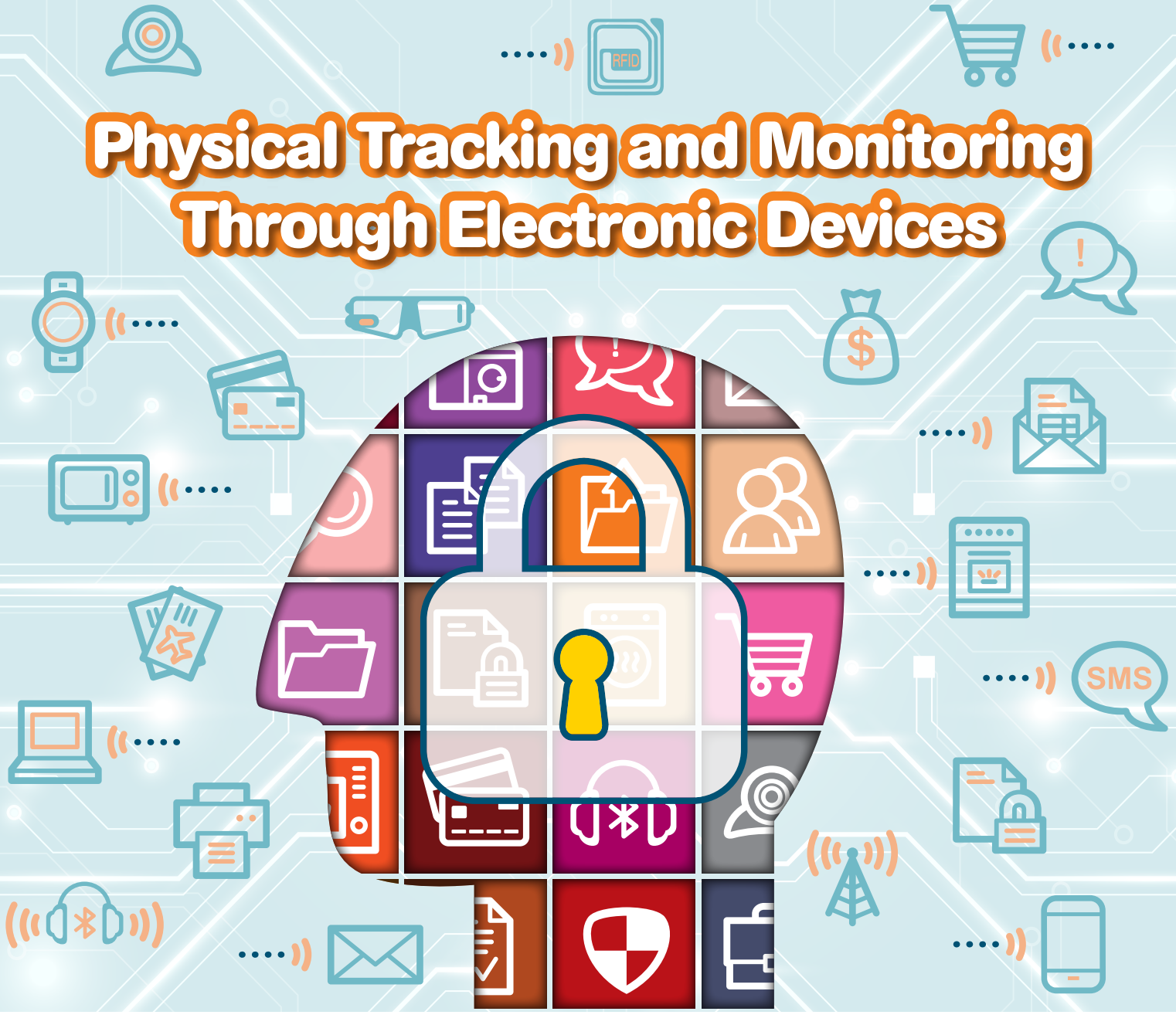
Physical Tracking and Monitoring Through Electronic Devices



PCPD
HK

PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Protect the Data Collected by Physical Tracking or Monitoring

Recommendations for Device Manufacturers

Smartphone manufacturers should:

- allow users to deny mobile apps accessing the location data;
- devise mechanisms to prevent occurrence of tracking without the knowledge of the users.

