temperature) and environmental variables (e.g., movements) that can be used for many different purposes. They detect human features – sleep habits, stress – and activities like walking, writing, drinking coffee, giving a talk, etc., being able to put them in the appropriate context.

Smart watches are characterized by one of the greatest adoption rate among the wearables and are deemed by the market researchers as the future of consumer electronics. IDC, for example, stated in June 2017 it expects smart watch shipments to increase from 71.4 million units in 2017 to 161 million units in 2021 (Haselton, 2017). According to Allied Market Research, the global market has a potential to reach $32.9 billion by 2020 (Allied Market Research, 2017). Starting with the assumption that the success or failure of a technology is determined by the interaction of inventors and consumers (Thierer, 2015), we notice an analysis of the patents stored in Thomson Innovation database, made by (Dehghani & Dangelico, 2017), which presents an impressive evolution of patents granted for smart watches between 2011 and 2015: their number increased from 3 to 355, and the share of patents for smart watches in the total of smart wearables analyzed was of 50.56% (followed by smart glasses with 18.15%, smart clothes with almost 10%, smart textiles with 7.17%; all the others had shares below 5%).Smart watches were highly accepted by the consumers due to their similarity both to traditional watches and smart phones, their small size and light weight. The interaction with a smart watch is intuitive, and its multiple functions not only complement, but also supplement the connected smart phone. Smart watches users particularly enjoy their visual appeal (design and aesthetics), the smooth integration with body and smartphone, the easy customization and relatively simple set up, the overall comfort of wearing the device and its positive interferences with daily behavior or activities, battery durability, accuracy and reliability of collected and calculated data, performance, quality/robustness and high degree of resistance to wear and tear (Coorevits & Coenen, 2016). But, as any commodity devices in their early phase of use, there is an instable equilibrium between enjoyment and irritation – problems as instable connections with the paired phone, difficult configuration, and breakable bracelets are mentioned in different studies.

Interesting is that, among these problems, no concerns regarding the privacy and security of personal data and information were signaled by the users in this first phase of smart watch adoption. Academic literature and companies studies present vulnerabilities as unsecured data deluges, no legal framework to require manufacturers to adopt good and transparent security and privacy protection measures, no secure protocols such as https, privacy issues, lack of transport encryption, insecure Web interface, inadequate software protection, and insufficient authorization. (Williams, 2015) and (Thierer, 2015) present that a lot of personal info are collected by smart watches, information which is often sold and/or used to a ddress users with targeted advertising or marketing, and it's often not made clear to consumers how exactly the information will be used or what third parties (employers, banks, insurance companies?) could gain with access to that data. Proprietary and non-proprietary systems such as services, apps for smartphones and wearables, and programs for computers can be developed and maintained by external entities to provide specific functionalities (De Arriba-Pérez, Caeiro-Rodríguez, & Santos-Gago, 2016), but they are also involved in rich data collection scenarios that can be potentially dangerous (Guo & Ma, 2017). (Olson, 2016) shows that, in 2014, data from a Fitbit fitness tracker was admitted as evidence in a personal injury lawsuit. The attack surface associated with wearable devices is an extended one, due to frequent and long-time use. Bluetooth-related attacks like bluejacking (spamming nearby users with unsolicited messages), bluesnarfing (stealing the contact information found on vulnerable devices), bluebugging (accessing device commands without notifying or alerting the phone's user; the hacker can initiate phone calls, send and receive text messages, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet), various ways of exploiting motion sensors for keystrokes inference (touchlogging and keylogging) were demonstrated. It is true that. even if they were proven by academic literature, such attacks remain highly improbable in the life of an ordinary user, but it is also certain that we still can identify a serious range of threats associated with hand-worn devices, e.g. interferences, frequent disconnections, hardware and software malfunctions, improper/difficult configuration of the devices, which lead to weak authentication/other faulty security mechanisms, threats caused by natural factors (e. g. extremely high or low temperatures, excessive humidity or an excessively dusty environment which, in time, can determine devices to break down). As many wearables devices include an embedded OS that enables the installation of third-party applications and functionalities similar to the ones available in smartphones, and the paired smartphone works as a gateway collecting and transmitting data, it is also relevant to analyze the software-associated security problems.

