

What are the record-making and record-keeping issues implicit in Wearables? Be sure to consider the societal context in which the technology is used, as well as the various functions that records serve in society.

Wearables, or wearable technology, are terms that can denote simple mechanical devices such as reading glasses and hearing aids; however, the terms are now used more regularly to denote a wide range of smart electronic devices worn on the body for a variety of purposes, most of which have become available to consumers within the last five years.¹ They are 'smart' in that they can 'adapt automatically and modify behaviour to fit environment', sense, and provide data from what they sense, with the capability of learning to improve performance.² Wearable technology includes smart spectacles such as Google Glass, first launched in 2013 and soon to be relaunched more specifically as a smart tool particularly of use in manufacturing and design.³ Google Glass is a miniature computer with memory, processor, camera, speaker, microphone and other components, that projects its display in front of the user's eye.⁴ The most ubiquitous wearables amongst the general population are wrist-worn, and include smart watches such as the Apple Watch, which is a miniature computer worn on the wrist, incorporating the ability to send and receive calls, stream music, and monitor activity, as well as stand-alone activity monitors, such as Fitbits, which function solely to monitor the user's vital signs (heart rate and temperature, for example) and aspects of fitness, such as distances walked and calorie consumption.

These kinds of wearables are used to improve the accuracy and speed with which users carry out tasks, monitor and track health and fitness, and/or improve functionality. However, it should be remembered that wearable technology is also being harnessed to push the boundaries of fashion, theatre, and design as well as answering purely functional and quantitative requirements of users. For example, fashion designer Hussein Chalayan has for many years incorporated technology into his fashion designs,⁵ and Studio XO has married

¹ <https://www.wired.com/2013/12/wearable-computers/>, Accessed 7th March 2018.

² <https://www.igi-global.com/dictionary/smart-technology/38186>, Accessed 7th March 2018.

³ <https://www.theguardian.com/commentisfree/2017/jul/23/the-return-of-google-glass-surprising-merit-in-failure-enterprise-edition>, Accessed 6th March 2018.

⁴ Ibid.

⁵ See, for example, Spring/Summer 2007: <https://www.youtube.com/watch?v=Ae81Fcczsl8>, Accessed 6th March 2018.

fashion and technology to create sartorial spectacles such as Lady Gaga's 'Flying Dress'.⁶ Whether in the context of function or spectacle, or a combination of the two, the possibilities of wearable technology are now extending to considerations of 'digital skin', and 'hybrid humans': the use of technology not on the body, but *in* the body.⁷ Wearable technology therefore raises important philosophical questions regarding the relationship between humans and technology; such considerations lie outside the bounds of this essay, but it is important to note that record-making and record-keeping can only become more important as wearable technologies increase in sophistication and become embedded - literally, in some cases - within people and their everyday life.

Within this wide context, what are the record-making and record-keeping issues implicit in wearable technology in 2018? In answering this question, this essay will focus on one kind of wearable technology, activity monitors, although it will draw upon other forms of wearable technology during the course of analysis for contextual and comparative purposes. It will do so with an awareness of, and engagement with, the various functions that records serve within society. The primary function of records is to act as 'evidence of business activity and [as] information assets', according to BS ISO15489-1-2016,⁸ where 'business activities' encompass 'activities that support the purposes of the organisation's existence'; records are characterised by 'their reliance on metadata...to indicate and preserve context'.⁹ Therefore, as well as providing evidence for a transaction or activity, records may also function to provide information; additionally they also serve to demonstrate legal compliance where it is necessary.¹⁰ Within the context of activity monitors, the records in question act as evidence of an individual's physical activities, and various health indicators such as vital signs; they can also act as an information asset that allows the individual to maintain or change their activities for health reasons, or be advised to do so by a third party.

Before exploring the issues relating to record-making and record-keeping, it is important to describe what activity monitors are in more detail and how they operate. Activity monitors can be divided into two categories in relation to their functionality: smartbands, which have limited capabilities and are used solely to record data regarding physical activities, such as Fitbits, and smartwatches, which are more complex devices

⁶ <https://www.youtube.com/watch?v=ZVtURELhy1w>, Accessed 6th March 2018.

⁷ Ibid. See also 'The Next Black - The Future of Clothing', <https://www.youtube.com/watch?v=XCsgLWrfE4Y>, Accessed 6th March 2018.

⁸ BS ISO15489-1-2016, p. v.

⁹ Ibid.

