Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Asia-Pacific news

Gabriela Kennedy *

Mayer Brown JSM, Hong Kong

Keywords:
Asia-Pacific
IT/Information technology
Communications
Internet
Media
Law

A B S T R A C T

This column provides a country-by-country analysis of the latest legal developments, cases and issues relevant to the IT, media and telecommunications' industries in key jurisdictions across the Asia-Pacific region. The articles appearing in this column are intended to serve as 'alerts' and are not submitted as detailed analyses of cases or legal developments.

1. Hong Kong

Gabriela Kennedy *(Partner), Mayer Brown JSM (gabriela.kennedy@mayerbrownjsm.com);*

Karen H.F. Lee *(Senior Associate), Mayer Brown JSM (karen.hf.lee@mayerbrownjsm.com).*

1.1. *IoT (I Own Thee): Hong Kong releases results of study on wearable technology devices*

In January 2017, the Hong Kong Privacy Commissioner ("**PC**") announced the results of the Hong Kong study of the privacy and security practices and protection measures of manufacturers of wearable technology devices, such as fitness bands.

Wearable technologies are a subset of the Internet of Things ("**IoT**"). They are networked devices that collect vast amounts of data, can track activities and behaviours, and enhance and customise users' experiences. Their popularity is on the rise. However, how transparent are the manufacturers of the wearable technologies regarding their collection and use of personal data? This was the question raised as part of the 2016 Global Privacy Enforcement Network Sweep ("**Global Sweep**"), in which 25 privacy enforcement authorities (including those in Hong Kong, Canada, the UK and Australia) carried out a review.

1.1.1. *The study*

During April to June 2016, the PC carried out a study on five Hong Kong-manufactured fitness bands and their related mobile applications. For the purposes of benchmarking, the PC also examined a popular US-manufactured fitness band.

The main aim of the study was to determine the privacy challenges and implications presented by both fitness bands and IoT devices in general, and to raise the awareness of manufacturers on their obligations under the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**").

Collectively, 314 IoT devices were globally examined as part of the Sweep by the PC and 24 other privacy enforcement authorities. The majority were medical or health related devices (e.g. monitoring sleep and blood pressure) and fitness wearables.

On 24 January 2017, the PC announced the results of the study.

1.1.2. *Key findings*

The PC found that only two out of the five manufacturers in Hong Kong (i.e. 40%) provided their users with a privacy policy

For further information see: www.mayerbrown.com

* Mayer Brown JSM, 16th–19th Floors, Prince's Building, 10 Chater Road Central, Hong Kong.
Email address: gabriela.kennedy@mayerbrownjsm.com.

http://dx.doi.org/10.1016/j.clsr.2017.03.028

on how their personal data would be handled. However, only one of those policies was specifically in relation to the fitness device and set out the types of personal data collected and how it was collected. The other privacy policy was a general one that related to the collection of personal data by the manufacturer's website, and did not address how or what type of personal data did the relevant fitness band collect.

The results of the study in Hong Kong were consistent with the findings of the other 24 privacy enforcement authorities. In short, 59% of the IoT devices examined globally did not provide specific privacy policies tailored to the relevant device, which sufficiently informed users on how their personal data would be collected, used and disclosed.

The PC also found that all five of the Hong Kong-manufacturers examined, required users to not only provide personal data during registration on the related mobile application, but also obtained access to other functions and data on the users' smartphones (e.g. location data, photo albums, social media accounts, camera, etc). Concerns were raised by the PC and other privacy enforcement authorities as to whether or not all of the data being collected by the IoT devices was actually necessary. The PC also noted an inconsistency in the default access settings of the mobile applications, depending on whether or not the user is using the iOS operating system or Android system.

Further, none of the Hong Kong-manufactured fitness bands that were examined provided sufficient information on where the personal data would be stored, or whether third party vendors are used to help store the data. This was again consistent with the global results, where only 32% provided information on how a user's personal data was stored. However, out of these 32%, only a few actually explained to users where their data was stored, the period of retention and the form in which their data was kept.

Despite the current climate of cyber-attacks and data leaks, only one of the Hong Kong-manufactured fitness bands examined committed to users that it would employ security measures to safeguard their personal data. After further enquiries, the PC found that two out of the five local manufacturers did not encrypt the data whilst it was being stored and transmitted (note that two of the other local manufacturers did not respond to the PC's enquiries). In comparison, 51% of the global IoT devices examined provided information to users on how their personal data was being safeguarded.

The study also revealed that none of the local manufacturers informed users how they could delete their personal data collected by the fitness bands and related mobile apps – although one of the local manufacturers did provide users with an email address for the sending of data erasure requests. This is in line with the global results, where only 28% of the IoT devices reviewed provided such information to users.

Lastly, only two of the five local manufacturers provided contact details to users for them to submit any privacy-related queries and to exercise their data access and correction rights. This is lower than the global figure of 62%.

The Global Sweep clearly revealed a general lack of transparency and the potential collection of excessive data amongst IoT devices – or even possibly a lack of awareness by manufacturers of their obligations under data privacy laws.

1.1.3. *Recommendations*

The PC highlighted the need for further transparency and safeguards in relation to the handling of personal data by IoT devices. In particular, IoT devices (and their related mobile applications) should:

- provide a privacy policy to users, which informs them in a clear and simple manner the types of personal data that will be collected, the purpose of collection, any potential transferees of the personal data, and the security safeguarding measures in place;
- adopt privacy as the default position (i.e. "privacy by design") in order to minimise the excessive collection of personal data, including using default settings that are the least privacy intrusive;
- implement security measures to protect personal data whilst it is being transmitted or stored;
- explicitly inform users that they have the right to opt-out of the collection of data that is not relevant to the main function of the IoT device (e.g. phone book, etc);
- provide clear instructions to users on how they can delete their personal data stored on the IoT device, the related mobile application and any backend servers; and
- provide the data user's contact information to consumers so that they have a channel with which to submit any privacy-related queries or data access and correction requests.

Do not assume that a "one size fits all" approach will be sufficient, as this is usually not the case. A common mistake made by data users is to assume that they can simply use the same privacy policy on their website for their mobile applications. However, these privacy policies are usually not appropriate, as they do not specifically address and deal with the particular personal data being collected for the purposes of the mobile applications. Data users should also not forget about their notification obligations under data protection principle 1 of the PDPO, or the direct marketing restrictions.

These observations and recommendations are interesting. To a certain extent they do not move the discussion much further as they zoom into a small section of IoT, namely that of manufacturers of wearable technology devices. The more difficult question concerns the increase of connectivity of day-to-day experiences and the move towards smaller devices, with little or no user interface at all. How realistic in such a context is the fundamental principle of privacy law of notice and consent? How many times should consumers be asked to make decisions about their data given its almost ubiquitous collection?

The concerns surrounding wearable technology, which relate to privacy and security cannot be underplayed. A bigger and very interesting conversation is just beginning.

2. Japan

Kiyoko Nakaoka *(Attorney-at-Law and Patent Attorney), Kubota* (nakaoka@kubota-law.com).