Our research question, based on the above formulated elements, is related to the extent in which users are aware of the privacy and security concerns related to wearables use. es.

3. Methodology

In order to identify, analyze and understand the problems faced by the consumers when using wrist worn wearables, we collected 931 critical reviews posted on emag.ro (the largest and oldest e-commerce site in Romania) by smart watches buyers. Smart watches were selected mainly due to their popularity on Romanian market, and we benefited from the tech-savvy profile of the consumers. The comments referred to 10 most popular smart watches from a total of 667, in descending ordered by the reviews number. The sample included various brands (Samsung, Apple, Vector, Huawei, E-Boda, Evolio), with prices varying from 16 to 510 EUR, and review numbers between 55 and 197. During data analysis, we combined a qualitative approach (coding the user concerns which could be considered threats from the security/privacy point of view) and a quantitative interpretation (frequencies of occurrences). We read individually each comment and eliminated all the aspects considered irrelevant to our objective. When a vulnerability/potential threat was noticed in a comment, we manually extracted it from the website and transferred it to an Excel spreadsheet, where it was individually coded. Codes referred to vulnerabilities types (hardware, software, and communication-related) and to the severity of the problem identified by the user (low, medium, and high). We aggregated the comments based on their similarity and classified them in order to identify the most frequent occurrences. Based on the users' comments, we identified a set of major vulnerabilities/threats associated to the smart watches use, which can determine serious security flaws. For the purpose or this paper, information security is defined as the set of processes adopted by an organization in order maintain the confidentiality, integrity and availability of data (Oprea, 2007). The analyses of the users' feedback led to a discussion about the causes and severity of those problems, and also to the definition of a set of security measures aimed at securing the user interaction with smart watches.

4. Results and Discussions

The analyzed smart watches, with their general and technical features are presented in tables 1 and 2.

Table 1. Smart watches analyzed during the study - general features.

Code	Name	Price (RON)	Rating (max 5)	Reviews	Average Battery Life	Compatible OS
SW1	Vector Luna	1499.00	4.59	208	30 days	iOS 8.0+, Android 4.4+, Windows 10+
SW2	E-Boda Smart Time 100	69.00	4.01	154	n/a	Android, iOS
SW3	Huawei Watch W1	1099.99	4.69	103	1,5 days	iOS 8.2+, Android 4.3+
SW4	E-Boda Smart Time 300	199.99	3.91	79	n/a	Android 4.4+, iOS 7.0+
SW5	Evolio x-watch PRO	199.99	3.54	75	n/a	Android, iOS
SW6	E-boda Smart Time 210	69.00	4.00	73	n/a	Android, iOS
SW7	Apple Watch 1	1589.99	4.72	67	18 hours	iOS
SW8	IMK DZ09 PLUS	119.00	3.66	64	n/a	Android < 5.0.2
SW9	Samsung Gear S3	1549.99	4.70	63	n/a	Android, iOS
SW10	Vonino KidsWatch S2	317.00	3.54	45	2 days	Android, iOS

Source: www.emag.ro, data collected in March and April 2017

Table 2. Smart watches analyzed during the study - technical features.

Code	Smartphone Sync Method	Sensors	On Watch Notifications	Activity Tracking
SW1	BLE (Bluetooth Low Energy)	Accelerometer, Gyroscope, Ambient Light Sensor	Incoming Call, Text Message, E-mail, Calendar Reminder, Alarm, Timer, Stopwatch, Link Loss Alert, Weather	Steps, Calories, Distance, Sleep
SW2	Bluetooth 3.0	Pedometer	Incoming Call, Text Message	Steps, Distance
SW3	Bluetooth 4.1 (BLE), Wi-Fi	Gyroscope, Accelerometer, Heart Rate, Barometer	Incoming Call, Text Messages, E-mail, Calendar Reminder, Alarm, Lists	Steps, Distance, Movement Type (walking, running or climbing)
SW4	Bluetooth 3.0	Pedometer	Incoming Call, Text Message	Steps, Distance, Sleep
SW5	Bluetooth 4.0	Pedometer	Incoming Call, Text Messages, E-mail, Facebook, Twitter, WhatsApp, Skype	Steps, Sleep
SW6	Bluetooth 3.0	Pedometer	Incoming Call, Text Message	Steps, Distance, Sleep
SW7	Bluetooth 4.0, Wi-Fi	Heart Rate, Accelerometer, Gyroscope, Light	Incoming Call, Text Messages, E-mail, Calendar Reminder, Alarm, Lists	Steps, Distance, Sleep
SW8	Bluetooth, micro USB	Accelerometer, Gyroscope, Barometer, Heart Rate Sensor	Incoming Call, Text Messages, E-mail, Calendar Reminder, Alarm, Phone Tracker	Steps, Distance, Sleep
SW9	Bluetooth 4.2, Wi-Fi, NFC, GPS	Accelerometer, Gyroscope, Barometer, Heart Rate Sensor	Incoming Call, Text Messages, E-mail, Calendar Reminder, Alarm, Lists	Steps, Distance, Heart Rate
SW10	GPS	GPS tracking	Acts as a phone	Distance