¹⁰ Ibid., p. 2.

incorporating an operating system and with wider capabilities comparable to a smartphone, such as the Apple Watch.¹¹ Both smartbands and smartwatches include a number of sensors as part of their activity monitoring capabilities, often including a heart-rate sensor, a gyroscope, an accelerometer, and GPS.¹² The data from these sensors are collected in the smartbands or smartwatches, subjected to algorithms,¹³ and then transferred to a smartphone or computer via proprietary or third party applications or programs, after which the data are stored permanently in proprietary servers, and are accessible to users and to third parties for analysis (Fig. 1).¹⁴ This usually comes to users through an app that presents the data in a 'friendly' format,¹⁵ a record with metadata, therefore assisting the users to make sense of the information. Users are also able to share their records and data with others through applications created by proprietary companies and third parties, including those that function as social media channels.¹⁶ Software Development Kits (SDKs) and REST APIs (Representational State Transfer Application Programming Interfaces) enable third parties to develop software to collect data from proprietary servers and send it to other systems, and to access to users' data when it is stored in proprietary data warehouses or on cloud services.¹⁷ Within an SDK, data can be collated: for example, Apple's Healthkit is an application programming interface (API) included in the iOS SDK that allows apps to interact with the iOS Health application, thus collating data, assigning metadata, and then sending it for analysis, potentially to a medical professional or another party.¹⁸

¹¹ Arriba-Pérez et. al., 2016, p. 3.

¹² Ibid.

¹³ <https://www.wareable.com/fitness-trackers/how-your-fitness-tracker-works-1449>, Accessed 7th March 2018.

¹⁴ Arriba-Pérez et. al., p. 5.

¹⁵ <https://www.wareable.com/fitness-trackers/how-your-fitness-tracker-works-1449>, Accessed 7th March 2018.

¹⁶ Ibid.

¹⁷ Arriba-Pérez et. al., p. 5.

¹⁸ <https://www.telegraph.co.uk/technology/apple/11395073/What-is-Apples-HealthKit.html>, Accessed 8th March 2018.

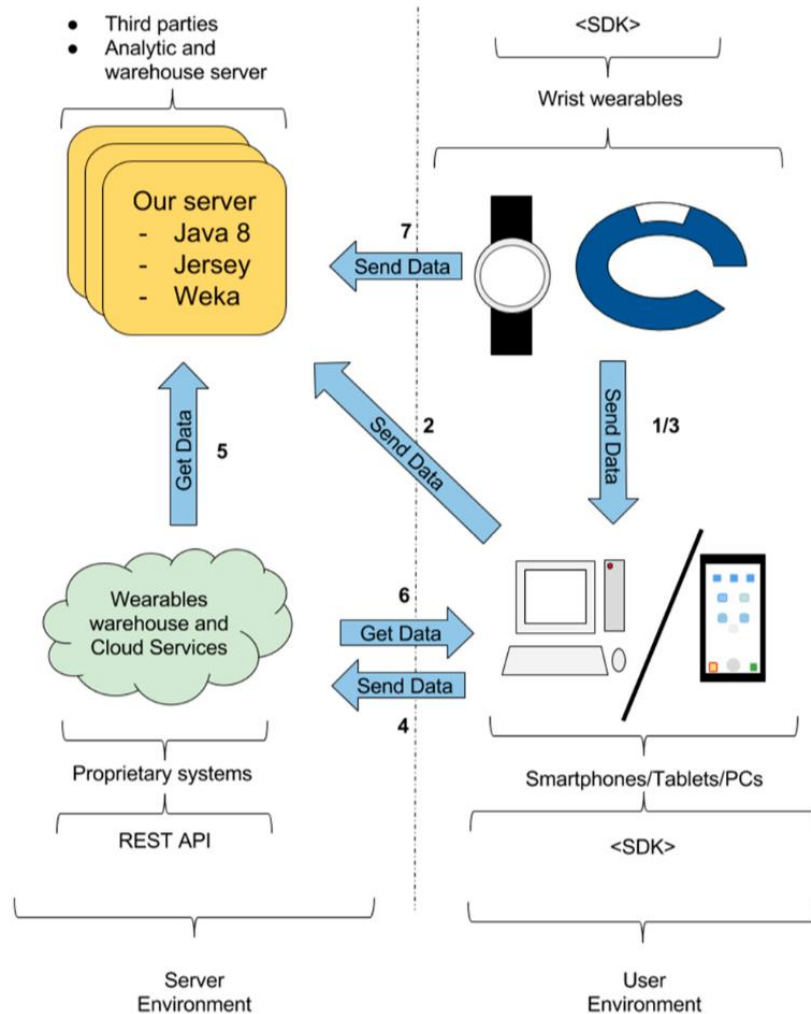


Fig. 1 Systems involved in data collection (Arriba-Pérez et. al., 2016, Fig. 4).