Manufacturers of IoT devices should:

- provide privacy policies in plain language;
- inform users the types of personal data to be collected, the purposes of collection, the potential transferees of the personal data and the security measures;
- minimise data collection, incorporate sufficient security safeguards and adopt the least privacy-intrusive default settings;
- offer opt-out choice to users for the access to the data that is not relevant to the main purpose of the IoT devices;
- give clear instructions to users on how to delete their personal data stored;
- provide users with contact information for pursuing privacy-related matters.

Manufacturers of wearable devices should:

- ensure the devices cannot read, collect or record data without the users' activation or knowledge;
- ensure that the data will not be used for any purposes about which the users have not been fully informed;
- ensure that no unique identification information of the devices can be read without the users' full knowledge;
- give sufficient warning when the devices collect or record information of individuals other than the users.

Manufacturers that would incorporate RFIDs in their products should:

- clearly inform consumers that RFID tags are used and embedded in products;
- offer options to consumers to disable or remove the RFID tags;
- avoid storing personal data in RFID tags;
- shield the information in the RFID tags from being read by unauthorised parties;
- avoid containing readable unique identification numbers in RFID tags;
- select the read range of RFID tags with due consideration to privacy and data protection.

* For details, please refer to the content of *Physical Tracking and Monitoring Through Electronic Devices*

PCPD.org.hk

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **enquiry@pcpd.org.hk**

First published in May 2017

PCPD H K
PCPD.org.hk
Information Leaflet
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Physical Tracking and Monitoring Through Electronic Devices

Executive Summary

Tracking the physical locations and monitoring the behaviours of individuals through electronic devices, like Wi-Fi transmitters and radio frequency identification ("**RFID**[1]") tags, are becoming increasingly common nowadays. Monitoring by, for example, scanning the RFID tags on the goods carried by an individual may even reveal his intimate information like health conditions, and as a result cause intrusion to his privacy. More significantly, the data collected by physical tracking or monitoring may reveal the identities of the individuals concerned, and hence may be caught by the provisions of the Personal Data (Privacy) Ordinance (the "**Ordinance**"). Core requirements of the Ordinance will be elaborated in this leaflet.

Any person or organisation planning to roll out tracking or monitoring by electronic devices should perform Privacy Impact Assessment ("**PIA**") to minimise-

(a) the extent and sensitivity of data collected;

(b) any surprises to the affected individuals; and

(c) the privacy risk posed to the affected individuals.

Best practice recommendations on PIA will be discussed in this leaflet.

There are also a number of steps that should be taken by manufacturers of electronic devices to minimise the negative impact of the devices on personal data privacy. For example, a manufacturer should be transparent in its privacy policy and the privacy settings of its devices. The manufacturer should also adopt a "Privacy by Design[2]" approach by, for example, minimising data collection and incorporating sufficient safeguards to protect personal data. The practicable steps for data protection will be set out at the last section of this leaflet.

Introduction

Tracking the physical locations and monitoring the behaviours of individuals through electronic devices, like Wi-Fi transmitters and RFID tags, are becoming increasingly common nowadays. Tracking and monitoring arrangements may be intended for the management of logistics, the workforce, the safety of people and the security of goods; for marketing activities; or for other purposes, such as enabling the use of "smart" appliances including smart thermostats[3], smart refrigerators[4] and environmental control systems at home. The technological developments on this front reflect innovations often referred to as the Internet of Things ("**IoT**"), whereby increased connectivity amongst people, their belongings and their environment can improve efficiency, safety and wellbeing, but at the same time raise important personal data privacy issues.

This leaflet aims to highlight the personal data privacy concerns arising from tracking and monitoring. This leaflet does not, however, address privacy issues related to the use of closed circuit television ("**CCTV**") systems (or similar devices) for surveillance purposes. These issues are examined separately in the *Guidance on CCTV Surveillance and Use of Drones*[5] published by the Privacy Commissioner for Personal Data, Hong Kong ("the **Commissioner**").

1 RFIDs usually refer to devices with embedded radio wave equipment that can transmit electronic identification signals (usually unique numbers) wirelessly to other devices. Apart from storing the unique identifiers, RFIDs may also be able to store and process other data.

2 "Privacy by Design" refers to a practice in which privacy protection would be considered at the design stage of products, with privacy-protecting measures incorporated into the designs of the products concerned.

3 Smart thermostats control room temperature automatically by using sensors and real-time weather forecasts, reducing energy consumption, saving bills and keeping the room temperature comfortable.

4 Smart refrigerators, equipped with internal cameras and sensors, can alert users to restock. The users can also go online to make purchases via the smart refrigerators.

