

Could wearable technology transform the traditional concept of *habeas corpus*?

By Elena Falletti, Università Carlo Cattaneo, Castellanza, Italy

1. Introduction: Is privacy a right or a product?

The aim of this paper regards the analysis of privacy management of wearable devices (hereinafter “WD”) absorbing personal data from a user’s body and from his or her behaviour. There are many discussions on privacy, and WD privacy management is only one of them, while the main one is about what privacy is. Indeed, there are different opinions on managing the most individual private information. On the one hand, some people affirm that privacy, in an age of invasive electronic communication, should be a fundamental right. On the other hand, other views support that privacy has to be treated as an additional service that the user can buy if markets are interested in it. Indeed, the strict contact between the user’s body and the wearable device may give the impression that privacy is a “plus” service included with the WD product. However, privacy regards an individual fundamental right, and personal data collected through WD (or through other devices that are in close contact with user’s body and life) have to be strongly protected.

This paper is organized as follows: 1. it analyzes what WDs are and what the privacy issues are involved using them; 2. then, the paper briefly defines habeas corpus in an historical sense and its transformation into the concept of “habeas data”; 3. it shows some of the most sensitive cases of privacy protection using WDs; 4. the article compares the U. S. and E. U. legal perspective on these issues; 5. finally, it offers some concise conclusions.

2. What are “wearable devices”?

Wearable devices (WD) are a specific part of the general category of the “Internet of Things”. The term “Internet of Things” (IoT) references to infrastructure in which many sensors are designed to record, process, and store data locally, or interact with each other both in the medium range, through the use of radio frequency technologies (e.g. RFID, bluetooth, etc.), or through an electronic communications network. The devices involved are not only traditional computers or smartphones, but also daily life objects (“things”), such as wearable devices, home automation georeferencing, and assisted navigation objects. Indeed, the “Internet of Things” refers to a further development of the Internet resulting from physical objects networking. These objects may be equipped with a unique identifier (for example, a serial number), recognizable even by radio frequency. However, the identification of these objects could also be made without resorting to radio tags, but by combining sensors and automatic recognition procedures (for example, the recognition of a barcode carried out with a mobile phone connected to the Internet (M. Iaselli, 2015, 5). However, there is no universal definition of the “Internet of Things” (K. Rose, S. Eldridge, L. Chapin, 2015, 1) or wearable apps.

Scholars provide different kinds of definitions: “*Wearable technologies are networked devices that can collect data, track activities, and customize experiences to users' needs and desires*” (A. D. Thierer, 2015, 1); “*consumer devices are capable of monitoring sensitive vital sign information, and companies are readily collecting an inordinate amount of individual data. These devices are known as “wearables” and can monitor an individual's heart rate, stress level, brain activity, respiration, body temperature, hydration level, and other related information*” (M. R. Langley, 2015, 1642); “*Wearable Technology refers to items of clothing or accessories further improved by*

using electronics, intended for information or entertainment purposes. This type of technology is usually attached to the body and can be used to monitor information about users and their surroundings” (L. H., Segura Anaya, A., Abeer, N., Costadopoulos, P. W., Prasad, 2017, 1).

These definitions of wearable apps/devices have two points in common:

a) on the one hand WD, through IoT technologies, are able to record personal sensitive data of those who wear them. In fact, wearable devices have specific characteristics allowing these instruments to manage massive data storage (regarding big data issues as well), use minaturized computer and cameras, and use wireless communication capacity at lower and lower prices (A. D. Thierer, 2015, 6);

b) on the other hand, WD communicates such data to third parties. What are these “third parties”? They are wearable devices manufactures themselves, that collect and store users’ personal data, and private or public entities interested in them for commercial, political, health or other purposes. These purposes could involve some sensitive knowledge and business areas, for instance as suggested by some scholars: medicine (such as surgery, rehabilitation, emergency care, pharmaceuticals, chronic illness and so on), public safety (surveillance, anti-terrorism activities, firefighting, airlines checking, and so on), law enforcement, retailing, entertainment services, financial services, political campaign and sports (A. D. Thierer, 2015, cit.). Wearable devices could have a so wide range of applications that also science fiction could help imagining future developments, and now we only can make hypothesis on its future developments (A. D. Thierer, 2015, 32).

Analysts (L. Van Woense, G. Archer, 2015, 16) affirmed that one of the area of greatest development of wereable devices in future will cover everything that has to do with the massive collection of personal data, such as health care and labor context, both sensitive areas of discrimination. Indeed, research and development of WD could have positive effects especially for disabled and elderly people that could have impediment in movement, or in the patient-doctor relationship which could be more precise, and overcome embarrassment and shyness because the disease symptom description is delegated to these devices. However, some side-effects could emerge, especially in health care areas, such as the manifestation of informed consent of the patient or the re-emergence of medical paternalism which excludes the patient from treatment strategies concerning him or her. At the same time, using wearable devices in workplaces could improve workers’ performance through checking the effectiveness of their work method, especially in some exhausting jobs. However, some workers could feel these tools as invasive under their personal religious or cultural points of views. From these perspectives some ethical issues could rise, especially on the user’s awareness of which and how much of his or her personal sensitive data could be stored and, above all, transfert to third parties.

