Summary

Data security and privacy when using physiological wearables in the judicial context
A case study with the Empatica E4

Background and research questions

Research shows that technological self-measurement methods have the potential to personalize treatment, improve security in detention, enrich probation supervision and increase the self-reliance of offenders. Nevertheless, there are also serious concerns and risks associated with the use of technological self-measurement methods. For example, it is often unclear what exactly happens with the data after they are collected. Data collected with technological self-measurement methods are often accessible to the manufacturer and may be shared with third parties. The technology itself is also sometimes vulnerable, resulting in the interception or theft of data by third parties. This is certainly not desirable in the judicial context – where security and privacy protection are paramount. Before technological self-measurement methods can be used on a larger scale in the judicial context, it is therefore important to investigate the state of data security regarding self-measurement methods, and to assess what could be done in the judicial context to ensure the security of the collected data and thereby the privacy of those involved.

In this report, we describe a case study on data security and privacy, focusing on physiological wearables. These are portable devices that are worn around the wrist or on the body and with which physiological data can be collected by means of sensors. We conducted this case study with a specific wearable: the Empatica E4.

The following questions were answered:
1. What happens to the physiological data of the Empatica E4 after these have been collected by the user with regard to: data storage, data transfer and third party access? How is the data secured?
2. What are the risks for the security of the data and for the privacy of the wearer? And how does the Empatica E4 compare to other wearables regarding risks and functionality?
3. What are the knowledge, experiences and concerns of professional users of the Empatica E4 regarding data storage, access to data by third parties and privacy?
4. What do the answers to the sub-questions mean for the use of the Empatica E4 and other physiological wearables in the judicial context?

Based on the case study, we make recommendations about how best to deal with the security and privacy of data collected with physiological wearables in the judicial context. Security of the data relates to the security regarding data storage and transmission. In this report, privacy means the protection of the collected (personal) data of the wearer of the physiological wearable against disclosures.

This report mainly discusses the use of wearables for research, treatment or supervision in the judicial context. We distinguish between the user and the wearer. The user (for example a researcher, forensic clinician or probation officer) is the person who...
who collects, stores, processes, analyses, and deletes the data. Often the user is also the person who purchases the wearable, enters into the agreement with the manufacturer, and provides his or her personal data to the manufacturer (for instance to make an online account). The wearer is the person who wears the wearable and whose physiological data are collected. The wearer can, for example, be a detainee who takes part in scientific research.

**Methods and Limitations**

Questions 1 and 2 were answered by carrying out desk research. Information and documentation about security and privacy was searched on the Empatica-website and additional questions were asked via email to Empatica. An account was created to try out the storage, transfer and use of data with the Empatica E4 in practice. For the comparison of the data security and privacy of the Empatica E4 with those of other wearables (part of question 2), relevant wearables were searched by consulting various internet sources using systematic search terms and by questioning experts. For the analysis, we only selected wearables that, like the Empatica E4, can measure skin conductance and/or heart rate, and ideally also movement and/or skin temperature. Question 3 was answered by means of a short survey among ten professional users of the Empatica E4, and question 4 was answered on the basis of the findings regarding the first three questions.

In this study we compared the Empatica E4 with a number of other wearables. On the one hand we looked at the functionality offered and on the other hand at the data security and privacy. An important limitation is that this comparison is not exhaustive. A limitation is that we were not able to map all risks relating to data security and privacy for all wearables in detail because we collected the information through public sources like websites. These sources do not always include all details for each wearable. Another limitation is that we investigated the user experiences in a very small sample of ten users (partly because there are few users in the Netherlands). This consultation also took place before the General Data Protection Regulation (GDPR) came into effect and the knowledge of users may have increased in the meantime.

**Data security and privacy when using the Empatica E4**

The Empatica E4 wristband which contains four different sensors (skin conductance, heart rate, acceleration and skin temperature) can be used in two ways. In streaming mode, the wristband data are displayed directly in real time in an app on a mobile device. This data is then automatically uploaded to the user's E4 Connect account on Empatica's servers. In recording mode, after connecting the Empatica E4 to a computer, the data stored on the wristband are automatically moved to a storage location on the computer and then automatically uploaded to the user's E4 Connect account. The data can be viewed on the E4 Connect website.

