International Working Group
on Data Protection
in Telecommunications

675.50.15

Working Paper on Privacy and Wearable Computing Devices[1]

57th Meeting, 27-28 April 2015, Seoul (Republic of Korea)

General Background and scope

Wearable computing is a term used to describe computer-powered devices or equipment that are small enough to be worn or carried on a user's body.[2] These devices incorporate various types of sensors with different capabilities. For example, sensors have the ability to collect, in real time, information about the user's body (mood, habits, physical activities, health status, speed, mobility) and the user's environment (images, sounds, temperature, humidity, location, social environment) as well as computer-generated data to mediate the user's experience of the world around them.

Many wearable devices include a camera of some form. Though a camera would only capture some of the above elements, the camera feature is the focus of many current privacy concerns.[3] It is the ability of these devices to record, perhaps constantly, and perhaps covertly, that leads to many concerns, particularly with respect to the privacy of non-users who may be the subject of those recordings.

There are currently four main segments in the wearable technology marketplace[4]:

a) fitness, wellness and life tracking (e.g., smart clothing and smart sports glasses, activity monitors, sleep sensors) which are gaining popular appeal for those inclined to track many aspects of their lives;[5]

---

[1] This Working Paper draws heavily on the Report by the Research Branch of the Office of the Privacy Commissioner of Canada "Wearable Computing: Challenges and Opportunities for Privacy Protection", January 2014, with further references; https://www.priv.gc.ca/information/research-recherche/2014/wc_201401_e.asp .

[2] There are several different definitions for the term "wearable computing". See, for example, Steve Mann, (1996a): Smart Clothing: The Shift to Wearable Computing. In Communications of the ACM, 39 (8) pp. 23-24. See Mann, Steve (2014): Wearable Computing. In: Soegaard, Mads and Dam, Rikke Friis (eds.). *The Encyclopedia of Human-Computer Interaction*, 2nd Ed., Aarhus, Denmark: The Interaction Design Foundation. Available online at https://www.interaction-design.org/encyclopedia/wearable_computing.html, accessed 11 March 2015. See also, Webopedia, "wearable computing", http://www.webopedia.com/TERM/W/wearable_computing.html) or dictionary.com, "wearable computer", http://dictionary.reference.com/browse/wearable+computer).

[3] Donald Melanson and Michael Gorman, "Our augmented selves: The promise of wearable computing." Engadget. December 12, 2012. Accessed on July 8, 2013.

[4] "Wearable Technology Market - Global Scenario, Trends, Industry Analysis, Size, Share And Forecast, 2012 – 2018." *Market Research Reports Biz*. January 2013. Accessed June 13, 2013.

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

The Working Group has been initiated
by Data Protection Commissioners
from different countries in order
to improve privacy and data protection
in telecommunications and media

b) infotainment (e.g., smart watches, augmented reality headsets, smart glasses);[6]

c) healthcare and medical (e.g., continuous glucose monitors, wearable biosensor patches);[7] and

d) industrial, police and military (e.g., hand worn terminals, body-mounted cameras, augmented reality headsets).[8]

Segments c) and d) will not be dealt with in this Working Paper. Although this Working Paper does not deal with segment c) – health care and medical data – it acknowledges that data in segment a) – fitness, wellness and life tracking data – may qualify as health data[9].

The wearable era creates new or amplifies existing privacy risks in the mobile environment by gathering additional, and possibly sensitive, personal information and by doing so in unobtrusive, or covert, ways. Real-time information about someone's mood, physical fitness and health status are likely to be captured by the definition of personal information. Even information about a healthy person (e.g., heartbeat) may be considered to be sensitive information. The differences between a smart phone and many wearable computing devices are more of degree than of kind, but they are important differences from the point of view of privacy protection.

With wearable computing devices, computing power seems to disappear in clothing, glasses and watches, and eventually under the skin, removing many of the traditional cues that would let an individual know that such devices are present and operating. The result is an increasing lack of transparency and the ensuing difficulty for users and other data subjects to make informed choices. Furthermore many wearable devices come with an obligation to connect with the manufacturer of the hardware, of the mobile operating system or with cloud service providers. This can lead to the data subject's loss of control over the collected personal data.

Conveying meaningful information about privacy choices remains a challenge in the mobile space, with a small screen and intermittent user attention. These design characteristics add to the difficulty in reaching users with the right information about their privacy rights, in a form they can understand

---

[5] Emily Waltz, "How I Quantified Myself: Can self-measurement gadgets help us live healthier and better lives?" IEEE Spectrum, August 30, 2012. As referenced in Steve Mann. "Steve Mann: My "Augmediated" Life." *IEEE Spectrum*. March 1, 2013. Accessed on June 14, 2013.

[6] Examples of wearable devices in this category include Google Glass (www.google.com/glass/start), Oculus Rift (www.oculus.com, purchased by Facebook in), Google Cardboard (https://developers.google.com/cardboard/), and Samsung's Gear VR (http://www.samsung.com/global/microsite/gearvr/gearvr_specs.html).