After analyzing the 931 comments, the user opinions that can be seen as problems/ possible security vulnerabilities were grouped in categories, based on their type (hardware, software, connectivity with the network/paired smartphone) and their severity (low, medium, and high). The problems were coded as show in table 3.

Table 3. Hardware, software and connectivity smart watches' problems identified during the study.

	Low	Medium	High
Hardware	HL1. Non-uniform screen brightness HL2. Poor screen resolution HL3. Missing sensors, compared to expectations	HM1. Low battery life HM2. Imprecise sensors HM3. Insufficient memory HM4. Bad sound HM5. Improper functioning of camera HM6. Fragile wake/power button HM7. Poor contact with the power cord HM8. Problems with the screen (screen is unclear, direct light affects visibility, screen came off etc.)	HH1. Faulty/nonfunctional microphone HH2. Faulty/nonfunctional battery HH3. Faulty/nonfunctional camera HH4. Faulty/nonfunctional touch screen HH5. Completely broken in 1 week/1/2/3 months HH6. Faulty/nonfunctional speakers HH7. Various malfunctions provoked by low temperatures HH8. Resets caused by wrist perspiration HH9. Non-responsive buttons
Software	SL1. Difficulties in using the menu SL2. The software is hard to learn SL3. Lags in executing tasks SL4. Imprecise wake-up gesture feature	SM1. Operating system dependency SM2. Notifications don't function as expected SM3. Difficult updates SM4. Problems when installing new apps SM5. Bad synchronization with the phone apps SM6. Low utility software SM7. Slow apps SM8. Touchscreen lags SM9. Rare phone disconnections (once in 3-4 days)	SH1. Nonfunctional apps SH2. Frequent crashes, impossible/difficult navigation SH3. Impossible reset after a crash SH4. Impossible browser installation SH5. Sudden/inexplicable reset to factory settings SH6. Smart watch starts calls by its own
Communication	CL1. Rare but causeless disconnections CL2. Fragile/unstable phone connection CL3. Lost connection during the call	CM1. When disconnected, it consumes the battery very fast CM2. Interrupted calls CM3. No Wi-Fi connection CM4. No Bluetooth headset connection CM5. SMS reading is not possible CM6. Imprecise location CM7. Weak GSM signal	CH1. Difficult/impossible phone connection CH2. Frequent disconnections CH3. Lost GSM signal - in order to make it functional again, battery must be removed CH4. No SIM recognition

The calculated frequencies of appearance of a specific problem for each analyzed smart watch are presented in tables 4, 5, and 6.

Table 4. Frequencies of hardware problems identified during the study.

