COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

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

ABSTRACT

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. *Always on track? Hong Kong Privacy Commissioner issues guidelines on tracking and monitoring by devices*

On 11 May 2017, the Hong Kong Privacy Commissioner ("**PC**") issued a new Information Leaflet on Physical Tracking and Monitoring Through Electronic Devices ("**Information Leaflet**"). The Information Leaflet provides operators and manufacturers of electronic devices with practical advice on how to ensure compliance with the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**").

1.1.1. *Background*

Internet of Things ("**IoT**") devices provide efficient solutions and methods of tracking and gathering data and other information (e.g. monitoring the contents of your fridge, keeping track of your belongings, recording the number of steps you have taken and tracking your sleep patterns). Common features of IoT devices include the ability to track physical locations and monitor individual behaviour (e.g. through the use of Wi-Fi transmitters or radio frequency identification ("**RFID**") tags). Given the ever increasing popularity of IoT devices, it is inevitable that privacy concerns should arise considering the amount of personal data being collected through such devices. Many users may be unaware that their movements or behaviour are being tracked by their IoT devices, and even fewer are aware how such data may be used. Is it being used to build their profile (e.g. their personal preferences, daily activities, shopping habits, etc) and, if so, how is this profile going to be used in the future? Can the individual concerned review it or have a say regarding its further use?

On 24 January 2017, the PC issued the results of a study on fitness bands and their related mobile applications ("**Study**"). The Study was carried out as part of the 2016 Global Privacy Enforcement Network Sweep ("**Global Sweep**"), which concerned the collection and use of personal data by IoT devices – 25 privacy enforcement authorities (including those in Hong Kong, Canada, the UK and Australia) participated in the Global Sweep. The Global Sweep revealed a general lack of transparency

For further information see: www.mayerbrown.com.

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

http://dx.doi.org/10.1016/j.clsr.2017.06.002

Please cite this article in press as: Gabriela Kennedy, Asia Pacific news, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.06.002

in respect of privacy practices and security safeguards by IoT device manufacturers.[1]

Spurred on by the results of the Study and the Global Sweep, the PC has issued the Information Leaflet as a first step towards tackling the privacy concerns identified in relation to IoT devices.

1.1.2. *Information leaflet*

If the identity of an individual can be directly or indirectly ascertained based on the data being collected by any electronic device that monitors behaviour or tracks physical locations, e.g. IoT devices ("**Devices**"), then this will amount to personal data that is subject to protection under the PDPO and the Information Leaflet. Even data, which by itself may appear to be anonymous (e.g. GPS location data), may still amount to personal data if an individual can be identified when such data is combined with other information held by or accessible to the Device operator.

Prior to launching a Device, operators must first carry out a privacy impact assessment ("**PIA**").[2] The overall aim of the PIA is to reduce the extent and sensitive nature of the data being collected by the Devices; reduce the privacy risks to which individuals are exposed; and provide transparency in order to minimise any surprises to the relevant individuals. The PIA will help Device operators identify and detect any potential privacy issues from the outset, and to address them prior to launch.

Even if the data being collected is not capable of identifying an individual user, the user may still perceive the Device as collecting and using their data in a manner that violates their privacy. For example, targeted advertising based on anonymous profile information. Therefore, the PC recommends that the PIA should be carried out bearing in mind the potential user perceptions in relation to their privacy.

When carrying out the PIA, the Device operators should:

(a) assess each type of data being collected to determine whether or not it is necessary, and whether the collection of such data can be minimised whilst still achieving the same purpose;
(b) assess whether or not the Device operator is transparent with individual users about how their data is being tracked and monitored, and allow the individuals to opt-out where possible;
(c) identify any privacy concerns and implement controls or remedial actions to deal with them; and
(d) keep a record of the PIA analysis carried out, so that the Device operator can rely on it in the event of any investigation or enquiry by the PC.

Manufacturers of Devices are strongly advised by the PC to adopt a "privacy by design" approach. For example, minimising the amount of data being collected to what is essential and implementing default settings that are the least privacy-intrusive.

In addition to the above, the Information Leaflet also provides the following recommendations:

(1) Device operators must be transparent about how they will use the location or behavioural data collected. Individual users of the Device must be informed beforehand, in clear and simple language, about the location or behavioural data which will be collected and the purpose of collection. If the tracking or monitoring features of the Device are not essential to the main function of the Device, then individual users must be notified that they can opt-out and should be provided with an easy mechanism in order to exercise such opt-out rights. If such features are compulsory, then the individual users must be informed of the consequences if they do not want their movements or behaviour to be tracked (e.g. the Device cannot properly function, etc).
(2) If any tracking or monitoring will be carried out for direct marketing purposes (e.g. to send targeted marketing materials to users based on the data collected), then this cannot be done without the individual users' prior consent. The PDPO has stringent requirements on the collection, use and transfer of personal data for direct marketing purposes and such requirements will equally apply to any Devices. For example, if a Device tracks an individual user's preferences in terms of routes for jogging, then using that data to send direct marketing emails addressed to that individual on breakfast offers at restaurants along that route would require the individual user's prior consent. In addition, no such data may be transferred to a third party for them to send direct marketing materials to the relevant individual, unless their prior written consent has been obtained.
(3) Device operators should ensure that no personal data is kept longer than necessary to fulfil the purpose of collection (or a directly related purpose). All practicable steps should also be taken to ensure that the personal data collected is accurate before it is used. This is especially important if adverse consequences may occur or adverse inferences may be drawn in relation to the data. For example, the individual users should be allowed to provide comments before their data is used in any adverse manner.
(4) The personal data collected via the Device should only be used for the purpose (or a directly related purpose) for which it was originally collected, as notified to the individual user on or before the collection of their data. If the Device operator would like to use it for any new purpose, then it must obtain the prior express consent of the relevant individual.
(5) Device operators should implement an appropriate level of encryption to protect the data collected, both during transmission and storage. Internal measures must also be adopted to prevent any unauthorised access of the data by employees or third parties.

[1] For further details on the Study and the Global Sweep, see our article entitled "IoT (I Own Thee): Hong Kong Releases Results of Study on Wearable Technology Devices": https://www.mayerbrown.com/files/Publication/98f5a31d-b5f1-4333-abb4-db11fefdf564/Presentation/PublicationAttachment/90274712-8db3-419a-a123-c128c4da060b/170323-ASI-IP-TMT-QuarterlyReview-2017Q1.pdf.

[2] See the PC's Information Leaflet on Privacy Impact Assessments issued in October 2015: https://www.pcpd.org.hk//english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf.

Please cite this article in press as: Gabriela Kennedy, Asia Pacific news, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.06.002