Actxa Pte. Ltd.

[2018] SGPDPC 5

Tan Kiat How, Commissioner — Case No DP-1611-B0320

Data Protection – Consent obligation – Collection, use and disclosure of personal data without consent – Failure to notify individual of purposes for collection and use of personal data – Inadequate privacy policy

Data Protection – Purpose limitation obligation – Use of personal data without notifying individual of purposes for collection and use of personal data – Inadequate privacy policy

Data Protection – Personal data – Collection of personal data through mobile application and multiple connected devices (Internet of Things)

Data Protection – Consent obligation – Reliance on deemed consent

19 April 2018

Background

1 Organisations are increasingly integrating information technology components and computer network connectivity into the products they develop ("**connected devices**"). The embedded technology and connectivity helps turn ordinary products, such as a weighing scale, into a "smart" version of the product with the ability to collect and transfer data wirelessly through the network.

2 These connected devices have the potential to offer a multitude of benefits to improve the lives of users of these devices. A "smart" refrigerator may be able to understand your grocery shopping habits, alert you when you are low on ingredients you commonly use and order these ingredients from an online grocery store and pay for the purchase. A "smart" pacemaker may warn you when you have an impending heart attack, notify the nearest hospital and call for an ambulance.

3 Organisations may use multiple connected devices to collect users' personal data. This would assist organisations in providing an integrated suite of services. As an example, an organisation may collect your body measurements from a "smart" weighing machine and your dietary preferences from your "smart" refrigerator and suggest the amount of daily exercise you should undertake to maintain a healthy body weight through your "smart" watch. Some of these organisations may rely on a single document to notify users of the purposes, and obtain consent, for the collection, use and disclosure of personal data collected through these connected devices and across different platforms. To be clear, there is nothing wrong with this practice. However, such organisations need to ensure that they comply with their notification and consent obligations across all these different connected devices and any other platforms or sources used to collect personal data.

4 In this matter, Actxa Pte. Ltd. ("the **Organisation**"), which sells healthcare and fitness related Internet of Things ("**IoT**") devices, such as "smart" weighing scales, relied on its website's privacy policy to notify its customers of the purposes, and to obtain the customers' consent, for the collection of personal data across all the Organisation's platforms. The Organisation did not have separate privacy policies, or other documentation,

relating to the collection, use and disclosure of personal data collected through the IoT devices it develops and sells.

5 The issue for determination in this case is whether the Organisation, via its website's privacy policy, sufficiently notified its customers of the purposes, and obtained the customers' valid consent, for the collection, use and disclosure of personal data collected through the IoT devices the Organisation develops and sells.

Material Facts and Documents

6 The IoT devices which the Organisation develops and sells include (a) a "smart" weighing machine (the "**Scale**"), marketed under the brand "Sense Smart Scale", that uses bioelectrical impedance analysis technology to measure bone mass, muscle mass, total body fat and total body water, as well as (b) wearable fitness trackers (collectively, the "**Fitness Trackers**"), marketed under the brands "Actxa Swift" and "Actxa Swift+", that use built-in accelerometers to wirelessly detect movements of the user to track the user's activity levels throughout the day.

7 These IoT devices collect data via sensors fitted to these devices. A user can download and install an app (the "**Actxa App**") onto his mobile device, create his user account, and link the IoT devices to his user account. Thereafter, the user can access the data collected by the IoT devices through the Actxa App to monitor his health data, such as sleep pattern, heart rate and weight trends. The Actxa App will reflect the data collected by the IoT devices; though the data may also be amended by the user. The data is automatically collected by the Organisation's servers through the Actxa App.

Personal Data collected through the Actxa App and the IoT devices

8 When a user downloads the Actxa App and creates an account, the user will be asked to submit the following personal data via the Actxa App: name; email; password (encrypted); gender; date of birth; height; weight; profile picture (optional); and country ("**Personal Data Set A**"). This type of personal data is often referred to as declared data.

9 The Scale collects the following personal data: weight; height; Body Mass Index ("**BMI**"); total body water; total body fat; bone mass; and muscle mass ("**Personal Data Set B**"). It is possible for the Scale to be used independently of the Actxa App, in which case it will operate as a simple and unconnected weighing scale.

10 The Fitness Trackers collect the following personal data: steps and goal; calories and goal; distance and goal; active minutes and goal; sleep duration and goal; start of sleep (date and time); end of sleep (date and time); sleep duration; and raw sleep data ("**Personal Data Set C**").