One of the most pressing record-making issues in relation to activity monitors and other wearable technology is that of the reliability of the data contained within the records created by the proprietary companies or third parties. Reliability, along with authenticity, integrity, and usability, are key characteristics of records according to BS ISO15489.¹⁹ A reliable record is one whose

contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and...can be depended upon in the course of subsequent transactions or activities.²⁰

¹⁹ BS ISO15489-1-2016, p. 4: 5.2.2.

²⁰ Ibid., 5.2.2.2, a and b.

There is some debate as to whether activity monitors provide 'full and accurate' representation of the activities to which they attest. There is a variability in the quantity and precision of sensors within activity monitors, and precision can be affected by how and where the smartband or smartwatch is worn.²¹ This kind of variation may not be crucial within the course of monitoring of general fitness for personal interest and goal-setting, and in general activity monitors such as the Fitbit or that within the Apple Watch may be considered reliable for everyday life.²² However, the growing use of activity monitors within the practice of medicine, for instance to collect data during clinical trials or patient treatment, is such that activity monitors' accuracy is, in this context, of paramount importance as it has potentially crucial consequences to human health and life.²³ The accuracy of activity monitors and other wearable technology is also becoming increasingly important in relation to another sphere, as records of activity are increasingly being used in legal proceedings for evidential purposes. For example, data from the Fitbit device worn by Connie Dabate, a woman murdered in Connecticut in 2015, has been used as evidence to demonstrate that her husband, suspected of the murder, was lying about her death occurring as soon as she returned home from a workout, and therefore casting doubt on his story that an unknown assailant killed her before escaping their house.²⁴ Conversely, the ability of activity monitors and other wearables to provide and share accurate records of GPS data in real-time, therefore sharing evidence of users' exact locations, can pose a security risk: this is potentially highly important in circumstances where individuals are engaged in high-risk employment such as law enforcement or military operations.²⁵

There are numerous record-keeping issues implicit in activity monitors and other wearable technology once records have been created. These include issues related to authenticity, integrity, and usability. Firstly, the issue of the ownership of records and the data within them is of great importance, and one that is widely acknowledged as not necessarily clear. For example, The American Bar Association's assessment of the legal implications of data from wearables advises litigants to establish as a primary step who owns

²¹ Arriba-Pérez et. al., p. 4.

²² <https://www.theguardian.com/technology/2017/may/24/fitness-trackers-out-of-step-when-measuring-calories-research-shows>, Accessed 7th March 2018.

²³ Kroll et. al., 2016.

²⁴ <https://www.theguardian.com/technology/2017/apr/25/fitbit-data-murder-suspect-richard-dabate>, Accessed 7th March 2018.

²⁵ <https://www.cio.com/article/3185946/wearable-technology/10-things-you-need-to-know-about-the-security-risks-of-wearables.html>, Accessed 8th March 2018.

the data: the wearable company or the individual.²⁶ Yet even this is not necessarily made clear by wearable companies: Fitbit's legal page, for example, does not include an explicit statement regarding ownership.²⁷ Rather, it concentrates on specifying the information it collects and how it uses this information. Apple's wording under its Privacy page's section on 'Health and Fitness' is ostensibly reassuring to the user: 'the information you add about yourself in the Health app is yours to use and share',²⁸ although it should be noted that this refers to the information 'you *add* about yourself [my emphasis]' to the Health app, therefore not necessarily the data that is automatically collected and exported by the device. The grey area of record and data ownership is made even more complex when users allow third parties access to their data or allow the wearable company to share data with third parties.

The issue of the security of the records created by wearables and the data they contain is also pressing. Wearable devices are vulnerable to cyber-attack, sophisticated smartwatches more so than less complex devices that solely function as activity monitors, but also, due to their relative lack of built-in security measures, they can act as conduits for hackers to attack networks to which they are connected, whether this be the cloud or a corporate network: this in turn endangers other records and data that may be of value to hackers, such as financial records.²⁹ Measures such as automatic security updates, or updates that prompt the user by identifying their urgency, and the encryption of data in transit and during storage helps to safeguard records and the data within them.³⁰ For example, Apple assures its users that data from its Health app is encrypted in transit and when stored on their servers,³¹ and Fitbit operates a 'Critical/Important/Moderate/Low' system to alert users to the urgency with which they should act on prompts to install security updates.³² Whilst most reputable companies have been aware of the need for security measures, especially in relation to sensitive data, in the UK for instance there is still no mandatory legislation in relation to data security and smart devices: the UK government has, for instance, only published a voluntary code of conduct for manufacturers of smart devices, which advises that, amongst other things, sensitive data should be subject to encryption when transmitted via apps.³³

²⁶ <https://www.americanbar.org/publications/litigation-news/technology/legal-implications-of-data-from-wearable-devices.html>, Accessed 7th March 2018.