It could be wondered if a hypothetical (and unauthorized, thus unlawful) transfer of personal (and immaterial) data could be blocked (in a “physical” sense).

For instance, in American common law, the concept of privacy is linked to the idea of property and with the impassability of private, fenced land (Singleton 2000: 100). The unauthorized entry upon land is punishable under the tort of trespass. Prosecution of unauthorized electronic intrusion and the violation of online information systems, principally by American courts, has been defended using the concept of cybertrespass (Balganesh 2006: 278). Some scholars have criticized this doctrine, emphasizing that on the Internet there is no competition for resources, which is one of the requirements in the definition of trespass. A different opinion argues that Fourth Amendment of the

U.S. Constitution “*effects can include smart objects and related data that populate the Internet of Things*” (A. G. Ferguson, 2016, 809 ss). Indeed, the Fourth Amendment evolved beyond constitutional definitions: persons, houses, papers, and effects including wider things and concepts than in their original sense, so an "effect" would not only be the physical object but also the smart data and communicating signals emanating from the device (A. G. Ferguson, 2016, cit.).

But in my perspective, the main issue does not regard the competition for limited resources, but rather the safeguarding of massive personal data collection from illicit transfer and misuse. For these reasons, Google Glass, a work-in-progress WD once ubiquitous on Internet and main news media, was stopped due to both marketing failure and severe privacy concerns, “*with people afraid of being recorded during private moments*” (N. Bilton, 2015, E1; Id., 2013, 2013, B6).

In this sense, my view is closer to a wider interpretation of the Fourth Amendment than that of cybertrespass. However, in my European perspective I would try to adapt the traditional concept of *habeas corpus* to collection and storage of personal data.

3. Habeas corpus, habeas data and wereable devices:

Practically everybody has an idea of what habeas corpus is. Traditionally, the expression “Habeas Corpus” refers to the judicial determination of the legality of the detention of someone (B. Farrell, 2008, 551). The writ of habeas corpus was established in the XIII Century in English common law (W. F. Duker, 1980, 17) and subsequently this writ was transformed into a guarantee of personal liberty (B. Farrell, 2008, 553). However, at the beginning, it did not consist of a right, but of a privilege (P. D., Halliday, G. E., White, 2008, 593). As one of the king’s writs of command, it was founded on the royal prerogative and issued at the discretion of the justices sitting on the King’s Bench after a motion making a *prima face* case for issuance (P. D. Halliday, G. E. White, cit.). At its origins, habeas corpus was an issue about balancing power in protection of individual liberty (A. L. Tyler, 2016, 1956), specifically on wrongs committed by jailers on prisoners’ bodies (P. D. Halliday, 2012, 11). Through the writ of habeas corpus, that was a “*writ of prerogative*” the king “*demanding account for his subject who is restrained (deprived) of his liberty*” (P. D. Halliday, G. E. White, cit.; A. L. Tyler, cit.). Why did the king care about liberties and bodies of his subjects? Interpreting ancient case law, scholars answered that the king’s power to free them came from the need to command their bodies: “*Thus a writ concerned with moving, holding, and releasing bodies from imprisonment arose directly from this fundamental aspect of the king's prerogative*” (P. D. Halliday, G. E. White, cit.). In “modern” terms, it seems to be a manifestation of the mutual pact of care (from the king to his subjects) and obedience (of the subjects to the king), as an allegiance:

"the bond of allegiance is not a bond of servitude but of freedom: come liber homo." By giving allegiance to the person of the king, the person of the free subject was protected. Not only was his body protected, so too was what was thought of as his "inheritance." Inheritance did not mean only the ability to gain possessions from one's family. It meant something far greater: succession to the traditional privileges of a subject. Law was part of that inheritance because it helped protect subjects. In protecting law, partly through the use of the royal prerogative, the king protected the subject, just as the protected subject protected the king. To our eyes, this reasoning appears circular (P. D. Halliday, G. E. White, cit.).

Sir Edward Coke changed the nature of habeas corpus. In fact, it became a tool for correcting any "manner of misgovernment" (E. Coke, 1644, 4), during turbulent times "at the height of the Popish Plot when men seemingly were more interested in getting their fellow Englishmen into jail than out of it" (H. A. Nutting, 1960, 527).

In England, XVII Century was turbulent because of the struggle between King Charles I Stuart, his government, the parliament and common and equity courts (K. Zweigert, J. Kötz, 1998, 189). Parliament reinforced the habeas corpus protections to limit the effects of the actions of the Crown and its government, in particular the Privy Council (B. Farrell, cit., 555). Sir Edward Coke and William Blackstone, both among the most influential jurists of that time, argued that the legal basis of habeas corpus were founded on the Magna Charta, but today this reconstruction is debated (Clarke, A., 1998). King Charles I Stuart suspended Parliament between 1629 to 1640, however common law courts continued to issue habeas corpus writs against arbitrary imprisonment ordered by the king himself (B. Farrell, cit.). The Habeas Corpus Act 1640 led to civil war, and despite the beheading of the king in 1649, arbitrary imprisonments continued even under Oliver Cromwell's rule. During his Protectorate, Cromwell pressed the courts to be more compliant with his will (B. Farrell, op . cit.). After the restoration of the monarchy, arbitrary detentions continued and prisoners were deported overseas. In 1679, Parliament finally approved a new Habeas Corpus Act attributing new guarantees to detainees both procedural, such as the right to a speedy trial, and substantive, such as the ban on unauthorized or overseas transfers. Habeas Corpus Act 1679 confirmed the fundamental and constitutional nature of habeas corpus, which continued to evolve in jurisprudence as a guarantee of personal freedom (B. Farrell, op. Cit.).