11 Personal Data Sets B and C are typically referred to as observable data as these are collected through sensors either in the Scale or Fitness Trackers. The volume of observable data that is collected through regular usage of the Scale or Fitness Trackers will be much higher than declared data in Personal Data Set A. For convenience the defined terms "Personal Data Set A", "Personal Data Set B" and "Personal Data Set C" will be collectively referred to as "**Personal Data**" in this decision.

12 At the material time, a total of 2,609 customers had downloaded and used the Actxa App, out of which 40 customers were users of the Scale and 2,569 customers were users of the Fitness Trackers.

The Complaint

13 A complaint was made to the Personal Data Protection Commission ("**Commission**") on 7 November 2016 by an individual (the "**Complainant**") alleging that the Organisation failed to notify him of, and obtain his consent for, its collection of his personal data.

14 The Complainant's spouse had bought a Scale from the Organisation's website (the "**Website**") on or around 2 November 2016. The Complainant downloaded the Actxa App, created an account and profile, and started using the Scale around the same time.

15 On 5 November 2016, the Complainant sent an email to the Organisation requesting a refund for the Scale, alleging that the Actxa App transferred the Complainant's personal data to the Organisation's server without the Complainant's knowledge or consent.

16 In response to the Complainant's request, the Organisation deleted the Complainant's account, removed all his personal data from its server, and provided the Complainant with a full refund for the Scale.

The Organisation's Privacy Policy

17 At the time when the complaint was made, the Organisation had a privacy policy that was effective from September 2015 ("**Privacy Policy**"). All users of the Actxa App ("**Actxa App users**") were required to agree to this Privacy Policy before they were allowed to use the Actxa App. The Organisation confirmed that all Actxa App users, regardless of which IoT device they were using, were required to agree to the same Privacy Policy. Notably, the Privacy Policy did not contain any references to the collection, use

and disclosure of personal data through the Actxa App, Scale or other IoT devices, and instead only referenced the Actxa Website.

18 However, after the complaint was made, the Organisation issued a revised privacy policy which took effect from 13 December 2016 ("**Revised Privacy Policy**"), and included specific references to the Actxa App and details on the types of personal data that it collected, used and disclosed. According to the Organisation, all Actxa App users have been notified of the Revised Privacy Policy via email.

Commissioner's Findings and Basis for Determination

19 The issues to be determined in this case are:

(a) whether the Organisation failed to obtain the consent of the Complainant and other Actxa App users before collecting and/or using their personal data in breach of section 13 of the Personal Data Protection Act 2012 ("**PDPA**") ("**Consent Obligation**"); and

(b) whether the Organisation failed to collect and use personal data only for purposes that a reasonable person would consider appropriate in the circumstances and for which the impacted individual has been informed ("**Purpose Limitation Obligation**").

Whether the Organisation is in breach of section 13 of the PDPA

20 Section 13 of the PDPA prohibits organisations from collecting, using or disclosing personal data about an individual unless:

(a) the individual gives, or is deemed to have given, consent under the PDPA to such collection, use or disclosure; or

(b) the collection, use or disclosure of the personal data without the individual's consent is required or authorised under the PDPA or any written law.

21 In the present case, the Commissioner is of the view that the Organisation did not obtain valid consent from the Complainant and other Actxa App users to collect Personal Data Sets B and C[1] (collectively referred to as the "**Observed Personal Data**") and store the said personal data on the Organisation's servers. The Organisation represented to the Commissioner that it collected the Personal Data of the Complainant and other individuals so that the Actxa App would be able to "*display, store and retrieve the data and present historical data for the user's consumption*".

22 The Organisation relies on its Privacy Policy to obtain consent for, and notify the Actxa App users of, the collection, use and disclosure of Personal Data. However, the Privacy Policy only made reference to the Website and did not expressly address the collection, use and disclosure of personal data via the Scale and other IoT Devices through the Actxa App. The first few sentences of the Privacy Policy reads as follows:

> "This Privacy Policy discloses the privacy practices for the Actxa website (collectively, the "Website" located at www.actxa.com). Actxa, the provider of the Website (referred to as "use" or "we"), is committed to protecting your privacy online in compliance with Personal Data Protection Ordinance (PDPO) ("PDPO"). Please read the following to learn what information we collect from you (the "User" or the "End User") and how we use that information…
>
> …

1 As will be discussed later at paragraphs [30] to [34], the Actxa App users are deemed to have provided consent for the collection and use of Personal Data Set A by virtue of section 15 of the PDPA.

