Paying via a wearable device: the legal issues to consider

While wearable devices such as the Apple Watch are on the radar of both consumers - thanks to some high-profile launches of such products - and the technology sector, with companies such as Google buying up patents, wearables have not fully hit the mainstream yet. In this article, Edwin Jacobs and Ruben Roex of time.lex argue that payments could be the added value needed to really propel wearables into the mainstream. The use of wearables for payments however triggers a number of legal issues, which range from data protection and privacy concerns to considerations relating to unauthorised payments resulting from wearable technology. Edwin and Ruben discuss the relevant legal issues connected to the use of wearable devices for payments.

Wearable technologies have been in the public spotlight for a while now, with the smartwatch arguably being the poster boy for this new type of consumer device. And although the market for wearables shows great growth potential, at the moment mainstream adoption of these devices is still lacking. One of the reasons often cited why broad consumer adoption of wearables remains elusive is that consumers do not fully understand what added value wearable technologies can offer them. What is missing is that killer app or feature that really provides the catalyst for the wearables market to take off.

Payments might just be the domain where this killer app/feature comes from. The inclusion of payment technology in wearable devices, while not a new idea, has only recently had its first credible mainstream introduction with the launch of Apple Pay together with the Apple Watch. In the Android ecosystem as well there have been manufacturers incorporating payment capabilities into their wearables. Wearables indeed offer clear added value for payments, including increased convenience, speed and (in time) security as well as cost savings at the point of sale ('POS'). But with the market in its infancy, there are clearly a few hurdles still to overcome.

These legal hurdles are associated with wearables in general and when incorporating payment solutions especially. The legal issues come from many different angles, including privacy and data protection, payments law, consumer protection law, intellectual property, cyber crime and labour law and insurance. In this contribution the authors touch upon each of these angles and identify several core challenges posed by legislation, with slightly more emphasis placed on privacy/data protection and payments law.

Privacy and data protection

The legal risks associated with wearables have most commonly been analysed from the angle of privacy and data protection. That privacy and data protection are major concerns should not come as a surprise. Indeed, one of the main characteristics of a wearable is that it is necessarily very intimately linked with the wearer, who has it with them wherever they go. Wearables, such as smartwatches, are also stuffed with all kinds of sensors, giving them a sort of contextual awareness as well as the ability to acquire, store and transfer significant amounts of information regarding that context and - by extension - about the wearer. Hence, the potential impact on the wearer's privacy and right to data protection can be quite vast.

Smartphones

However, we would dare to assert that the same considerations apply to most smartphones, which are equally sensor rich and closely tied with their owners. This assertion is backed by the observation that most of the commercialised wearables today are nothing more than extensions of the smartphone, and for most of their features utterly dependent on a permanent connection with the phone. Moreover, people tend to take their smartphones wherever they go, even to more intimate places such as bathrooms and bedrooms, similar to how one would treat a wearable device. Of course, much will depend on the application of the wearable. A device implanted in one's body that is meant to capture medical data relying on a range of biometric sensors will have more profound implications than a smartphone with a

fingerprint sensor. But all in all, the challenges created by wearables are comparable to those created by smartphones.

Legal roles in the ecosystem

One of the principal challenges with respect to the protection of personal data in the context of wearables is the multitude of stakeholders and the roles each of them has to play. In data protection law, most obligations rest on the data controller and - to a lesser extent - on the data processor, while rights of protection are offered to data subjects. The correct assignment of these roles is therefore key to compliance, and among others instrumental for determining who has to provide information regarding the processing etc. Yet, since wearables are often part of a larger ecosystem in which many players operate, correct assignment can be quite a challenge. Moreover, a single player can assume different roles, depending on the processing under consideration. Hardware manufacturers, developers of operating systems, app developers, service providers offering services such as payments or cloud storage and even the wearers themselves can all have such differing roles. This complicates the correct interpretation and application of the law. Guidance provided by national supervisory authorities and supranational bodies such as the Article 29 Data Protection Working Party can help shed light on this issue and assign roles correctly.

Another challenge in this area is the amount of data acquired, combined and subsequently transferred through a network of interconnected service providers. The purposes for which initial acquisition took place might not be the same as those for which data are combined or transferred. This has its implications for the legitimacy of the processing and compliance with the data quality principles. It may be for instance that a wearer consents to the registration of biometric data for the purposes of authentication in a payment app, but that they do not intend these data to be used by a health or fitness application.