What can we learn today from this experience? Can we refer to the Habeas Corpus Act of 1679 for modern personal data protection? Indeed, some years ago the overseas of transfer suspected terrorists related to 9/11 was much discussed in the United States. My actual point is the comparison with personal data transfer today.

The idea that gave birth to this contribution concerns the extension of the guarantees of habeas corpus to personal data, because although personal data are intangible, they are the projection of the individual as a physical person, so they deserve the warranties extention in the physical sense.

Scholars are divided, and two widely divergent models have emerged. The first was proposed in particular by Richard A. Posner (1978: 393), and concerns the right of individuals not to be placed in a bad light as a result of the publication of false and defamatory data. Its consequences entail the control and deletion only of those personal data that are harmful to the person, along with prevention of the spread of false information and misleading interpretations.

The second model refers to the law of *habeas data* and follows Alan Westin (1970) and Stefano Rodotà (2012) in defining the inviolability of digital identity as the personal right of individuals to control the use of data released in the course of their daily activities, and to ask for their deletion (A. Guadamuz, 2000; M. T. Gonzales, 2016, 642; K. S. Rosenn, 2011, 1022; W. O. Bastos, 2007, 2).

In this perspective, some comparative experiences showed how a similar approach in protecting personal data could be possible, although it now appears minoritarian, connected with non-English speaking areas. Indeed, it spread from Constitutions of several Latin America countries in the 1990s and arrived in the European Union, especially in Germany, in the case law of the Federal Constitutional Court some years later (M. T. Gonzalez, 2016, 642; A. Guadamuz, 2000, 7). However, scholars and case law are divided on the "habeas data" concept. According to the

innovative Brazilian constitutional experience, it refers to the right to check and control personal information. Indeed, Article No. 5 of the Brazilian Constitution states that

habeas data shall be granted: a) to assure knowledge of personal information about the petitioner contained in records or data banks of government agencies or entities of public character; b) to correct data whenever the petitioner prefers not to do so through confidential or administrative proceedings[.]

It is applied to all persons and the writ could be used against public databases. Brazilian Congress did not approve a statute regulating habeas data until 1997, when the legislator made clear that an entity with a register or database is public in character if the data is being transmitted or could be transmitted to third parties (K. S. Rosenn, cit.). This is the leading model for South American experiences, followed by other countries such as Paraguay, Peru, Argentina and Costa Rica (A. Guadamuz, cit.; L. Parraguez Kobek, E. Caldera, 2016, 111).

Apparently, this regulation is similar to that developed in the Charter of Fundamental Rights of the European Union, precisely Article No. 8, elaborated on the basis of the European Court of Human Rights case law. Indeed, Article No. 8 (Protection of personal data) affirms that

1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.

Privacy is closely connected to the expression of individual personality, since it allows a person to reveal his or her personal convictions, even the most intimate. The evolution of information technology has caused an unexpected explosion of this issue. With the proposed application of the habeas corpus principle to WDs, I intend to advocate not just about personal data checking aspects, which are anyway relevant, but I want to refer precisely to the creation of a limit, a boundary, a fence or an obstacle to the collection of personal data through physical instruments. In this sense, and from a conceptual point of view, I considered the German constitutional case law of the Federal Constitutional Court, especially in the decision issued on 27th February 2008 (BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07).

This decision recognized the existence of the right of any telematic technologies user to be entitled to his or her freedom as an expression of his or her digital personality, so even his or her digital home where the individual encloses his or her data, collected in webmail, or a laptop, or a device for daily use. Actually, that constitutional case was promoted by a group of people (a journalist, a member of a local political party and three lawyers) against a provision of the Nord-Rhine Westphalia Constitution Protection Act. (§ 5.2 no. 11 sentence 1 alternative 2 of the Constitution Protection Act) admitted online searches through secret access to information technology systems. It was declared null and void because it admitted online searches made by state agencies under surveillance programmes. Indeed, such surveillance programmes were in violation of the general right of personality “*as a fundamental right to the guarantee of the confidentiality and integrity of information technology systems*”, violating the principle of proportionality. According to the German Constitutional Court,

“the guarantee of the inviolability of the home leaves loopholes as regards access to information technology systems. Article 13.1 GG does not confer on the individual any across-the-board protection regardless of the access modalities against the infiltration of his or her information technology system, even if this system is located in a dwelling. The encroachment may take place regardless of the location, so that space-oriented protection is unable to avert the specific endangerment of the information technology system. Insofar as the infiltration uses the connection of the computer concerned to form a computer network, it leaves the spatial privacy provided by delimitation of the dwelling unaffected. (...) The manifestations of the general right of personality, in particular the guarantees of the protection of privacy and of the right to informational self-determination, previously recognised in the case-law of the Federal Constitutional Court, also do not comply sufficiently with the special need for the protection of the user of information technology systems. The need for protection of the user of an information technology system is however not restricted solely to data to be allotted to his or her privacy. The right to informational self-determination also does not fully do justice to personality endangerments. A third party accessing such a system can obtain data stocks which are potentially extremely large and revealing without having to rely on further data collection and data processing measures. In its severity for the personality of the person concerned, such access goes far beyond individual data collections against which the right to informational self-determination provides protection.”