Hardware problems	SW1	SW2	SW3	SW4	SW5	SW6	SW7	SW8	SW9	SW10
HL1. Non-uniform screen brightness	2.88%	-	-	-	-	-	-	-	-	-
HL2. Poor screen resolution	2.88%	3.37%	-	-	-	-	-	-	-	-
HL3. Missing sensors, compared to expectations	-	-	2.40%	-	-	-	-	-	-	-
HM1. Low battery life	-	4.33%	3.37%	0.96%	3.37%	2.88%	-	0.48%	0.48%	6.25%
HM2. Imprecise sensors	1.44%	-	-	0.48%	-	1.92%	-	0.48%	-	-
HM3. Insufficient memory	0.48%	-	-	-	-	-	-	-	-	-
HM4. Bad sound	-	1.92%	-	-	-	-	-	-	-	-
HM5. Improper functioning of camera	-	-	-	0.48%	-	-	-	-	-	-
HM6. Fragile wake/power button	-	-	-	1.92%	-	-	-	-	-	-
HM7. Poor contact with the power cord	-	-	-	-	-	2.40%	-	-	-	2.88%
HM8. Problems with the screen	-	0.48%	-	-	-	-	-	-	-	-
HH1. Faulty/nonfunctional microphone	-	0.48%	-	-	-	-	-	-	-	-
HH2. Faulty/nonfunctional battery	-	-	-	0.48%	0.48%	-	-	0.96%	-	-
HH3. Faulty/nonfunctional camera	-	0.96%	-	-	-	1.44%	-	0.96%	-	-
HH4. Faulty/nonfunctional touch screen	-	-	-	-	0.48%	-	-	0.48%	-	-
HH5. Completely broken in 1 week/1/2/3 months	-	-	-	-	0.48%	0.48%	-	0.48%	-	1.92%
HH6. Faulty speakers	-	-	-	-	-	-	-	-	-	0.48%
HH7. Malfunctions provoked by low temperatures	-	0.48%	-	-	-	-	-	-	-	-
HH8. Resets caused by perspiration	-	0.48%	-	-	-	-	-	-	-	-
HH9. Non-responsive buttons	-	-	-	-	0.48%	-	-	-	-	-

Table 5. Frequencies of software problems identified during the study.

Software problems	SW1	SW2	SW3	SW4	SW5	SW6	SW7	SW8	SW9	SW10
SL1. Difficulties in using the menu	-	0.96%	0.48%	-	-	-	-	-	0.48%	-
SL2. The software is hard to learn	-	-	0.48%	0.48%	-	0.96%	-	-	0.48%	-
SL3. Lags in executing tasks	-	-	-	-	-	-	-	-	0.96%	-
SL4. Imprecise wake-up gesture feature	-	-	0.48%	-	-	-	-	-	-	-
SM1. Operating system dependency	0.96%	-	-	-	1.92%	-	-	0.48%	-	-
SM2. „Missing" and non-accurate notifications	1.44%	0.96%	0.48%	-	2.88%	0.96%	-	0.96%	2.40%	-
SM3. Difficult update	0.48%	-	-	-	-	-	-	-	-	-
SM4. Problems when installing new apps	-	-	-	-	-	0.48%	-	-	-	4.33%
SM5. Faulty synchronization with the phone apps	-	0.48%	2.40%	0.48%	0.48%	0.48%	-	-	-	0.48%
SM6. Low utility software	0.48%	-	-	-	-	-	-	-	-	-
SM7. Slow apps	-	-	-	0.96%	-	-	-	-	-	-
SM8. Touchscreen lags	-	-	-	-	1.44%	-	-	-	-	-
SH1. Nonfunctional apps	0.48%	-	0.48%	0.96%	-	0.96%	-	1.92%	-	-
SH2. Frequent crashes, impossible/difficult navigation	-	-	-	0.96%	-	-	-	-	-	0.48%
SH3. Impossible reset after a crash	-	-	-	0.96%	-	-	-	-	-	-
SH4. Impossible browser installation	-	-	-	-	-	-	-	0.96%	-	-
SH5. Sudden reset to factory settings	-	-	-	0.48%	0.48%	-	-	-	-	-
SH6.SW started calls by its own	-	-	-	-	-	-	-	-	-	0.48%

Table 6. Frequencies of communication software problems identified during the study.