5 Available at www.pcpd.org.hk//english/resources_centre/publications/files/GN_CCTV_Drones_e.pdf

What is Physical Tracking or Monitoring by Electronic Devices?

An individual's whereabouts, profile or behaviour may be tracked or monitored directly or indirectly by electronic devices (or goods with wireless communications components, such as a Wi-Fi transmitter or a RFID tag) that are carried or worn by him, or installed in his home or workplace.

Workforce movements may also be monitored through the use of company-supplied mobile applications ("**apps**") or smartphones. Similarly, shoppers may be tracked and profiled through their carrying of smartphones and other objects with RFID tags attached, such as credit cards, stored value cards, or merchandise embedded with RFID tags which were originally intended only for supply-chain management. The adverse privacy implications and risks associated with physical tracking or monitoring arrangements are similar in these cases, regardless of their original purposes. Whilst installing data transmission equipment in appliances, environmental control systems and other equipment at home can bring great benefits to consumers, it can at the same time generate significant volumes of potentially sensitive personal data about the consumers.

Is Data Collected Through Physical Tracking or Monitoring Personal Data?

If data collected through physical tracking or monitoring can be used to identify an individual, the data may be considered personal data under the Ordinance[6]. Accordingly, individuals and organisations that control the collection, holding, processing and / or use of such data may be considered data users under the Ordinance.

In the course of tracking the movements or monitoring the behaviours of individuals, the trackers (individuals or organisations) may not be able to ascertain the identities of the individuals concerned and, as such, the collected data may be considered as anonymous, e.g. time-stamped movement records of unidentified shoppers used to evaluate traffic patterns within a shopping centre. However, this anonymous data, when combined with other data (such as time-stamped sales records in shops, card payment records at car park barriers or Wi-Fi log-in information collected on premises), may lead to the identification of individuals. Once the identity of an individual has been established, his identity and the other information obtained through the tracking or monitoring may be considered to be personal data under the Ordinance.

Trackers and monitors are also reminded that while many tracking or monitoring arrangements may aim only at identifying groups of individuals rather than the individuals themselves, the data collected may enable the trackers or monitors to identify the identities of individuals of those groups, especially when combined with other data that is already in the possession of or readily available to the trackers or monitors. In the circumstances, the data collected may be personal data.

In other words, if a tracker or monitor already holds records of personal data of certain individuals (e.g. as customers or employees) and links the tracking or monitoring information to such records, the information relating to the tracking or monitoring of the behaviours or activities of the individuals concerned may be considered as personal data in totality.

What are the Privacy Risks Associated with Physical Tracking or Monitoring?

Apart from the possible risk of identification of individuals by combining anonymous data collected through physical tracking or monitoring arrangements with other personal data, there are other related privacy risks, including profiling and labelling of the individuals, and adverse effects on the individuals, intended or unintended by the trackers, monitors or third parties.

Personal data privacy concerns arise where individuals are unaware of the existence of the tracking or monitoring arrangements, their purposes, the intended or unintended adverse effects on the individuals concerned, and whether the individuals can opt out of the arrangements.

---

[6] "Personal data" is defined under the Ordinance to mean any data:-

(a) relating directly or indirectly to a living individual;

(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

(c) in a form in which access to or processing of the data is practicable.

The tracking or monitoring of individuals' movements and locations, and the time of staying in each location, may enable the profiling of the individuals, indicating their personal preferences, interests, genders, or spending power. This profiling information, accurate or otherwise, may be further used by the trackers, monitors or third parties to, for example, label the individuals, causing them vulnerable to discrimination, or exclude the individuals from eligible services or treatments as a result of the conclusions drawn on the basis of their profiles which indicate that they are not valuable customers.

Many RFID tags attached to merchandise are designed to send standard Electronic Product Codes to RFID readers, disclosing the details of the merchandise that individuals are carrying. This could facilitate quite detailed information being provided to the trackers, monitors or third parties, for extended profiling of the individuals, such as the brands and sizes of their clothing, the brands and types of their wristwatches, the titles of books they are reading, the types of credit cards they hold, and even the types of medicine they carry. The tracking of goods carried by individuals therefore also poses personal data privacy risks.

If trackers or third parties are able to profile or guess otherwise hidden characteristics of individuals without the individuals' knowledge, any decision made on the basis of such profiling may have negative impacts on the individuals concerned, for example, adverse decisions or even discrimination based on inaccurate profiling. The individuals concerned may not be aware of the adverse decisions or their basis and as a result will not have the means to redress the impacts.