Even though the German constitutional judges’ decision, which regarded a case of the hidden use of spying software (so-called “Trojan Horses”) is from nine years ago, the critical issue of collected data transfer and use emerges again. In this sense, a transformative version of the concept of habeas corpus, adapted to immateriality, may be helpful. In common law similar approach already happened with the abovementioned cybertrespass.

This approach could be disputed by two objections, which could be easily overcome. On the one hand, it could be underlined that these data are intangible and therefore they cannot be treated as physical objects. The reply to this statement is that they are part of the human body and belong to the body of the rightholder. In other words: the data on my body, my health, my behavior belong to my body, and therefore belong to me, and they should be treated as such.

On the other hand, it could be argued that the immateriality of the data could prevent their treatment like the other (physical) legal goods. However, in other circumstances, these concerns about immateriality of such goods does not arise. For instance, in case of seizure of illicit materials disseminated by Internet websites or peer-to-peer programmes, such as infringed copyrighted materials or child abuse images.

4. Some sensitive cases for applying habeas corpus doctrine to wearable devices data transmission

Since IoT and WDs represent both increasing technologies, the issues to analyse can be very numerous, but for this purpose I will focus on issues that are relevant in my perspective about the application of habeas corpus. In fact, among several legal issues that WD data collection could face,

there are some more relevant because they concern personal dignity, physical and psychological integrity. Among them, I will deal with four of them, representing problematic issues that could be seen as a model for other sensitive cases.

The following issues have been chosen under a specific perspective, namely a business-oriented view considering privacy as a paid service for WD consumers, rather than a fundamental right protecting sensitive data.

4.1 WD and health issues

WD medical apps seem to be the most attractive tool for medical markets. WDs include: smart-watches, heartbeat monitors, pain management devices, glucose monitoring systems, blood oxygen level monitors, hearing technologies and so on

The huge dissemination of these tools seems to set up several issues:

a) Use of WD needs a distinction from a legal perspective. For instance, distinguishing the cases in which WD use is really necessary for patient care and it can improve his or her health in case of illness. In this situation, personal data protection has to be immediate, given the situation of health weakness of the patient him or herself.

b) Indeed, WD could be used for collecting data related to wellness or fitness. Invasion of privacy in these cases may appear to be irrelevant, but there is always a potential risk for the future, when the patient's condition may change or health information collected could come back to haunt him or her, as in the case of a trial discovery or health insurance applications;

c) Since collected data pertain to the user/patient health protection, the manifestation of his or her informed medical consent is due (E. A. Brown, 2016, 34). However, a question arises regarding the temporal validity of his/her medical consent: it has to be valid according the original consensus (when the user bought the WD or it was given to him/her), or the medical consent has to be renewed after a certain time of use or manifested each time the user/patient accesses the WD.

d) Some scholars speak about "*Democratization of medicine*" (N. Cortez, 2014, 1197; S. J. Kilker, 2016, 1355) or even of "*Uberization of Medicine*" (F. Khan, 2016, 128) to warn of the double risk of disclosure of such data by the users/patients on social networks. On the one hand, this disclosure turns the role of social networks into something different, since they accumulate these data (with the abovementioned consequences). On the other hand, issues not directly relevant to this topic may arise, which are still relevant, such as: the risk of self-diagnosis and dissemination of pseudo-medicine.

e) Extensive use of WDs will boost personalized medicine (W. Boyd, 2016, 548). Indeed, involving both pharmacogenetics and health development use of WD for checking life parameters is bringing a remarkable change in privacy protection, access to health care and medical informed consent (I. Ajunwa, K. Crawford, J.S. Ford., 2016, 476 ss). Furthermore, pure research funding will suffer competition in gaining funding by this remunerative field of applied research.

Cases a) and b) may have repercussions under private law such as access to information by insurance companies for health coverage, or by business companies for recruitment. But even under a public law perspective processing aggregating data (big data) could have influences in order to

promote a public policy or a cut in the budget. From an ethical perspective, WDs give rise to multiple sensitive issues, especially in medicine and health protection, areas of massive research and developing of devices and apps. These regard privacy, informed consent and security, especially about data transmission from the device to data base (I. Ajunwa, K. Crawford, J.S. Ford., 2016, cit.).