²⁷ <https://www.fitbit.com/uk/legal/privacy-policy>, Accessed 8th March 2018.

²⁸ <https://www.apple.com/uk/privacy/approach-to-privacy/>, Accessed 8th March 2018.

²⁹ <https://www.cio.com/article/3185946/wearable-technology/10-things-you-need-to-know-about-the-security-risks-of-wearables.html>, Accessed 8th March 2018.

³⁰ Ibid.

³¹ Ibid.

³² <https://eng.fitbit.com/stepping-up-working-with-the-security-community/>, Accessed 8th March 2018.

³³ <http://www.bbc.co.uk/news/technology-43305346>, Accessed 7th March 2018.

Privacy is another record-keeping issue implicit in wearable technology. The collection of personal data, including sensitive data, via wearable technology means that compliance with the Data Protection Act 1998 in the UK and, from 25th May 2018 onwards, the EU General Data Protection Regulation is imperative; the Information Commissioner's Office in the UK has recently highlighted the 'shortcomings' in this kind of compliance that will need to be remedied to avoid the significant penalties the GDPR stipulates for non-compliance.³⁴ Larger companies such as Apple do have privacy policies in place in relation to the records and data they collect, and during its own analysis of data, Apple makes use of Differential Privacy so that it can learn about the 'user community without learning about individuals within the user community', a model that may be employed elsewhere in relation to data privacy.³⁵ Privacy policies are mandatory for third party apps that use Apple's Healthkit.³⁶ In turn, these apps using Healthkit are prohibited from using or disclosing data to other parties 'for advertising or data mining'; it is only with a user's permission that they can share data for research purposes.³⁷ Privacy is something that both companies and users have some responsibility for, however, as illustrated by the recent case concerning Strava, a running app that allows users to record their exercise and share it with others. The app's makers produced a data visualisation map of all its users' activity, in the course of which revealing sensitive information such as the locations and layouts of US military bases in countries such as Syria, where military personnel had been using the app.³⁸ The company was able to construct and publish the map, aggregating and anonymising the data, due to the majority of users not changing their default privacy settings, which allow data to be shared publicly. Non-anonymised data is, however, available on the company's website, which lists individuals' running times and locations, and the dates of their activity. The high level of sensitivity of some of this data has been highlighted in relation to the possibility it raises of the tracking of active military personnel.³⁹ Such a scenario will be less likely under the rules

³⁴ <https://www.tltsolicitors.com/insights-and-events/insight/your-heart-on-your-sleeve-the-data-protection-implications-of-wearable-tech/>, Accessed 9th March 2018; <https://gdpr-info.eu>, Accessed 9th March 2018.

³⁵ https://images.apple.com/euro/privacy/e/generic/docs/Differential_Privacy_Overview.pdf, Accessed 9th March 2018.

³⁶ <https://www.apple.com/uk/privacy/approach-to-privacy/>, Accessed 8th March 2018.

³⁷ Ibid.

³⁸ <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>, Accessed 7th March 2018.

³⁹ <https://www.theguardian.com/technology/2018/jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban>, Accessed 7th March 2018.

of the GDPR, which will ensure that users opt-in to allowing their information to be used in this way.⁴⁰

A related issue to those of the ownership of records containing data from wearables and the privacy with which they can or should be treated are the issues of the accessibility and usability of these records. Several years ago, in 2015, data was accessible to users for export from smartphones' activity monitors, though it was not necessarily easy to export and convert into records that would be easily usable: for example Apple's Health app gave users their data in XML format.⁴¹ The development of apps such as Hipbone, which automatically backs up data from activity monitors and iPhones to a Dropbox account, is an example of the kind of innovations that have made it easier for users to access and to use their data, thereby creating their own records as well as being stored on proprietary or third party servers.⁴²

Whilst the record-making and record-keeping afforded by wearable technology, particularly activity monitors, have huge identified and potential benefits to improving health and leading to innovations in medical treatment, there is also much discussion on the potential pitfalls of creating and keeping these data and records, especially those from everyday activities not collected for specific analysis within a medical context: how healthy for society is this mass of data and records regarding activity and health?⁴³ There are concerns that this intensive monitoring, sharing, and retaining of these data and records may cause, or be symptoms of, anxiety, health-obsession, and narcissism. Yet records and data regarding other aspects of life, such as identity, are not considered as such. This may be where record-keepers' skills and methodologies can make an additional contribution to the area of wearable technology, in advocating for and applying skills of appraisal to records and the data they contain.

p

Bibliography

⁴⁰ <https://www.itgovernance.eu/blog/en/gaining-explicit-consent-under-the-gdpr-2/>, Accessed 9th March 2018.