> "**Information Gathering**
>
> Actxa only collects two types of information about our Website Users: Personally Identifiable Information and Non-Personally Identifiable Information.
>
> Personally Identifiable Information. Personally Identifiable Information is information that pertains to a specific End Use. The information we collect includes but is not limited to your name, email address, phone number to complete registration. We use this information to provide services and customer support to you."
>
> [Emphasis added.]

23 There is no mention of the Actxa App throughout the entire Privacy Policy nor any mention of how the Personal Data of Actxa App users may be collected by the Organisation from the Actxa App. The complete absence of any reference to the Actxa App in the Privacy Policy shows that the Privacy Policy was only intended to govern the data collection activities undertaken through the Actxa Website, and not the Actxa App nor the IoT Devices. The opening statement of the Privacy Policy, makes express reference to the Actxa Website (and even provides the URL link). In addition, the subsequent paragraph in the "Information Gathering" portion of the Privacy Policy refers to information collected from "Website Users" without any reference to users of the Actxa App, Scale and other IoT Devices. From the above, it is clear from the wording that the Privacy Policy was tailored to the Actxa Website, and the Organisation made no effort to adapt the Privacy Policy to include the personal data protection activities carried out through the Actxa App, Scale and other IoT Devices.

24 The Organisation alleged that since the Privacy Policy would be shown to the Actxa App users prior to their use of the Actxa App, the Actxa App users would have known that the Privacy Policy was applicable to the Actxa App and IoT devices, and not just the Website. However, in the Commissioner's view,

this is not an acceptable practice. Displaying a Privacy Policy that has no relevance to the Actxa App cannot amount to proper notification for the Actxa App users, and consent, if any, that is obtained in this manner cannot be valid. It may well be that consent obtained through pretence or obfuscation could amount to a deceptive or misleading practice under section 14(2)(b) of the PDPA. To be clear, there is nothing to suggest that in this case, the Organisation was any more culpable than mere omission. Pertinently, it is not a reasonable nor acceptable practice to expect individuals who were shown the Privacy Policy to figure out how the Organisation intends for the terms which are tailored to collection of data from the Actxa Website to be adapted for the collection, use or disclosure of personal data via the Actxa App, Scale and other IoT Devices.

25 Compared to declared personal data in Personal Data Set A, the volume, variety and velocity of generation (and collection) of the Observed Personal Data is much higher. The feature set of the Actxa App is non-trivial and likely to become more sophisticated with successive new releases. The use of the Observed Personal Data can also be expected to change in tandem. Accordingly, the purposes for which such personal data will be used should be properly notified to the Actxa App users, in order to obtain their consent. In the circumstances, the Organisation failed to obtain consent from the Actxa App users for, and notify them of, the collection and use of the Observed Personal Data before collection and, thus, the Organisation is in breach of section 13 of the PDPA.

26 Other data protection authorities take similar positions in respect of providing clear notification to users to obtain adequate consent. In Canada, the Office of the Privacy Commissioner of Canada ("**OPC**"), in a case relating to

targeted advertising, emphasised the importance of providing clear notification for adequate consent by stating the following:[2]

> "Organizations must make a reasonable effort to ensure that the individual is advised of the purposes for which their personal information will be used. To make the individual's consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed".

27 The case above concerned a unique device identifier ("**UDID**") that was used by Apple Canada Inc. ("**Apple**"), and disclosed to third party app developers via Apple's iOS operating system, for the purpose of delivering targeted advertising to iOS device users. The OPC considered the UDID to be sensitive personal information as it could be used to create a detailed user profile. Although Apple offered easily accessible opt-out options for the use of the UDID with regard to the delivery of targeted advertising, the OPC found Apple's privacy policy to be insufficient as a form of notification as it contained statements which were too broad and generalised. As a result, the OPC recommended Apple to, amongst other things, amend its privacy policy to inform its users in a manner that is "*clear, apparent and understandable*" how it uses UDIDs to deliver advertising and interest-based ads.[3]

28 In another case, the OPC issued a report of its findings after an investigation into the complaints filed by the Canadian Internet Policy and Public Interest Clinic against Facebook Inc. ("**Facebook**"). The OPC found,

---

2 PIPEDA Report of Findings # 2013-017: *Apple called upon to provide greater clarity on its use and disclosure of unique device identifiers for targeted advertising* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/pipeda-2013-017/> at fifth bullet point in the "Lessons Learned" section at p 2.

3 *Ibid*. at [48].