One question is whether the wearer can be held responsible for any unauthorised payments if he/she jeopardises the security of their device by tampering with its inherent properties

Finally, data controllers and processors are required to take appropriate technical and organisational measures to ensure the security of personal data processed. For wearables, as with many other embedded devices, different stakeholders are concurrently responsible for the security of the device and the data contained therein. Indeed, since apps and services often use shared data resources, the security of these resources becomes a joint responsibility. Where wearables require the connection with a smartphone the number of responsible stakeholders will be even higher. Given this plethora of responsible entities, security concerns, especially at the early stages of product commercialisation, cannot be neglected and each stakeholder must maximise its own efforts. If and when a data breach happens, it will be difficult to find the responsible entity and to allocate liability for it.

Payments law

As mentioned earlier, payments are an area where wearables could really offer added value. Most commercialised applications nowadays are based on so-called contactless payments relying on Near Field Communication ('NFC'), whereby the wearable (a watch or a wristband) is brought in very close proximity with the payment module of the merchant at the point of sale. Realising this added value necessarily implies that the payment solution offered through a wearable complies with the pertinent legislation. With respect to payments law, issues could arise regarding the authorisation of a payment as well as with the loss of the payment-enabled wearable.

Payment instrument

The first issue that arises is whether the wearable itself should be considered a payment instrument. If it is, then the payment service user - here the wearer - must make sure that they keep the wearable safe. Should they lose their wearable, they would have to notify the payment service provider as soon as possible. This also begs the question as to whether the wearer is still allowed to lend their payment-enabled wearable to someone else. In principle the wearable will be a very personal device, but this doesn't mean that it can't be the case that more than one person uses on occasion the same smartwatch for instance. Another - closely related - question is whether the wearer can be held responsible for any unauthorised payments if he/she jeopardises the security of their device by tampering with its inherent properties (e.g. by gaining root access) or by downloading high-risk apps. These issues are by no means different than when a smartphone is used for making payments, but are still highly relevant.

Unauthorised payments

A second issue pertains to the authorisation of payments made via the wearable itself. There are applications imaginable where the mere proximity of the device to a reader at the POS is enough to authorise a payment. It is easy to see that where the payment is made via a wristband for instance, the payment could potentially be

made by accident and not by deliberate choice. This would mean that the wearer would be able to challenge the authorisation of the payment pretty easily, opening the door to potential misuse. It would mean an almost impossible burden of proof for the payment service provider wanting to challenge the alleged absence of authorisation, as the provider must provide evidence that the wearer did indeed authorise the payment.

Other legal issues

Consumer protection law

The main issue from the angle of consumer protection law pertains to the very extensive information obligations. Payment services offered through wearables often rely on other service providers to get the payment service to the consumer. Consumer protection law obliges such service providers to provide consumers - here the wearer - with pertinent information on the services they provide. It is quite a challenge, however, to provide sufficient information to the consumer where the wearable has virtually no screen real estate to display information on or where a screen is simply not present. Where the smartphone is still needed for the wearable to work, this problem might be solved by showing the relevant information on the phone's larger screen, but with standalone wearables this problem will be quite palpable.

Intellectual property - trade secrets

With regard to intellectual property, the main issues relating to wearables are not significantly different from those that apply to smartphones. Emma Poole of the WIPO indicated in mid-2014 that the "intellectual property arms race" in the wearables sector had begun. The world's largest technology giants including Google, Apple and Microsoft are amassing patents pertaining to wearables at a staggering rate. But one of the main questions concerning wearables and their ability to 'log' their wearer's life will no doubt be who owns the data created by wearable devices. In this age of big data, the value of the raw data produced by wearables and their sensors will undoubtedly be vast. Adding payments data to this will only increase that value, which definitely makes the ownership question a burning one.

Cyber crime

Wearables offering contactless payment functionality entail the risk of so-called digital pickpocketing. The process involves the configuration of a mobile phone as a RFID scanner and then the use of that mobile to exploit the contactless payment functionality of the wearable. Such actions are criminalised in the Cybercrime Convention as illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery and fraud. Wearables do not only pose a risk from cyber criminals, however, but also from law enforcement. Indeed, given the wealth of information that a wearable contains, search and seizure of such a device is much further reaching. This implies that law enforcement agents should only be allowed to search the contents of a wearable when they have obtained a proper mandate from a competent member of the judicial authorities.

Labour law

Last but not least, wearables have significant implications when used in the workplace. Issues include easier theft of corporate trade secrets since these devices can be used covertly but also enhanced monitoring capabilities for employers. Given specific data protection rules that often apply in a labour context, it will be very important to cover these issues thoroughly in labour agreements and regulations.

This contribution has concisely highlighted several highly relevant legal issues and challenges related to wearables. What is important to take away from this is that many of these issues are not new but are very similar to those associated with smartphones. As wearables develop further, however, the differences between wearables and smartphones will no doubt become more pronounced and the legal implications more specific.

Edwin Jacobs Partner
Ruben Roex Lawyer
time.lex, Brussels
edwin.jacobs@timelex.eu
ruben.roex@timelex.eu