[7] See Vital Connect's HealthPatch. Viewed on January 6, 2014.

[8] Kopin's Golden-i device is being developed to provide live video streaming, mobile internet access, GPS navigation and hands-free control for maintenance workers, police, paramedics and firefighters. For more information, see www.mygoldeni.com/home/.

[9] The Art.- 29 Working Party recognised that some types of processing in health and lifestyle apps and devices can be difficult to determine whether or not health data is being processed – the so-called grey area - cf. letter and annex from the Art. 29 Working Party to the European Commission, DG CNECT, on mHealth of 05/02/2015; http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf (letter) and http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf (annex).

and at the right time for them to make informed choices. Wearable computing further compounds these challenges.

Recommendations

The Working Group recommends that:

- The processing of personal data in and by wearable computing devices should be as transparent as possible for the user and others whose data are processed; in the case of hidden or miniaturized devices transparency should be provided for by other than visual means. This includes transparency of connections to ancillary devices such as smart phones.

- By default personal data should be processed under the control of the person wearing the device. There should be no obligation to connect to the servers of hard- or software manufacturers, platforms or cloud service providers.

- The transmission or disclosure of data requires clear signalization to and informed as well as explicit consent by the user of the wearable device.

- The rights of the data subject, and namely those of access, correction and deletion, need to be respected. In particular, individuals should have a way to launch a meaningful challenge to the accuracy of the data generated, or the analysis that is done, based on data collected by a wearable device.

- Any products and /or services should embody the principle of user control. This should, among other things, include:

    - The ability to modify device functionality (e.g., by switching the conversation from audio to text in order to enhance privacy (dynamic user control).
    - The ability to stop the collection of their personal data temporarily on a case-by-case basis (e.g., for certain time periods and/or activities where they do not wish to be monitored), and
    - The ability to select or control the granularity of data being processed or sent to third parties.

- Individuals should have the ability to withdraw their consent to data disclosure at any time. They should also have the option to switch to local storage (e.g., a smart phone or another device under the control of the user) and to backup their data.

- Means for ensuring data portability should be provided.

- The use of wearable devices in the employment sector raises additional issues with regard to employee's free choice. Employees who opt not to participate in any programs based on wearable devices should not be adversely affected by their decision.

- When data processed by wearable computing devices qualifies as health data, the further processing of that data should only be permitted after having obtained the explicit consent of the data subject(s).

In addition to the recommendations above, the Working Group encourages consideration of the recommendations included in the Art. 29 Working Party Opinion 8/2014 on the Recent Developments on the Internet of Things - WP 223 as applicable.[10]

Background to the Recommendations[11]

Characteristics of wearable computing

Many wearable technologies currently under development, or on the market, have appealing characteristics that could contribute to broad consumer adoption. For example, they:

a) have a visual appeal,

b) can be seamlessly integrated with the wearer's clothing or body;

c) can be customized and adapted to the needs of the user and provide feedback;

d) can provide useful feedback to the wearer, either in real time or not, and directly or through another smart device (typically a smartphone);

e) can supplement the user's own physical or mental abilities;

f) are relatively low cost for the benefit derived;

g) are versatile and have a wide variety of personal and workplace applications; and

h) are relatively simple for a consumer to set up and operate.

Constant interaction between the user and the computer, where the computer "learns" what the user is experiencing, at the time he or she is experiencing it, and super-imposes on that experience additional information, is an objective of current wearable computing design.

Implications for privacy:

In a recent industry-funded opinion survey on the social implications of wearable computing in the UK and US, 51% of respondents cited privacy as a barrier to adoption and 62% thought Google Glass and other wearable devices should be regulated in some form, while 20% called for these devices to be banned entirely. Forrester Research has concluded that fulfilling the promise of wearable computing is dependent on putting users in control of their own data, such as being able to choose whether to share it or not.

Challenges to the existing consent model

Information collected by sensors within objects that are connected to each other, whether those objects are worn by individuals or simply carried with them, can yield a tremendous amount of data that can be combined, analyzed and acted upon without adequate transparency, accountability or meaningful consent.

[10] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf; p. 21 ff.

[11] This part is largely derived from the Research Report quoted in footnote 1 above.

These developments pose profound challenges to existing privacy frameworks around the world. For example, the purpose limitation principle, intended to limit the collection of personal information, subject to consent being given for those specific purposes, is becoming increasingly difficult to apply in a world of ubiquitous computing and mobile devices. Moreover, it remains a challenge to obtain meaningful consent through mobile devices. More needs to be done to show users, in a creative and meaningful way, what is actually happening with their personal information.

New surveillance options

Some wearable computing devices gather photos, videos, sounds, locations and record the general environment around the device, including nearby people and other devices. The camera in several of these devices is the source of many privacy concerns. Inexpensive, versatile, everyday items, such as baseball caps, MP3 music players and shirt buttons, are available with hidden cameras. Many of these devices have the ability to record constantly and covertly.