4.2. *WDs and workplace issues*

WD use at workplaces reveals interesting issues under different aspects:

- a) On the one hand, a possible direct discrimination of employees could emerge through the collection and storage of data relating to their work performances and tasks as regards the control of the workers behaviour. In fact, profiling data collected through WD not only regards abstract categories to which workers pertain (such as sex, origin, religion and so on) but it also allows to reconstruct the most important features of the individual on his or her most intimate and sensitive personal data (as we saw above, his or her health or illness, ability to work, level of attention, concentration, distraction and so on).
- b) The increasing adoption of social and corporate policies on fringe benefits could have an expansion, and one may wonder whether the award of such benefits to employees can be influenced by the use of WDs, which are able to identify the good behavior of workers qualifying them to access these advantages. This is especially valid in Europe where public support to welfare state and public health is suffering funding cuts due to the economic crisis,
- c) Nevertheless, WD could improve workplace safety, especially for hazardous and strenuous jobs or workers wellness, especially in customer services (E. A. Brown, 2016, cit., 8).
- d) The intention in using employees' collected data by employers is crucial: on the one hand, collectors may develop some sort of intrusive and illegal control over the employers' privacy; while on the other hand, data use, even if oriented to the welfare of workers, could itself carry the risk of paternalism and promotion of conformist behaviour.

4.3. *WD and big data*

“Big data” was qualified as a “(P)roblem-solving philosophy that leverages massive datasets and algorithmic analysis to extract “hidden information and surprising correlations” (W. Hartzog, E. Selinger, 2013, 81; M. M. Christovich, 2016, 104). As noted (K. Michael, K. W. Miller, 2013, 23),

Big data can expose people’s hidden behavioral patterns and even shed light on their intentions. More precisely, it can bridge the gap between what people want to do and what they actually do as well as how they interact with others and their environment. This information is useful to government agencies as well as private companies to support decision making in areas ranging from law enforcement to social services to homeland security. It’s particularly of interest to applied areas of situational awareness and the anticipatory approaches required for near-real-time discovery.

The collection of big data becomes a key issue in the protection of personal privacy perspective since individuals show their lives on social networks (hereinafter SN), showing themselves off spontaneously without adequate precautions.

A double issue could arise: a) massive data collection by WD producers, and b) massive data collection by third parties, especially SN, through the initiative of individuals who use social platforms.

These data must be anonymised by both WD manufacturers and external users. Indeed, users are forced to accept a waiver form to gain access to use of both WD and SN, and both of them allow profiling every aspect of the person's behaviour and how the user interacts with other users as an individual, his or her relationship with user groups, and collectively. These circumstances bring enormous competitive and market advantages because it means knowing with absolute certainty, obtained from the personal source of data, the users' preferences; either individually or collectively (F. Provost, T. Fawcett, 2013, 51 ss). Furthermore, this personal unveiling manifests no chance to "return" to the user of personal inclinations, and health and well-being data (see supra par. 4.1.).

4.4. WD, hacking and security issues

Hacking and security issues are major vulnerability for IoT products (S. Shahmiri, 2016, 28; S. R. Pepper, 2014, 135). Mainly because "*they have not necessarily been engineered to protect data security*" (S. R. Pepper, 2014, cit.). Since these products are often designed and manufactured by traditional consumer-goods producers and not computer hardware or software firms, the engineers creating these products may not be as experienced with data security issues and therefore may not adequately address security concerns (S. Shahmiri, 2016, cit.).

5. Legal overview in a comparative perspective

Legal regulation in this issue is a complex matter since it includes different legal fields. On the one hand, under the producers' perspective, it concerns patent law. However, WD patent developers have to come up with a system for the collection and transmission of personal data that is respectful of the users' dignity, even when they are aware of and consent to use their personal data.

On the other hand, there are issues such as healthcare access, manifestation of informed consent, privacy and consumer protection. However, the approach of the consumer protection seems to be unsatisfactory since it focuses mainly on the product and how it works, and not on privacy protection of collected data under a privacy protection perspective. A further issue exists related to which jurisdiction collected personal data are stored in, therefore a comparative approach is necessary and useful.

5.1 U. S. perspective

In the U. S. there is no general privacy law (S. Shahmiri, 2016, cit.30), the Federal Trade Commission (hereinafter FTC) has authority to promote consumer protection, making it the de facto data protection and consumer privacy regulator (S. Shahmiri, 2016, cit.; S. R. Pepper, 2014, cit.). The FTC was established in 1914, originally for ensuring fair competition in commerce. Later, it increased its policy competence, but only in 1995 the FTC became involved with consumer privacy issues (D. J. Solove, W. Hartzog, 2014, 598). Today, the FTC is considered as "the de facto federal data protection authority" (D. J. Solove, W. Hartzog, 2014, cit.; S. Hetcher, 2000, 109). Indeed,

The FTC's regulatory power is crucial in this field, since tort law cannot readily be applied to privacy breaches and unfair privacy practices. Traditional privacy torts, such as the public disclosure of private facts, do not readily fit within the

data breach framework. Under this tort, there is a cause of action when there is public widespread disclosure of a private matter that "...would be highly offensive to a reasonable person, and...not of legitimate" public concern. In a data breach, while data is compromised and accessed by some unauthorized hackers, the data itself is usually not disseminated widely; often, the data revealed - while sensitive - is not of the nature that would be highly offensive if disclosed, thus rendering the tort inapplicable. (S. Shahmiri, cit).