Compliance with the Law

Data users who collect, process and / or store personal data obtained through tracking or monitoring should familiarise themselves and comply with the provisions under the Ordinance and its six Data Protection Principles ("**DPPs**"). The requirements and their applications are demonstrated in the following examples:

DPP1 - Purpose and Manner of Collection

- Personal data shall only be collected for a lawful purpose that is directly related to a function and activity of the data user;
- The personal data collected should be adequate for the purpose and not excessive; and
- All practicable steps should be taken to inform the data subjects concerned of the purpose for which the data is collected and to be used[7].

Under this principle, data subjects should be informed in clear terms of the purposes of collection of their location and / or behavioural data. If tracking or monitoring is optional, data subjects should be clearly informed that they have a choice to opt out. On the other hand, if tracking or monitoring is compulsory, as in some of the worksite-related safety schemes, data subjects should be informed of the consequences if they do not wish to be tracked or monitored. If tracking or monitoring is for direct marketing purposes, data subjects should be clearly informed of such arrangement for which their consent must be obtained[8].

DPP2 - Accuracy and Retention Period

- All practicable steps shall be taken by a data user to ensure:
  - the accuracy of personal data before use; and
  - that personal data is not kept longer than necessary by the data user and its contractors.

If, for example, adverse action may be taken against data subjects based on the attendance data collected by tracking at the work place, the data subjects should be offered an opportunity to comment on the data collected and the actions to be taken.

DPP3 - Use of Data

- Unless the data subjects concerned have given prior consent, personal data shall be used only for the purpose(s) for which it was originally collected (or for a directly related purpose).

[7] See *Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement* issued by the Commissioner, available at www.pcpd.org.hk//english/resources_centre/publications/files/GN_picspps_e.pdf

[8] See *New Guidance on Direct Marketing* issued by the Commissioner, available at www.pcpd.org.hk//english/resources_centre/publications/files/GN_DM_e.pdf

A PIA[9] (more details to be explained in the next section "Best Practice Recommendations") should be carried out whenever there is a possibility of "function creep" to a tracking or monitoring arrangement. The PIA should determine if consent from the data subjects is required for the new functions.

DPP4 - Data Security

- Data users shall take all practicable steps to ensure that personal data is protected against unauthorised or accidental access, processing, erasure, loss or use, having regard to the harm that could result.

Data users should adopt, for example, an appropriate level of data encryption to protect tracking or monitoring information in transmission or in storage, and prevent unauthorised "cloning" of data in storage and "skimming" of data in transmission. Internal policies and procedures should be adopted to safeguard the security of tracking or monitoring data against unauthorised use by employees or other parties who have access to the data.

DPP5 - Policy and Transparency

- Data users should set out policies and practices in relation to the handling of personal data[10].

If, for example, a shopping centre collects location data of shoppers through the articles the shoppers carried, prominent notices should be displayed at appropriate places (including entrances) to alert the shoppers of this arrangement, including the purpose of collection and the potential transferees of the data. The shoppers should also be well informed of and provided with simple means to opt out.

DPP6 - Access and Correction

- Data users should comply with data access[11] or data correction[12] requests within the time limit imposed by the Ordinance.

If, for example, a shopping centre plans to collect personal data of shoppers, it should develop a mechanism for the shoppers to access or request correction of such data before the arrangement is carried out.

Best Practice Recommendations - Engaging a Privacy Impact Assessment

Anyone who plans to track or monitor individuals, or to carry out any project that has the effect of tracking or monitoring individuals, should consider carrying out a PIA as early as possible at the design stage to ensure that any personal data privacy impacts are carefully and properly assessed. A PIA is essentially a "minimisation exercise" that identifies and reduces personal data privacy risks to individuals.

Even if the data collected through physical tracking or monitoring is not intended to be used for identifying an individual, or the data collected cannot be so used, there may be instances where the affected individual may perceive otherwise and feel that his right to privacy is being violated. For example, targeted advertising based on anonymous profile information may appear to be intrusive even if there is no personal data involved. It is therefore recommended that a PIA be carried out with potential user perceptions in mind.

(i) Minimisation of the Extent and Sensitivity of Data

Key step - Consider the necessity of each type of data to be collected in a tracking or monitoring arrangement

Define and examine each type of data to be collected. Then assess whether the data can be regarded as personal data in totality, and whether the collection can be minimised while achieving the underlying purposes of the tracking or monitoring exercise.