⁴¹ https://www.buzzfeed.com/stephaniemlee/who-owns-your-steps?utm_term=.wKdKmxkrQ#.efDaZBaQ6, Accessed 8th March 2018.

⁴² <https://hipboneapp.com>, Accessed 8th March 2018.

⁴³ On the limitations of these records and data, see the section on Larry Smarr at http://www.washingtonpost.com/sf/national/2015/05/09/the-revolution-will-be-digitized/?utm_term=.c7fe927e1506, Accessed 9th March 2018.

Arriba-Pérez, F. de., et. al., 'Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios', *Sensors*, 16:9 (2016), available at <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5038811/>, Accessed 9th March 2018.

BS ISO15489-1-2016, Information and Documentation - Records Management. 1: Concepts and Principles (British Standards Institute, 2016).

<https://www.americanbar.org/publications/litigation-news/technology/legal-implications-of-data-from-wearable-devices.html>, Accessed 7th March 2018.

<https://www.apple.com/uk/privacy/approach-to-privacy/>, Accessed 8th March 2018.

https://www.buzzfeed.com/stephaniemlee/who-owns-your-steps?utm_term=.wkDkMxkrQ#.efDaZBaQ6, Accessed 8th March 2018.

<https://www.cio.com/article/3185946/wearable-technology/10-things-you-need-to-know-about-the-security-risks-of-wearables.html>, Accessed 8th March 2018.

<https://eng.fitbit.com/stepping-up-working-with-the-security-community/>, Accessed 8th March 2018.

<https://www.fitbit.com/uk/legal/privacy-policy>, Accessed 8th March 2018.

https://images.apple.com/euro/privacy/e/generic/docs/Differential_Privacy_Overview.pdf, Accessed 9th March 2018.

<https://gdpr-info.eu>, Accessed 9th March 2018

<https://www.igi-global.com/dictionary/smart-technology/38186>, Accessed 7th March 2018.

<https://www.itgovernance.eu/blog/en/gaining-explicit-consent-under-the-gdpr-2/>, Accessed 9th March 2018.

<https://hipboneapp.com>, Accessed 8th March 2018.

<https://www.theguardian.com/commentisfree/2017/jul/23/the-return-of-google-glass-surprising-merit-in-failure-enterprise-edition>, Accessed 6th March 2018.

<https://www.theguardian.com/technology/2017/apr/25/fitbit-data-murder-suspect-richard-dabate>, Accessed 7th March 2018.

<https://www.theguardian.com/technology/2017/may/24/fitness-trackers-out-of-step-when-measuring-calories-research-shows>, Accessed 7th March 2018.

<https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>, Accessed 7th March 2018.

<https://www.theguardian.com/technology/2018/jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban>, Accessed 7th March 2018.

<https://www.theguardian.com/technology/2015/jan/06/future-wearable-technology-analysing-data>, Accessed 9th March 2018.

<https://www.telegraph.co.uk/technology/apple/11395073/What-is-Apples-HealthKit.html>, Accessed 8th March 2018.

<https://www.tltsolicitors.com/insights-and-events/insight/your-heart-on-your-sleeve-the-data-protection-implications-of-wearable-tech/>, Accessed 9th March 2018.

<https://www.wareable.com/fitness-trackers/how-your-fitness-tracker-works-1449>, Accessed 7th March 2018.

http://www.washingtonpost.com/sf/national/2015/05/09/the-revolution-will-be-digitized/?utm_term=.c7fe927e1506, Accessed 9th March 2018.

<https://www.wired.com/2013/12/wearable-computers/>, Accessed 7th March 2018.

<https://www.youtube.com/watch?v=Ae81FcczsI8>, Accessed 6th March 2018.

<https://www.youtube.com/watch?v=XCsGLWrfE4Y>, Accessed 6th March 2018.

<https://www.youtube.com/watch?v=ZVtURELhy1w>, Accessed 6th March 2018.

Kroll, R.R., et. al., 'Accuracy of a Wrist-Worn Wearable Device for Monitoring Heart Rates in Hospital Inpatients: A Prospective Observational Study', *Journal of Medical Internet Research* 18 (9), 2016.