So, it seems reasonable to adapt the habeas corpus model as a tool for the protection of data linked to the user's individuality and personality. However, law suffers *horror vacui*, so we will look at what American case law decided on the point, despite the aforementioned problems related to the absence of a uniform approach to the regulation of privacy protection. However, in the United States, litigation on WD is related to patent litigation, especially on the tools that monitor, collect and transmit user's personal and health data: *Zoll Medical Corporation v. Respironics, Inc.*; *Fitbit Inc, v. Aliphcom, Et Al.*; *Smart Wearable Technologies Inc., v. Microsoft Corporation.*; *Fitbit, Inc., v. Aliphcom, Et Al.*; *Alfred E. Mann Foundation For Scientific Research, Advanced Bionics, Llc, v. Cochlear Corporation, Nka Cochlear Americas, Cochlear Ltd.*

Otherwise, on the one hand a more significant case law research on big data under a privacy issue could be done. For instance, the United States District Court for the Eastern District of Virginia, Richmond Division, in the case *Soutter v. Equifax Information Services*, affirmed that

"Even before the modern rise of "big data," Congress found that the credit industry's reliance upon "computerized data banks" posed a "great danger" that an individual's life and character would be "reduced to impersonal 'blips' and key-punch holes in a stolid and unthinking machine" and that, thereupon, his reputation would be ruined without cause. See Dalton v. Capital Associated Indus., Inc., 257 F.3d 409, 414 (4th Cir. 2001)" (307 F.R.D. 183; 2015 U.S. Dist. LEXIS 4999)

On the other hand, IoT issues see protecting consumer privacy as well. Indeed, the FTC made the first claim against TRENDnet, a firm producing web-enabled camera useful to check home safety, in this case to monitor babies in their cradle (S. Shahmiri, cit). According to FTC source: "the cameras had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet address" (FTC, 2014). The point of this decision is focused on the public display of security information of the cameras:

In settling the complaint, TRENDnet is prohibited from misrepresenting the security of its cameras or the security, privacy, confidentiality, or integrity of the information that its cameras or other devices transmit. In addition, the company is barred from misrepresenting the extent to which a consumer can control the security of information the cameras or other devices store, capture, access, or transmit. TRENDnet also is required to establish a comprehensive information security program designed to address security risks that could result in unauthorized access to or use of the company's devices, and to protect the security, confidentiality, and integrity of information that is stored, captured, accessed, or transmitted by its devices. The company also is required to obtain third-party

assessments of its security programs every two years for the next 20 years.(FTC, cit.).

However, the decision is silent on the treatment of collected personal data (in this case these data pertain to babies whose parents used these cameras). Even if this decision does not regard a proper wearable device, it is still relevant because it involves images of small children captured with a camera, which is a sensitive issue in privacy protection. In fact, the FCT decisions regard consumer protection, while privacy protection is underestimated as shown by this decision itself. According to this perspective, issues related to personal data collected through wearable devices seems not properly treated by U. S. Law, which is mainly focused on patent and consumer protection laws.

5.2. The E. U. (before Brexit) perspective

The European perspective is focused on protection of dignity and human rights. At the time this paper was written, the United Kingdom has not yet fulfilled the procedure to accomplish the exit from the European Union according to Article No. 50 of the Treaty of Lisbon. In this sense, the United Kingdom pertains and applies European Union Law.

First of all, the Charter of fundamental rights of the European Union became binding as the Lisbon Treaty came into force (G. Di Federico, 2011, 38). Its first article is dedicated to protecting human dignity: the innovative contribution of this perspective concerns dignity as an essential part of a human being, recognizing it as due to every individual without discrimination.

Regarding privacy protection, such issue concerns both article 7 (protection of private and family life) and article 8 (protection of personal data). Article 7 protects individualistic aspects of protection from interferences of other subjects in personal privacy, including discovery of health data pertaining to a single individual and to his or her family. For this reason this article grants the right to refuse to reveal one's own data in case of massive collecting of genetic data. Article 8 concerns protection of the personal data of each person or group of persons having some common characteristics. These data have to be processed according to law and following the principles of fairness and requirement for the consent of the data holder. Each individual has the right to access collected data and obtain rectification. Scholars affirm that the infringement of this right could prejudice the liberty and dignity of a person and interfere with the development of his or her personal identity. Article 8 tries to balance one of the most evident paradoxes of modern medicine, as it uses advanced scientific and medical research while reducing privacy about the dependence of the human body from technologic evolution (A. Torrice, 2009, 120). It seems very clear that articles No. 7 and 8 of the Charter of Fundamental Right of the European Union affect the hardware and software houses of WD and their programs.

Many other articles of the Charter are strictly connected with the guarantees set by article 8. One of the most important is article 21, related to the principle of non-discrimination based, among other matters, on health. This article could be read as a combination of several principles related to fair treatment such as equal opportunities between men and women (article 23), rights of children (article 24), rights of elderly people (article 25), rights of disabled people (article 26). The Charter specifies the protection of each category of people that may be at risk due to their vulnerability because of age, gender, psychological or physical situation. This is the perspective of the weak

parties of the abovementioned cases: health issues, workplace discrimination, big data collection, security issues.