(*cont'd on next page*)

inter alia, that Facebook had not been clear or specific enough in its notification to its users concerning the collection of a user's date of birth ("**DOB**") such that the user had the necessary information to make an informed choice about consent.[4] As such, the OPC required Facebook to amend its privacy policy so as to better explain the purpose for which a user's DOB is collected and used. Facebook was also required to indicate in its pop-up notification that it collected a user's DOB for the purposes of targeted advertising.[5]

29 In the present case, the Commissioner notices that the first line of the Organisation's Privacy Policy makes explicit reference to the "Personal Data Protection Ordinance (PDPO)", which presumably refers to the main data protection legislation in Hong Kong, instead of the PDPA, which is the main data protection legislation in Singapore. This suggests that the Organisation may not have had Singapore data protection law in mind when it was crafting its Privacy Policy. The Commissioner understands that it is common for organisations to adopt a consistent approach across all the jurisdictions in which they have operations and/or presence through privacy policies which apply across jurisdictions. Organisations are reminded that if they choose to adopt such an approach, they should ensure that such privacy policies are compliant with Singapore law.

---

4 PIPEDA Report of Findings #2009-008: *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act by Elizabeth Denham Assistant Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-008/> at [51].

5 *Ibid*. at [56].

Is the Complainant deemed to have consented to the collection and use of his personal data?

30 In certain case, an individual may be deemed to have consented to the collection, use and disclosure of his personal data even if he has not actually given consent. Section 15(1) of the PDPA provides that an individual is deemed to consent to the collection, use or disclosure of his personal data for a purpose if:

> (a) the individual voluntarily provides the personal data to the organisation for that purpose, and
>
> (b) it is reasonable that the individual would do so.

31 In the Commissioner's view, the Complainant could be deemed to have consented to the Organisation collecting, using and disclosing his Personal Data Set A as he had voluntarily entered Personal Data Set A into the Actxa App during the account and profile creation phase and it was reasonable that he would provide the Organisation this personal data for purpose of setting up and managing his account on the Actxa App.

32 However, in respect of Personal Data Set B, whilst the Complainant had used the Scale and Actxa App voluntarily, he was unaware that his Personal Data Set B was being collected by the Organisation and stored on the Organisation's servers. While the state of knowledge of the individual cannot be the limiter on the scope of deemed consent, neither can the purposes for which consent is deemed be so vague or broad that deemed consent ceases to be meaningful. Deemed consent is intended to be relied on in situations where the purpose for collection, use or disclosure of personal data is so clear that the reasonable bystander would have assumed that the individual would ordinarily have provided his consent. Deemed consent is helpful where the transaction is

not complex or where it is closely entwined with the performance of an underlying contract. For example, supplying one's payment details and shipping details during an e-commerce transaction, or when engaging a courier to make a delivery. Where the purpose for which consent is provided is clear, the scope of the consent that is deemed can also be reasonably demarcated.

33 In this case, the Commissioner considered the possibility that the features of the Scale and the Actxa App collectively establishes the purposes and that consent is deemed for this set of purposes. However, this approach may possibly supplement an inadequate Privacy Policy but cannot be used to construct an absent one for a set of complex functionalities and customer relationship like the present. The feature set of the Actxa App can be expected to change over time and Observed Personal Data will be used in different ways. Further, the relationship between Organisation and customer may last indefinitely, depending on the period of time the customer continues to use the Scale and the Actxa App. These features militate against reliance on deemed consent. In this case, as explained above, there is no Privacy Policy for the Scale or the Actxa App and, for reasons just provided, deemed consent cannot be relied on to create one by operation of law.

34 Similarly, other Actxa App users may be deemed to have consented to the Organisation's collection, use and disclosure of their Personal Data Set A, but not their Observed Personal Data (depending on which IoT device they use) for the same reasons articulated above. In the circumstances, the Organisation is found to be in breach of the section 13 obligation for failing to obtain consent:

(a) from the Complainant for the collection, use and disclosure of his Personal Data Set B; and

(b) from Actxa App users for the collection and use of Observed Personal Data depending on which IoT device they use.

35 With more developers creating mobile apps, it is unsurprising that guidance has been issued to guide app developers. In the United Kingdom, the Information Commission's Office ("**ICO**") has published guidance for mobile app developers, which states that "*transparency about purpose is crucial*"[6] and sets out important points that developers should take into consideration when drafting notification to users in a mobile environment. In particular, the guidance also highlights how organisations can give their users more control over their privacy such as providing notification when their data is about to be uploaded to the Internet:[7]

> "If your app processes personal data in an unexpected way or is of a more sensitive nature you might need to consider the use of additional 'just-in-time' notifications or other alert systems to inform the user what's happening. For example, if geo-location services are running in the background or you are uploading data to the internet, consider using clear and recognisable icons to indicate that this is occurring and where necessary the option to stop (eg to cancel an upload)."
>
> [Emphasis added.]