Such an environment in which data is not stored locally with the user, but on the servers of a third party, is called a cloud or cloud environment. The data in the cloud are accessible from any device with an internet connection. Empatica not only offers data storage with E4 Connect, but offers a website (also called a dashboard), with which the data can be viewed and managed.
Our case study shows that Empatica has taken several measures to secure the physiological data of the wearers during transport and when storage on Empatica’s servers against possible interception by third parties. For example, the data are linked to the user and not to the wearer, are stored in a special format and the data transfer is encrypted. As a result, the physiological data (from the wearer of the wristband) can only be traced back directly to individual persons by the user and not by the manufacturer. Nevertheless, we see various risks regarding the security of the collected data and the privacy of the wearer.

**Security risks**
The most important security risk is that the physiological data are automatically transferred to the online environment of the manufacturer. Local (offline) use of the wristband is not (easily) possible. Sending data over the internet and storing them in the cloud involves a greater risk of intercepting or stealing data by third parties than a solution that works completely offline and uses local storage. In the case of local offline storage, intercepting or stealing data is more difficult because the storage must first be accessed physically (while the cloud storage can be hacked or attacked remotely). With local use, the user has more flexibility and control over, for example, where the data collected are stored, and data from wearers are not (automatically) shared with an external party. The user is then responsible for adequate security of the devices on which the data are stored and analysed.

**Privacy risks**
Because the physiological data can say something about a person’s health, these belong to a special category of personal data (in the sense of the GDPR) that need to be protected more. These data must therefore be handled with care, in accordance with the (privacy) legislation applicable, in order not to harm the privacy of the wearer. Because the Empatica E4 uses a cloud environment, in which Empatica becomes the processor of the data, it is important to have a (privacy) lawyer conclude a data processing agreement with Empatica. This is mandatory to comply with privacy legislation. After inquiries from our side, Empatica has indicated to be willing to conclude such agreements, and that customization is possible. The agreement should include in which country the data will be stored, who will have access to the data and for how long they will be stored. For use in the judicial context, it should for instance be possible at any time to have all physiological data of wearers such as detainees completely and permanently erased.

**Comparison data security, privacy and functionality of the Empatica E4 with other physiological wearables**
Several manufacturers have developed wearables for use by professionals in research or treatment. In addition there are consumer wearables available that could also be used for research, treatment or supervision.

What is striking when looking at instruments intended for treatment and research is that there are roughly two variants: 1) wearables or portable devices for use in a lab or at a fixed location; and 2) wearables suitable for larger-scale research and/or remote treatment, with many different participants in different locations. Offline solutions are available for the first group. These wearables also offer users more configuration options, allowing them to determine which measurements are collected and where they are stored. The user is then responsible for taking measures to protect the data. Due to the many possibilities, some of these wearables seem to
require more technical expertise to use. In the second group of wearables, it is striking that all providers, like Empatica, opt for a cloud solution. This makes it easier for users to conduct larger studies. In addition, participation in a study is easier for the wearers: it is not necessary to come to a lab, the band can be worn at home for a long time (some products are even waterproof), and it takes little effort to send the measurements to the user because this is largely automated. For some products, the wearers can also gain (real time) insight into their own measurements by using a mobile app (none of these products have a screen on the wearable itself to show physiological data in real time).

The use of consumer wearables, mostly smartwatches, for research or treatment is also possible. This has the advantage that the wearer himself can keep an eye on the measurements (by using the directly readable screen and/or using an app) and at the same time use the other functionalities of the smartwatch. A disadvantage for the use of these wearables in the judicial context is that these instruments currently have (much) fewer sensors than the products aimed at professionals. For example, there are not many smartwatches that can measure skin conductance, but many smartwatches do contain a heart rate sensor. Furthermore, the sensors may not always be validated. These smartwatches generally use the cloud to store physiological data.

Our comparison showed that there are not many wearables on the market that, like the Empatica E4, both provide a combination of several different physiological sensors (both heart rate and skin conductance sensor), and are easily usable. There are instruments that do contain these sensors, but these make use of (less user-friendly) patches. However, several instruments do score better than the Empatica E4 in terms of: the possibility to use the instrument completely locally without the need for the cloud or a cloud service with better security measures.

