PRIVACY IMPLICATIONS OF WEARABLE TECHNOLOGIES – THE CASE OF SMART GLASSES

Category: Commercial Law,Privacy Law, Infosec, and POPIA
written by Tshepiso Hadebe | January 27, 2022

Introduction

The Internet of Things ("**IoT**") refers to the interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data. The IoT has become one of the most important emerging technologies. There are various devices that form part of the IoT, including wearable technologies.

As it stands there is no universally agreed upon definition of wearable technology. However, key elements of wearable technologies are that they are carried on or worn or embedded in the user, and the track and store data about the user. Such devices have the enhanced ability to send and receive data via the Internet. Importantly, these devices can only reach optimum performance by collecting personal information from the user. This includes information such as the user's personal health, GPS location, gender, contacts, search history and purchasing data. Such information, although relatively safe when isolated, together such information can reveal details such as a home address and passwords. The rapid adoption of such devices has placed wearable technologies at the forefront of IoT. This article looks at the privacy implications of the wearable technology known as "smart glasses".

The rise of Smart Glasses

Smart glasses can be defined as wearable computers with a mobile internet connection that are worn like glasses. The release of Ray-Ban Stories: First-Generation Smart Glasses ("**Ray-Ban Stories**") garnered worldwide attention. They are marketed as a unique tool that allows an individual to "capture life's moments as they happen from a unique first-person perspective".

There has been concerns expressed about the high potential of the Ray-Ban Stories to undermine the privacy of individuals and be used as a tool to secretly surveil people. The stealthy recording capabilities of the Ray-Ban Stories made possible by the cameras fitted into them and their ability to take photos and record up to 30-second videos make them a perfect surveillance tool. Their inability

to be distinguished from ordinary glasses means they can be exploited as a surveillance tool by various parties, including dictatorial governments.

The Irish Data Protection Commission ("**IDPC**") issued a statement in which it expressed concern about the means by which those captured in the videos and the photos by the wearer of the Ray-ban Stories can receive notice that they are being recorded. The IDPC further stated that while it accepted that many devices including smart phones can record third party individuals, it is generally the case that the camera or the phone is visible as the device by which recording is happening, thereby putting those captured in the recordings on notice. The main issue with the Ray-Ban Stories is that there is a very small indicator light that comes on when recording is occurring. According to the IDPC , neither Facebook nor Ray-Ban demonstrated to the IDPC that comprehensive testing in the field was done to ensure the indicator LED light is an effective means of giving notice.

The Protection of Personal Information Act and Ray-Ban Stories

Given the rise in the popularity of smart glasses, it is likely that Ray-Ban Stories will soon make their way into the South African market. In that case because of their privacy implications, they would have to be subject to the Protection of Personal Information Act ("**POPIA**"). The question becomes whether the Ray-Ban Stories processing of personal information as it is, would be in line with POPIA.

POPIA grants certain rights to data subjects, including the right to be notified if personal information about him/her is being collected (section 5 (a)(i)). Furthermore, Section 18 (1) (a) of POPIA states that if personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of the information being collected. Regulation 4(b) of the POPIA Regulations states that an information officer must ensure that a personal information impact assessment ("**PIIA**") is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.

In the context of Ray-Ban Stories, POPIA would require action similar to that required by the IDPC. The notification requirement set out in section 18 of POPIA would require that Meta (formerly known as Facebook) and Ray-Ban indicate that they have taken reasonably practicable steps to ensure that data subjects are well aware that they are being recorded.

The notification requirements set out under section 18 of POPIA, would ensure that data subjects are well aware that they are being recorded. However, South Africa could stand to benefit from a comprehensive system that lays out the requirements for Personal Information Impact Assessments for emerging technologies. This would ensure technologies like smart glasses, which are likely to result in high risk to data subjects are developed in line with POPIA. They would also enable the Information Regulator to assess the privacy implications of such technologies before they enter South African markets.

The use of Ray-Ban Stories by private citizens

In a case where a user has bought the Ray-Ban Stories and elects to use the glasses for personal uses, the same privacy concerns can be raised if the user decides to secretly record others. Section 6 (1) (a) POPIA states that POPIA does not apply to the processing of personal information in the course of purely personal or household activity. This would mean that users are not required to comply with the POPIA requirement of notification in order to make recordings. However, in cases where the user records others in private settings, they need to respect other people's rights to privacy. Section 14 of

the Constitution of the Republic of South Africa provides that everyone has the right to privacy. In addition to this constitutional right to privacy, the common law also protects this right to privacy. Where such recording has taken place without the knowledge and consent of the said individuals then they can have recourse under the common law right to privacy. However, in instances where the user elects to use the glasses in a public setting, such a recourse might not be available given that in a public setting there is no reasonable expectation of privacy.

Conclusion

Smart glasses are one of many wearable technologies that form part of the IoT. As most of these technologies are emerging at an unprecedented rate , their privacy implications together with the privacy risks have not been fully explored. It is up to regulatory authorities like the Information Regulator to hold the developers of wearable technologies accountable, especially if such technologies are likely to result in high risk to data subjects.

Contact us for more good, clear, precise advice.