Connectivity problems	SW1	SW2	SW3	SW4	SW5	SW6	SW7	SW8	SW9	SW10
CL1. Rare but causeless disconnections	-	-	1.92%	-	-	-	-	-	-	-
CL2. Fragile phone connection	-	-	1.92%	-	0.48%	-	-	-	-	-
CL3. Lost connection during the call	-	-	-	-	-	-	0.48%	-	-	-
CM1. Rare phone disconnections (once in 3-4 days)	-	1.44%	1.92%	-	0.48%	-	-	-	-	-
CM2. When disconnected, it consumes hardly the battery	-	-	0.48%	-	-	-	-	-	-	-
CM3. Interrupted calls	-	1.44%	-	1.92%	1.44%	-	-	0.48%	-	-
CM4. No Wi-Fi connection	-	-	-	0.48%	-	-	-	-	-	-
CM5. No Bluetooth headset connection	-	-	-	-	0.96%	-	-	-	-	-
CM6. SMS reading is not possible	-	-	-	-	1.44%	-	-	-	-	-
CM7. Imprecise location	-	-	-	-	-	-	-	-	-	15.38%
CM8. Weak GSM signal	-	-	-	-	-	-	-	0.48%	0.48%	0.96%
CH1. Difficult/impossible phone connection	3.37%	2.40%	0.48%	0.48%	-	-	-	0.48%	-	-
CH2. Frequent disconnections	-	1.44%	-	-	-	-	-	1.44%	-	1.44%
CH3. Lost GSM signal - in order to make it functional again, battery must be removed	-	-	-	-	0.48%	-	-	-	-	-
CH4. No SIM recognition	-	-	-	-	-	-	-	0.48%	-	1.44%

As can be seen in the tables above, a large variety of problems were identified by customers who have bought smart watches from emag.ro. In the hardware "zone", the most frequent reasons for dissatisfaction were related to the poor/bad quality of battery (the lifetime was appreciated as unsatisfactory for 8 smart watches out of 10, and for 3 devices there were occurrences of faulty or completely nonfunctional battery), the imprecision of sensors, and the low brightness and resolution of screens. Users mentioned that if the smart watch is used regularly to send messages, play games on apps, and chat on the phone, most likely the life span of the phone will be decreased as well. Other parts mentioned by users were cameras, wake/power buttons, power cord, speakers and microphone. The short life time of the entire device was a serious problem (some items were completely broken after up to three months of use). External factors as low temperatures and hand/wrist perspiration were identified as harmful. The most common software problems were the difficult synchronization with the paired smart phone applications, failures in applications' functionality, missing or non-accurate notifications, hard-to-learn software and hard-to-use menus. Regarding the communication with the paired smart phone through Bluetooth or with the mobile network in the case of GSM-able smart watched, the users were unpleased by bad, difficult or even impossible connection. All these problems can be seen as potential threats to the integrity and availability of the information stored/transmitted by smart watches, even if they are not recognized per se by the users.

This very little awareness about potential security problems among the users is, in our opinion, a real concern – no mention about data/security flaws was present in the whole 931 comments we have analyzed. More than that, on the other side of the story, even if the surveillance capabilities of smart watches are not comparable with those associated with Google Glass or Narrative clip-on camera, 5 users' reviews praised this "functionality": the possibility to use smart watches to cheat on exams was mentioned in 5 reviews.

This little-to-no awareness may be a consequence to the improbability of theft/loss or malware attacks in case of wrist worn wearable, but also to the complete absence of terms and conditions regarding data privacy and security when using smart watches on emag.ro website. Searching for this information on the websites of the manufacturers, we have identified privacy statements for Vector, Huawei, Apple and Samsung – relevant information is presented in table 7. For E-Boda and Evolio smart watches, confidentiality policies are available only in Romanian language and cover through their statements only the use of the website and the electronic payment system. No information about data collected, stored, processed during smart watches use is provided. No security or privacy policy for IMK DZ09 Plus and Vonino Kids watches could be identified.

Table 7. Privacy statements for Vector, Huawei, Apple and Samsung smart watches.