---

9 For more details on PIA, please see the information leaflet *Privacy Impact Assessments (PIA)* issued by the Commissioner, available at www.pcpd.org.hk//english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf

10 See *Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement* issued by the Commissioner, available at www.pcpd.org.hk//english/resources_centre/publications/files/GN_picspps_e.pdf

11 See *Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users* issued by the Commissioner, available at www.pcpd.org.hk//english/resources_centre/publications/files/DAR_e.pdf

12 See *Guidance on the Proper Handling of Data Correction Request by Data Users* issued by the Commissioner, available at www.pcpd.org.hk//english/resources_centre/publications/files/dcr_e.pdf

Examples:

1. If a shopping centre wishes to share information of shoppers' movements in and out of specific shops with those shops in the centre, it should consider excluding the sharing of the smartphone unique identifiers, location data of shoppers outside the specific shops, and precise time-stamps, as these are not necessary for the purpose and could potentially lead to identification and profiling of shoppers by the shops without knowledge of the shoppers.
2. A work-related tracking smartphone app used by employees should be automatically disabled after work.
3. A worksite-related safety system that tracks the locations of workers against hazardous locations or equipment, or ascertains whether workers have put on the necessary safety equipment, may serve its purpose by simply alerting a worker who goes near a hazardous location or does not have the necessary safety equipment on. It may not have a need to identify or record the whereabouts of each worker in non-hazardous areas.
4. It may not be necessary for a motion-sensing safety and location system, which detects whether a member in an elderly home may have fallen or wondered off premises, to record past movements of each member.

(ii) Minimisation of "Surprises" (to the Individuals)

Key step - Assess the real and potential "surprises" to individuals, and make them known to the individuals with an option to opt out

Be transparent about the tracking or monitoring arrangements and allow individuals to decide whether to participate so as to minimise surprises to individuals, especially when the purposes of the tracking or monitoring are not obvious.

Examples:

1. If the tracking of shoppers' movements in a shopping centre is based on the wireless unique identifiers of their smartphones (i.e. the unique Wi-Fi MAC addresses[13] of the smartphones), the shoppers should be made aware and given the opportunity to opt out of the tracking arrangement when they enter into the shopping centre.
2. If the tracking of shoppers' movements in a shopping centre is based on a smartphone app they have installed, the app should not be packaged or advertised as one that merely provides an enhanced shopping experience without clearly disclosing this privacy-intrusive function of the app.
3. Sharing of tracking information with third parties should be clearly communicated to data subjects. If the purpose of sharing is not directly related to the function of the tracker, an opt-out option should be provided.
4. If an organisation plans to scan individuals for RFID tags in order to track, profile or screen the individuals, it must clearly inform the affected individuals, including whether such tracking, profiling or screening is obligatory or voluntary; and
5. If the registration of a free Wi-Fi service in premises also facilitates the tracking of individuals with their registered names or email addresses, the individuals should be informed explicitly of this arrangement at the time when they register for the Wi-Fi service, so that they may decide if they wish to continue the registration and be tracked. For security purpose, they should also be reminded to "forget" the service (i.e. delete the Wi-Fi connection information from their devices) once they finished using it.

[13] A MAC address is a unique number belonging to a smartphone equipped with Wi-Fi function. It is often "broadcast" by the smartphone to nearby Wi-Fi hotspots, whether or not the smartphone is connected to them.

(iii) Minimisation of Privacy Risks

Key step - Identify real or potential privacy concerns and then develop controls and remedial actions to address them

Common privacy concerns include a real or perceived intrusion to privacy; the risk of identification or re-identification of the individuals concerned; profiling and the unintended adverse effects such as discrimination against the individuals; and data being used for direct marketing activities.

Examples:

1. If data collected through physical tracking can be used to identify individuals, there should be sufficient security measures safeguarding its transmission, storage, access, retention and sharing.
2. If data collected is to be used for direct marketing purpose, the data users must ensure that they have followed Part 6A of the Ordinance, and do not carry out direct marketing activities until all the relevant conditions have been satisfied.
3. If, after the tracking data is duly analysed, the data tracker wishes to use the data in a way that does not match the original purpose of collection, the impact of the use of the data for this new purpose must be assessed and the personal data shall be duly protected in accordance with the provisions under the Ordinance and its DPPs, particularly DPP3 on the use of personal data.

It is important that PIA exercises are duly recorded, in order to show that the data users, such as the trackers and monitors in shopping centres, have acted proactively in protecting personal data, and provide benchmarks for future audits and reviews. When dealing with complaints, the data users may also use the PIA documentation to demonstrate the steps they have taken to protect personal data privacy.