Under the new EU General Data Protection Regulation No. 679/2016, which will not come into force until 24 May 2018, software developers and service providers will have to implement "privacy by design." This includes enforcing personal data protection in the technical design of the application. That means that developers will have to supply "privacy by default". Under this perspective, they have to configure their application in a way that the applications will not share anything beyond what is strictly necessary, and the user will have to consent explicitly to any further disclosure. However, this new regulation shows some interesting points. For instance, it refers to codes of conduct approved by national privacy authorities (P. Marini, 2017, 1). This specific discipline seems to affect hardware and software houses manufacturing WDs and their programmes in several articles. For instance, Article No. 4, regards relevant definitions, such as what are a personal data (4.1.), processing data (4.2), profiling (4.4.), filing system (4.6), consent (4.11), personal data breach (4.12), genetic data (4.13). But the most relevant definitions under our perspective are

1. biometric data (4.14), that means "*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*"; and

2. 'data concerning health' (15), that means "*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*".

Article No. 7 states that the data use is only possible according on the data owner's consent, while Article No. Article 9 regards "Processing of special categories of personal data". Paragraph 1) affirms that

"(P)rocessing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".

Paragraph 2) disciplines exceptions to par. 1 applications, as follows a) explicit consent given by the data subject for specified purposes; b) data processing necessary for exercising specific rights in the field of employment and social security and social protection; c) to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; d) legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim; e) personal data which are manifestly made public by the data subject; f) the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; g) for reasons of substantial public interest; h) the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services; i) for

reasons of public interest in the area of public health; j) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

The regulation also addresses issues relevant to WD privacy management, such as personal data portability, rectification and erasure (Article No. 20), right to object (art. 21), right to be subject to a decision based solely on automated processing, including profiling (art. 22), especially in "any form of automated processing of personal data consisting in the use of such data (...) to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects of the performance at work, the economic situation, health, personal preferences, interests, reliability, behavior, location or movements of that individual. Facing the objection of a concerned person, the data controller is obliged to refrain from further processing of personal data, unless the data controller proves the existence of compelling legitimate grounds to proceed with treatment that prevail on the interests, rights and freedoms of concerned person or for the establishment, exercise or defense of a legal claim. (P. Marini, 2016, 2).

5. Conclusions

The concise comparison about privacy regulations in the WD environment shows that neither the U. S. nor the E. U. legal systems are aware of the specific risks about the spread of WD users' personal data. Indeed, regarding privacy protection, WD use represents a transformative concept of privacy, since processing the whole data pertaining to an individual involves the digital reconstruction of this person, and his or her physical and psychological characteristics. In this regard, habeas corpus represents the strong tradition of human dignity and human rights protection, and it could be a bridge between a legal institution of great historical tradition and modern needs in the field of personal data protection in the WD environment. It could overcome both American and European regulations limitations. Indeed, on the one hand the U. S. regulation seems focused exclusively on patent protection and consumer matters, and on the other hand, the E. U. discipline seems to have a very formalistic and bureaucratic approach. In both cases, rules do not seem to be sufficiently adequate. Rather, through this legal entity it seems to be possible to maintain high parameters of protection of individuality and to ensure the most intimate aspects of personal expression.

6. Bibliography:

- Ajunwa, I., Crawford, K., Ford J. S., (2016), Health and Big Data: An Ethical Framework for Health Information Collection by Corporate Wellness Programs, 44 J.L. Med. & Ethics 474;
- Balganesh, S., (2006): Common Law Property Metaphors on the Internet: The Real Problem with the Doctrine of Cybertrespass. Available at <http://dx.doi.org/10.2139/ssrn.882848>
- BASTOS, A. W. (2007), O habeas data e a proteção da privacidade individual: recuperação histórica da evolução conceitual e constitucional no Brasil, <<http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/15977/1554>>.
- Bilton, N., (2013), At Google Conference, Cameras Even in the Bathroom, New York Times, 20.5.2013, B6;
- Bilton, N., (2015), Why Google Glass Broke, New York Times, 5.2.2015, E1;
- Boyd, W., (2016), Imagining the Legal Landscape: Technology and the Law in 2030: Environmental Law, Big Data, and the Torrent of Singularities, 64 UCLA L. Rev. Disc. 544

Brown, E. A., (2016), The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work, 16 Yale J. Health Pol'y L. & Ethics 1;

Christovich, M. M., (2016), Why Should We Care What Fitbit Shares?: A Proposed Statutory Solution to Protect Sensitive Personal Fitness Information, 38 Hastings Comm. & Ent. L.J. 91;

Clarke, A., (1998), Habeas Corpus: The Historical Debate, 14 N.Y.L. SCH. J. HUM. RTS. 375, 377

Coke E., (1644), Institutes of the Laws of England;

Cortez, N., (2013), The Mobile Health Revolution? SSRN: <https://ssrn.com/abstract=2284448>

Di Federico, G. (2011), Fundamental Rights in the EU: Legal Pluralism and Multi-Level Protection After the Lisbon Treaty, in (G. Di Federico, ed.), The European Charter of Fundamental Rights: From Declaration to Binding Instrument;

Duker, W. A., (1980), A Constitutional History Of Habeas Corpus, Greenwood Press, Westport, Connecticut.