SW1, Vector Luna, http://vectorwatch.com/data-privacy-statement		
Purposes for data use	**Data collected**	**Adopted security measures**
Analysis of the accuracy, effectiveness, usability, or popularity of the services; Support, improved services, or new services; Personalized content, marketing e-mails, push notifications about Vector Watch products, software updates, and third-party products, software, and other services; Reports and data about the user base and service usage patterns; Update of the third party applications downloaded to the smart watch; Disclosure of personal information when required by law etc.	**Identification data**: name, username, password, email address, postal address, phone number, mobile phone number, payment information, device model and serial number; **User generated content and information posted during the use of social networks or mobile apps**: photos, texts, email address, biometrics: age, weight, height, gender, feedback etc.; **Any other information sent to Vector Watch** while requesting certain features (e.g., newsletters, updates, and other products), contacting customer support, applying for a job, entering contests or promotions campaigns, participating in blogs or online forums, using Vector Watch developer apps or developer blogs; **Automatically collected data**: proprietary features and third-party apps used, log files, buttons pressed, and support requests and results, device ID, device serial number, search queries, watch faces, streams and apps downloaded or stored; **Precise geolocation information**, if activated by user: i.e., real-time geographic location.	Reasonable technical and organizational precautions to prevent the loss, misuse or alteration of the information collected; Storage of the personal information on Vector's secure servers; Encryption of data in transit through the website ("information relating to electronic transactions entered into via this website or in the mobile apps is encrypted").
SW3, Huawei Watch W1, http://consumer.huawei.com/nz/legal/privacy-policy/		
Purposes for data use	**Data collected**	**Adopted security measures**
Fulfillment of purchase orders delivery, activation, or verification of products or services, changes upon user request; and technical support; Contact with the user and delivery of marketing information, only after an explicit consent; Informing the user about operating system or application updates and install them. Personalized user experience, delivery of personalized content activation of after-sale services; Internal audits, data analysis and research, for the improvement of products and services; Analysis of the efficiency of business operations and measurement of market share; Errors troubleshooting, improvement of loss prevention and anti-fraud programs etc.	**Identification data:** name, profile picture, phone number, email address, age and location; **Data submitted directly by the user**: product information, time of purchase and method of payment; **Friends' data**: contact information, including name, profile picture, phone number and email address (if content is shared with friends through HUAWEI services); **Service use data:** device name, system and application versions, regional and language settings, device version, device identification number (IMEI, ESN, MEID and SN), **geographic location** (the ID of the area where the device is located), service provider network ID (PLMN), usage habits and IP address, service access times, search query terms and the data stored in cookies on devices; **Third party data**: data about user from publicly and commercially available sources as permitted by law, including social networking sites as Facebook or Twitter; **Non-identifiable data:** aggregated statistics.	Industry-standard practices to safeguard personal data against unauthorized access, disclosure, use, modification, damage or loss; All reasonably practicable steps to protect personal data; Encryption to ensure data confidentiality; Trusted protection mechanisms to protect data from malicious attacks; Visit control mechanisms to ensure only authorized personnel can access personal data; Training sessions to raise awareness among employees; Collection of only relevant personal data.

SW7, Apple Watch, https://www.apple.com/privacy/approach-to-privacy/		
Purposes for data use	**Data collected**	**Adopted security measures**
Improvement of services without compromising individual privacy; Increasing the effectiveness of health and fitness feature; Payment data are used only to help Apple improve Apple Pay and other Apple products and services, no purchase history can be built and no personalized ads are generated.	**Data shown in the Health and Activity apps:** movement measurements, other installed fitness apps, the approximate location of the user, and how long Apple Watch has been used. This data does **not include personally identifiable information;** **Analytics about iOS device and any paired Apple Watch:** e. g. details about hardware and operating system specifications, performance statistics, and data about the use of devices and applications; **User generated content:** photos, documents, reminders, calendars, contacts, iCloud keychain, backup, bookmarks, reminders, find my iPhone, find my friends, notes, mail (encrypted in transit), notes; **Payment data**: the approximate time, location, and amount of the transaction.	Data stored by the user in Health app are encrypted if the phone is locked with a passcode, Touch ID or Face ID. Any data backed up to iCloud is encrypted both in transit and on Apple servers; Related third parties are required to provide a privacy policy for the user; When it's collected, personal data is either not logged at all, is removed from reports before they're sent to Apple, or protected by techniques such as Differential Privacy.
SW9, Samsung Gear S3, https://www.samsung.com/us/account/privacy-policy/		
Purposes for data use	**Data collected**	**Adopted security measures**
Registering the user/device for a service; Providing the user the requested functionalities and features, but also customized content, personalized services based on his/her past activities and advertising; Assessment and analysis of market, customers, products, and services; Understanding the way customers use the services, in order to improve them and to launch new products/services, providing maintenance, service, support; Free prize draws, prize competitions or promotions, as permitted by law; Otherwise with the user consent. Information may be shared with: affiliates (the Samsung family of companies), business partners (trusted companies that may provide information about products and services users might like), service providers (companies that provide services for or on behalf of Samsung), law enforcement.	**Identification data**: name and email address, contact information, shipping and billing address(es), and credit card information; **Automatically collected information about the use of services**: device information - such as hardware model, IMEI number and other unique device identifiers, MAC address, IP address, operating system versions, and settings of the devices; log information - time and duration of the service, search query terms entered through the services, and any information stored in cookies stored by Samsung on the devices; **Location information**: user device's GPS signal, information about nearby Wi-Fi access points and cell towers; Voice information: recordings of user voice made and stored on Samsung's servers when voice commands are used (shared with 3rd parties); **Other information:** used apps, visited websites, user interact with content offered through a service; **Information obtained from third-party sources:** information about the mobile device (IP address, OS version, regional and language settings, and IMEIs and other unique device identifiers), how, when and for how long the mobile device is used.	Reasonable physical and technical measures to safeguard the information collected in connection with the services.