Recommendations for Device Manufacturers

One way for physical tracking or monitoring of individuals is through the tracking of wireless objects carried by individuals or the monitoring of appliances or other equipment at their home. The wireless objects may be smartphones, IoT devices like smart thermostats and smart refrigerators, wearable devices like fitness bands, or RFID-tagged objects like payment cards, clothes, watches, or books, etc. Manufacturers of these devices, equipment and objects are advised to consider the personal data privacy impact of their products, and adopt "Privacy by Design", in order to safeguard the personal data privacy of the users. Following are some examples of how these manufacturers may help create a connected world without compromising personal data privacy or causing concerns to the users.

For Smartphone Manufacturers:

1. Smartphone users should be given and reminded of the option to decide if mobile apps should have access to the location data in their smartphones, and the level of granularity of location data to be read by the apps.
2. As the locations of smartphones may be tracked by third parties by using Wi-Fi, manufacturers of smartphones should devise mechanisms to prevent occurrence of such tracking without the knowledge of the users.

For Manufacturers of IoT Devices:

1. Users of IoT devices should be provided with privacy policies in plain language, so that they can understand and can retrieve information more easily. For example, the privacy policy should be presented in a brief and comprehensive way, and be divided into different sections with headings.
2. Users of IoT devices should be informed in clear terms of the types of personal data to be collected, the purposes of collection, the potential transferees of the personal data and the security measures adopted for protecting the data.
3. Manufacturers of IoT devices should adopt "Privacy by Design" by minimising data collection, incorporating sufficient security safeguards for personal data in storage and in transmission, and adopting the least privacy-intrusive default settings for the devices.

4. If IoT devices are used in conjunction with the supporting apps which have access to the data in the users' smartphones, the manufacturers should offer realistic and meaningful opt-out choice for the access to the data that is not directly relevant to the main purpose of the IoT devices (e.g. location data, contact list, etc.).

5. Users of IoT devices should be given clear instructions on how to delete their personal data stored in the devices and in remote storage (e.g. the backend servers of the manufacturers and its contractors).

6. Users of IoT devices should be provided with contact information (e.g. contact person, telephone number, email address and office address) for pursuing privacy-related matters, and their privacy concerns should be addressed in a timely manner.

For Manufacturers of Wearable Devices:

1. Manufacturers of wearable devices should ensure that data collected by sensors can be read only by using authorised means consciously activated by the owner.

2. Manufacturers should ensure that data collected by the devices (to which the manufacturers have access) will not be used for any purposes about which the users have not been fully informed.

3. Manufacturers should ensure that no unique identification information of the devices can be read by scanners without the users' full knowledge, in order to avoid the wearable device (and therefore the users) being tracked covertly by third parties.

4. Manufacturers should ensure that the devices cannot collect or record data without the users' activation or knowledge.

5. If wearable devices can collect or record information of individuals other than the users, there should be sufficient warning.

For Manufacturers that Would Incorporate RFIDs in Their Products:

1. The use and embedding of RFID tags in products must be made clear to consumers.

2. Consumers should be offered ways to opt out of the inclusion of RFID tags in products, or ways to disable or remove the tags.

3. Manufacturers should avoid storing personal data of product owners in RFID tags. But if one of the purposes of the tag is to store personal data[14], the relevant data users (e.g. a retailer) must comply with the requirements of the Ordinance, including taking all practicable steps to avoid the personal data on the tags from being read by unauthorised parties.

4. With regard to RFID tags that contain information of the goods to which they are attached (such as the common Electronic Product Code), which in turn can, in conjunction with personal data, be used to profile consumers individually. The consumers should be offered the option to have the tags disabled or removed. If the tags must be retained for warranty or authentication purpose, the information in the tags should be shielded from being read by unauthorised parties.

5. Regardless whether RFID tags contain product or personal data, if they cannot be removed or disabled by consumers, they should not contain readable unique identification numbers (such as a serial number) that would allow the tags (and hence the consumers) to be tracked persistently.

6. The choice of the read range of RFID tags should be carefully and properly made with a view to protecting the privacy of individuals.

[14] Such as in personalised contactless payment cards.

PCPD.org.hk

Enquiry Hotline : **(852) 2827 2827**
Fax : **(852) 2877 7026**
Address : **12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong**
Email : **enquiry@pcpd.org.hk**

First published in May 2017