Beyond the camera however, a new generation of fitness tracking technology is set to provide health insurance companies and employers with new insights into our health and behaviours. A number of insurance companies and employers in North America use tracking technology to monitor their clients and employees and to offer financial rewards in return for data showing physical activities. In Europe insurance companies are starting to offer similar contracts.

We can expect more developments of this nature. The emerging field of "physiolytics"[12] will link wearable devices with big data analytics to provide feedback and a suggestion system for behavioural change.

Aggregating data from wearable computing devices

We are witnessing a new generation of privacy challenges arising from the combination of seemingly innocuous and non-sensitive bits of personal information to derive insights into personal behaviour. We also know that combining disparate bits of information, derived from multiple sources, can lead to detailed profiles that could identify individuals. It is already challenging for individuals to make informed judgments about whether to disclose personal information, as they are not in a position to fully understand how their information may be combined and used in the future. Wearable computing devices that are constantly collecting, processing and sending data are likely to compound this problem.

Accelerating "context collapse"

Individuals may try to maintain distinctions between different spheres of their lives, whether it is among different social circles that they inhabit or simply between work and home life. Social media and the online environment generally have been undermining our ability to maintain these distinctions. This dissolution, which social scientists have referred to as "context collapse," may be accelerated as a result of sensors that are always on and always interacting with the user's body and other devices in the user's environment.

New authentication methods, new personal information

Wearable computing may be configured to manage personal information in a way that protects privacy and security. For example, research is underway to combine data generated by sensors within the current generation of smart phones so as to identify and authenticate individuals, just by having the smart phone in a pocket as those individuals go about their daily activities.

[12] H. James Wilson, Wearables in the Workplace. Harvard Business Review, September 2013, https://hbr.org/2013/09/wearables-in-the-workplace/ar/1

This means that simply walking, jogging, climbing and going down stairs with a smart phone in a pocket all have the potential to create biometric signatures of the user. While this creates the potential to improve security by means of authenticating the user, it also creates new privacy risks.

Design considerations

Dynamic User Control

Current thinking on the concept of privacy suggests that it should be thought of as a dynamic condition because the individual's social and cultural environment is constantly changing. A constellation of creative options needs to be explored to make consent more meaningful, appropriate to changing circumstances and preferences and to minimize decision overload in the wearable computing environment. For example, work should be done to:

a) develop dynamically calibrated privacy rules to meet individuals' privacy needs and expectations;

b) integrate simple design features so that the wearable device can reflect individual privacy preferences, and

c) call on organizations to enhance their privacy policies with dynamic and interactive data maps and infographics to show relationships in the wearable computing device ecosystem.

The design requirements for interacting with the wearable device will impact on the user's privacy. For example, a wearable device that relies on voice commands creates a similar privacy issue to holding a phone conversation in public. The individual's ability to modify behaviour, perhaps switching the conversation from audio to text, would be an interesting design adaptation to enhance privacy.

Evolving transparency models

There are opportunities and challenges for transparency in the wearable computing context. For example, wearable devices that use vision, hearing or other senses may be more tightly integrated with the user, so it may be easier in some ways to get the user's immediate attention. In this way, making consent and notice "visceral" in the design of a wearable device may be easier than on a smart phone. The design of some wearable computing devices does not require screens at all, so new models for negotiating privacy with users will need to be developed.

User privacy is one issue but the privacy of those around the user is another, and perhaps more vexing, problem. It is already difficult to know when someone is using a smart phone or other device to capture audio or video. With wearable computing devices, where the computers become more seamlessly integrated into unremarkable items, such as frames for everyday eyeglasses, others' ability to know and control the collection of information about themselves is greatly diminished.

Access to data and challenging accuracy in automated decision-making

Directly related to transparency is the issue of access to personal information. It is not obvious how individuals will be able to determine what is collected by a wearable device, who it is being collected by and how it is being used and disclosed. Users will need a way to challenge the personal information gathered and used by organizations as a foundation for their decisions, as accuracy is not guaranteed.

A recent study of some fitness-related wearable devices questioned the reliability of tracking the energy costs of light-intensity activities like standing or cleaning. Inaccuracies in capturing these kinds of data could have real implications for individuals using these devices. For example, inaccurate readings from a new early detection method for Alzheimer's disease, involving the assessment of patient movements by means of an accelerometer, could impact patient diagnosis and care. Inaccurate readings could also create issues in the workplace if an employer were to rely on these devices to monitor aspects of employee productivity. Ensuring individuals have a way to launch a meaningful challenge to the accuracy of the data generated, or the analysis that is done, based on data collected by a wearable device would be an important design feature.

Security vulnerabilities

Wearable computing devices without proper security and authentication systems in place are vulnerable to attack. Compromised wearable computing devices can put not only the individual’s personal information and reputation at risk but their health as well. For example, eavesdropping on and impersonation of a wearable device charged with regulating insulin could result in dire consequences for the individual’s health. As one commentator expressed it, “your personal data security is only as strong as the weakest link in your quantified self ecosystem”.