Farrell, B., (2008), From Westminster to the World: The Right to Habeas Corpus in International Constitutional Law, 17 Mich. St. J. Int'l L. 551

Ferguson, A. G., (2016), The Internet of Things and the Fourth Amendment of Effects, 104 Calif. L. Rev. 805;

FTC Approves Final Order Settling Charges Against TRENDnet, Inc. (2014), <https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc>

Gonzalez, M. T., (2016), Habeas Data: Comparative Constitutional Interventions From Latin America Against Neoliberal States Of Insecurity And Surveillance, 90 Chi.-Kent L. Rev. 641;

Guadamuz A., (2000) 'Habeas Data: The Latin-American Response to Data Protection', 2000 (2) The Journal of Information, Law and Technology (JILT), <http://www2.warwick.ac.uk/fac/cos/law/elj/jilt/2000_2/guadamuz/>

Halliday, P. D. (2012), Habeas Corpus: From England to Empire, Harvard University Press, Boston;

Halliday, P. D., White, G. E., (2008), The Suspension Clause: English Text, Imperial Contexts, and American Implications, 94 Va. L. Rev. 575;

Hartzog, W., Selinger, E. (2013), Big Data in Small Hands, 66 STAN. L. REV. ONLINE 81

Hetcher, S., (2000), The De Facto Federal Privacy Commission, 19 J. Marshall J. Computer & Info. L. 109;

Iaselli, M., (2015) Internet of Things, droni e robotica. Problemi giuridici e possibili soluzioni, Altalex Editore;

Khan, F., (2016), The 'Uberization' of Healthcare: The Forthcoming Legal Storm Over Mobile Health Technology's Impact on the Medical Profession , 26 Health Matrix: The Journal of Law-Medicine 123;

Kilker, S. J., (2016), Effectiveness of Federal Regulation of Mobile Medical Applications, 93 Wash. U. L. Rev. 1341;

Langley, M. R., (2015), Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables, 103 Geo. L.J. 1641;

Marini P., (2017), Regolamento europeo Privacy: i codici di condotta e le certificazioni, Il Quotidiano Giuridico, 27.2.2017;

Marini, P., (2016), Oblio e portabilità dei dati: novità dal nuovo Regolamento Privacy europeo, Il Quotidiano Giuridico, 26.7.2016

Michael, K. Miller, K. W., (2013), Big Data: New Opportunities and New Challenges, Computer, Vol. 46, Issue 6, 22-24;

Nutting, H. A., (1960), The Most Wholesome Law - The Habeas Corpus Act of 1679, 65 Am. Hist. Rev. 527;

Parraguez Kobek, L., Caldera, E., (2016), Cyber Security and Habeas Data: The Latin American Response to Information Security and Data Protection SSRN: <https://ssrn.com/abstract=2868039>

Peppet, S. R., (2014), Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85, 135 (2014);

Peyton, A., (2016), A Litigator's Guide to the Internet of Things, <http://jolt.richmond.edu/v22i3/article9.pdf>.

Provost, F., Fawcett, T., (2013), Data Science and Its Relationship to Big Data and Data-Driven Decision Making, Big Data. February 2013, 1(1): 51-59. doi:10.1089/big.2013.1508;

Rodotà, S. (2012), *Il diritto di avere diritti* (Bari).

Rose, K., Eldridge, S., Chapin, L., The Internet of Things: An Overview. Understanding the Issues and Challenges of a More Connected World, (2015), <http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151022.pdf>;

Rosenn, K. S. (2011), Procedural Protection of Constitutional Rights in Brazil, 59 Am. J. Comp. L. 1009;

Segura Anaya, L. H., Abeer A., Costadopoulos, N., Prasad P. W., Ethical Implications of User Perceptions of Wearable Devices, Sci Eng Ethics, Doi: 10.1007/s11948-017-9872-8, 2017

Shahmiri, S., (2016), Wearing Your Data on Your Sleeve: Wearables, the FTC, and the Privacy Implications of this New Technology, 18 Tex. Rev. Ent. & Sports L. 25;

Singleton, S., (2000): Privacy Versus the First Amendment: A Skeptical Approach. In: *Fordham Intellectual Property, Media & Entertainment Law Journal*, Vol. 11, pp. 97-153

Solove D. J., Hartzog, W., (2014), The FTC and the New Common Law Of Privacy, 114 Colum. L. Rev. 583;

Thierer, A. D., (2015), *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, 21 RICH. J.L. & TECH. 6 (2015), <http://jolt.richmond.edu/v21i2/article6.pdf>.

Torrice, A., (2009), Commento Art. 8, in (G. Bisogni, G. Bronzini, V. Piccone, eds), *La Carta dei diritti dell'unione europea. Casi e materiali*;

Tyler, A. L. (2016), Federal Courts, Practice & Procedure Honoring Daniel Meltzer "SECOND Magna Carta": The English Habeas Corpus Act And The Statutory Origins Of The Habeas Privilege, 91 Notre Dame L. Rev. 1949

Van Woense, L., Archer, G., (2015), Ten technologies which could change our lives, Potential Impacts and policy implications, European Parliamentary Research Service

Westin, A. (1970), *Privacy and Freedom* (London);