Experiences of professional users

Although a majority of the users of the Empatica E4 have read the privacy statement beforehand, a third of the users have not. It is therefore not surprising that most of them do not know or answer neutrally to a question about how the manufacturer of the wearable deals with data storage and access. Hardly any user knows where and for how long the collected data are stored. There are also concerns about access by third parties and misuse of data. In conclusion, users are concerned about the security of data storage and access, but nevertheless use the wearable. This is called the ‘privacy paradox’ and may be due to the fact that there are few alternatives available.

The use of physiological wearables in the judicial context

Based on our case study, we distil a number of aspects and recommendations that are important for the use of physiological wearables in the judicial context and more specifically the collection of physiological data from detainees, forensic patients, parolees or other subjects within the criminal justice system.
Important options for physiological wearables in the judicial context
The following characteristics are important for a wearable in the judicial context with respect to data security and privacy:
- the possibility of full local use; or
- if online use is (also) desirable: adequate security options and a data processing agreement that complies with the applicable privacy legislation;
- the possibility to selectively switch on and off individual measurement functions.

In addition, with respect to functionality and ease of use (partly depending on the desired application), it is important to have the following characteristics:
- a good range of reliable, valid and accurate measurement functions such as heart rate, skin conductance, movement and (skin) temperature;
- sufficient wearing comfort so that the wearable can be easily integrated into everyday life;
- the possibility of a feedback function (for example via an app on another mobile device or via a screen on the device itself).

The choice of a particular instrument and its suitability depends on the precise purpose (for example: which measuring functions are required, whether direct feedback to the wearer via a screen is required, etc.). Our research reveals two variants: an offline variant and an online variant. Which variant is preferred in the judicial context depends on the aim, subjects and specific context of the research, treatment or supervision. An analysis of possible risks regarding data security and privacy is in all cases of crucial importance.

Recommendations
Based on this case study, we have the following three recommendations.

1 Encourage awareness, but also responsible behaviour, regarding data security and privacy risks among employees who use physiological wearables in pilots, scientific research, treatment or supervision.
Use the possibilities of physiological wearables in research and for treatment and supervision, but facilitate that this is done responsibly and ensure that the applicable privacy legislation is complied with. From a legal point of view, users are required as controllers to demonstrate that data are processed in accordance with privacy legislation. Users of wearables therefore play an important role in handling the collected data safely (for example: protecting data with a strong password, erasing data from the cloud environment as quickly as possible, not measuring more aspects than necessary).

2 Before selecting a wearable, perform a risk analysis with regard to that wearable and apply the principles of privacy by design.
The ex-ante risk analysis should focus on the above-mentioned issues of data security and privacy. It is recommended to consult a Privacy Officer and/or Chief Information Security Officer. This also fits with the concept of privacy by design: paying attention to and taking privacy into account in the early phases of a project. In the judicial context, it is therefore advisable to use the following concrete method for research, treatment or supervision with physiological wearables: The user takes appropriate technical and organizational measures, follows the principles of privacy by design and, as controller, demonstrates compliance with privacy legislation by among other things:
- maintaining a record of processing activities;
- conducting a Data Protection Impact Assessment (DPIA);
• concluding a data processing agreement with the data processor (if applicable).

The often vulnerable target group is handled with care:
• members of the group of interest are asked if they want to take part and wear the wearable (this cannot be compulsory);
• the wearer is informed about the purpose of the research study, treatment or supervision, about the consequences of wearing and what happens to the physiological data, so that he or she can make an informed decision whether or not to participate;
• consent of the wearer is recorded in writing and can be withdrawn at any time.

3 If necessary, invest in adapting the software of an existing wearable in such a way that it meets the characteristics that are desirable for use in the judicial context.

There are various practical examples of research projects in the Netherlands in which the software of the wearables has been adapted. A disadvantage of adapting an existing (commercial) wearable may be that there is still dependence on a commercial third party. This can have financial consequences and there is also a risk that production will stop and support and updates may cease, and the instrument will become obsolete or security will deteriorate. In order to have full control over the functionalities and to meet the security and privacy requirements, the Ministry of Justice and Security could itself invest in developing or continuing the development of an (existing) wearable.