It could be noticed that the amount and variety of data collected is impressive, and the purposes of use and approaches of security measures vary depending on manufacturer. While Apple philosophy of giving the user all the confidentiality needed, through strong encryption and Differential Privacy, is visible also in the privacy terms for Apple smart watches, the other manufactures' statements are not so … user-friendly: in some cases, data may be transferred to and from third parties, and the adopted security measures are not clearly specified.

Conclusions

Smart wearables are soon to be worn everywhere and by everyone. Connected to other devices in the ubiquitous IoT, they will be used in a wide range of domains, such as medical and healthcare, transportation, home and building automation, service and manufacturing sector, etc. This greatest growth potential can generate strange scenarios in which user privacy is affected. In order for the manufacturers to build solid trust among the users of smart watches, not only the above-reported problems must be addressed with emergency. In our study, we identified that users complain about various hardware, software and communication technical faults. These problems are going to be solved in a natural way with the advancement of technology and maturity of the market. On the other hand, the producers do not experience the same pressure regarding the lack of security features of smart watches. The significant amount of data collected by each smart watch, which is added to the contemporary data deluge and certainly used in business intelligence and consumer marketing, seem to be ignored by the customers, who are data blind – they lack the ability to know whether, when and where their data is used. In this conditions, secure design and development of hardware, software and communication solutions is mandatory - security methods should be built into the equipment and network at the very beginning of the process, and not after its implementation. The design and manufacturing processes must be open and transparent, and users should be clearly informed about the security of using the devices, through easy-to-understand policies. After adaptation and adoption of classical security methods as encryption, identity management techniques, device authentication mechanisms, digital certificates, digital signatures and watermarking, consistent feedback should be required from the users in a coherent way; and consumers' opinion must be taken into consideration when devices/networks are redesigned.

While authors like (Thierer, 2015) affirm that there is no need for prophylactic measures on the use of smart wearables, and that precautionary principles should be left away and the default position toward these technologies should be "innovation allowed" or "permissionless innovation", we consider that, on the background of little-to-none security awareness of the user, an intervention through stronger policies is needed because in time privacy and security issues may become harder to address. The industry should adjust itself to the privacy and security concerns. Also, a distinction must be made between consumers using commercial devices (in general for fitness or well-being) and patients using clinical devices. In the second case especially, manufactures have to address carefully the notions of information assets, vulnerabilities, trust, risk, security and privacy. The buyers have to be well and fair informed about all the problems related to wearables use, in a more active, visible and active manner – building habits of ignoring the importance of data stored and transferred through wearables use is and their privacy and security is not desirable.

The paper offers only a non-exhaustive review of hardware, software and connectivity problems attached to smart watches use, with the intention to raise the awareness in this area of large public interest. Further in-depth analyses for each vulnerability, attack scenario and adequate security measures are necessary.

References

Allied Market Research. (2017, May 9). Smartwatch Market is Expected to Reach $32.9 Billion, Globally, by 2020 - Allied Market Research. Retrieved from Nasdaq GlobeNewswire: https://globenewswire.com/news-release/2017/05/09/981125/0/en/Smartwatch-Market-is-Expected-to-Reach-32-9-Billion-Globally-by-2020-Allied-Market-Research.html

Bauer, D., Wutzke, R., & Bauernhanls, T. (2016). Wear@Work – A new approach for data acquisition using wearables. Procedia CIRP 50 (pp. 529 – 534). Elsevier B.V.

Beltramelli, T. (2015). Deep-Spying: Spying using Smartwatch and Deep Learning. Copenhagen, Denmark: IT University of Copenhagen.

Biamino, G. (2012). A Semantic Model for Socially Aware Objects. Advances in Internet of Things, 2(3), 47-55.

Coorevits, L., & Coenen, T. (2016). The Rise and Fall of Wearable Fitness Trackers . Academy of Management.

De Arriba-Pérez, F., Caeiro-Rodríguez, M., & Santos-Gago, J. M. (2016, September 21). Collection and Processing of Data from Wrist Wearables Devices in Heterogeneous and Multiple-User Scenarios. Sensors, 16(1538), 1-31.

Dehghani, M., & Dangelico, R. M. (2017). Smart wearable technologies: Current status and market orientation through a patent analysis. In IEEE (Ed.), Conference on Industrial Technology (ICIT). Toronto.

Emrich, T. (2017, February 9). 12 wearables predictions for 2017. Retrieved April 3, 2017, from betakit.com: http://betakit.com/12-wearables-predictions-for-2017/

Genaro Motti, V., & Caine, K. (2016). Smart Wearables or Dumb Wearables? Understanding how Context Impacts the UX in Wrist Worn Interaction. SIGDOC '16 Proceedings of the 34th ACM International Conference on the Design of Communication (pp. 1-10). Silver Spring, MD, USA : ACM.

Guo, A., & Ma, J. (2017, February 8). Context-Aware Scheduling in Personal Data Collection From Multiple Wearable Devices. (IEEE, Ed.) IEEE Access, 5, 2169-3536.

Haselton, T. (2017, June 21). Smart clothing and smartwatches will help double wearable market by 2021: IDC. Retrieved from CNBC: https://www.cnbc.com/2017/06/21/idc-wearables-market-to-double-by-2021.html

Hughes, A. (2014). Threat assessment of wearable technology . Ann Arbor : ProQuest.

Kim, K. J., & Shin, D.-H. (2015). An acceptance model for smart watches Implications for the adoption of future wearable technology. Internet Research, 25(4), 527 - 541.

Kolamunna, H., Chauhan, J., Hu, Y., Perino, D., Thilakarathna, K., Makaroff, D., & Seneviratne, A. (2015, August). Are wearable devices ready for HTTPS?Measuring the cost of secure communication protocols onwearable devices. Retrieved from http://www.cornell.edu/: https://arxiv.org/abs/1608.04180

Lee, L. N., Egelman, S., Lee, J. H., & Wagner, D. (2015, April 22). Risk Perceptions for Wearable Devices. Retrieved from https://arxiv.org: https://arxiv.org/pdf/1504.05694v1.pdf

Madakam, S. (2015, August). Internet of Things: Smart Things. International Journal of Future Computer and Communication, 4(4), 250-253.

marketsandmarkets.com. (2017). Wearable Technology Market by Product (Wristwear, Headwear/Eyewear, Footwear, Neckwear, Bodywear), Type (Smart Textile, Non-Textile), Application (Consumer Electronics, Healthcare, Enterprise & Industrial), and Geography - Global Forecast to 2022.

Mittelstadt, B. (2017, July 04). Ethics of the health-related internet of things: a narrative review. Ethics and Information Technology.

Olson, P. (2016, November 16). Fitbit Data Now Being Used in the Courtroom. Retrieved January 11, 2017, from Forbes Tech: http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-datacourt-room-personal-injury-claim

Oprea, D. (2007). Protectia si securitatea informatiilor. Iasi: Polirom.

Poladian, C. (2017, February 23). 5 New Marketing Trends Brought to Us Via Wearables: 2017 Edition. Retrieved from skyword.com: https://www.skyword.com/contentstandard/creativity/5-new-marketing-trends-brought-to-us-via-wearables-2017-edition/

Thierer, A. D. (2015). The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation. Richmond Journal of Law & Technology, XXI(2). Retrieved from http://jolt.richmond.edu/jolt-archive/v21i2/article6.pdf

Tomico, O., & Wilde, D. (2016). Soft, embodied, situated & connected: enriching interaction with soft wearables. The Journal of Mobile User Experience, 5(3), 1-17.

Williams, J. L. (2015). Privacy in the Age of the Internet of Things. Human Rights, 14-16.