36 The use of just-in-time notifications in order to obtain consent dynamically and in bite-sized portions (as opposed to a lengthy privacy policy) is one of the ways that the Commission has recommended for adoption in its Guide to Data Sharing.[8]

---

6 UK, ICO, Privacy in mobile apps: Guidance for app developers (December 2013) <https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf> at p. 10.

7 *Ibid*. at p. 17.

8 PDPC, Guide to Data Sharing (27 July 2017) <https://www.pdpc.gov.sg/Legislation-and-Guidelines/Guidelines/Other-Guides> at [3.6] - [3.7].

(*cont'd on next page*)

37 Similarly, the Office of the Privacy Commissioner for Personal Data of Hong Kong ("**PCPD**") has issued an information leaflet in which it highlights the privacy implications that mobile app developers should consider, including the designing of a privacy policy statement:[9]

> "***Privacy Policy Statement (PPS)***
>
> Apps Developers should prepare a PPS to outline their policies and practices in relation to personal data. Technical terms and elusive language should be avoided in the PPS. It should be easily readable and easily understandable, and in appropriate length. Its location on the mobile apps should be prominent. Its availability also on the businesses' normal websites is recommended.
>
> ***Giving examples in PPS***
>
> When describing the purposes for which the information is to be used in the PPS, Apps Developers should consider giving real-case examples (as opposed to generic statements) specific to the mobile apps to assist mobile device users in understanding why such information needs to be collected, accessed or shared.
>
> ***Relevance and Accuracy***
>
> Apps Developers should ensure that their PPS are accurate and specific for individual mobile apps. If the description is vague or unclear, the Apps Developers may be perceived as hiding the real purpose of data collection and access. Similarly, if the PPS is copied or extracted from a standard template or another mobile app, Apps Developers have to review the contents to ensure their relevance and accuracy."
>
> [Emphasis added.]

38 The Commissioner agrees with many of the general positions taken by the PCPD. In this regard, a privacy policy for a mobile app should, amongst other things:

---

9 HK, PCPD, *Personal data privacy protection: what mobile app developers and their clients should know* (November 2012) <https://www.pcpd.org.hk/english/publications/files/apps_developers_e.pdf> at p. 5.

(a) aim to enhance a user's understanding as to why certain personal data needs to be collected, accessed or shared;

(b) avoid technical terms and elusive language, be easily readable and understandable, and be of an appropriate length;

(c) be prominently located on the app;

(d) consider using icons and/or just-in-time notifications to obtain specific consent dynamically; and

(e) be reviewed carefully to ensure relevance and accuracy if a standard template is used.

Whether the Organisation is in breach of section 18 of the PDPA

39 Section 18 of the PDPA allows organisations to collect, use and disclose personal data only for purposes which a reasonable person would consider appropriate in the circumstances and for which the impacted individual has been notified.

40 Given that the Commissioner has found above, at paragraph 25, that the Organisation failed to notify Actxa App users of the collection, use and disclosure of the Observed Personal Data before collecting the said personal data, the Organisation is in breach of section 18 of the PDPA for the same reasons set out above to substantiate a breach of the Organisation's section 13 obligations.

Enforcement Action by the Commissioner

41 Given that the Organisation has been found to be in breach of sections 13 and 18 of the PDPA, the Commissioner is empowered under section 29 of

the PDPA to give the Organisation such directions as it deems fit to ensure the Organisation's compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding S$1 million as the Commissioner thinks fit.

42 In assessing the breach and determining the directions to be imposed to the Organisation in this case, the Commissioner took into account the following mitigating factors:

(a) the Organisation had accepted the complaint in good faith and taken prompt steps to broaden the coverage of its Privacy Policy. The Revised Privacy Policy now makes explicit mention of the "Actxa App" and the types of personal data that the Actxa App would collect from the Actxa App users. Hence, the consent obtained and notification provided by the Organisation is now directly relevant to the Actxa App;

(b) the Organisation had cooperated fully with investigations and was forthcoming in providing information to the Commission;

(c) there were no other complaints received from other Actxa App users, besides the Complainant; and

(d) the Organisation had engaged the Complainant in a meaningful manner, and voluntarily offered a refund which the Complainant accepted.

43 The Commissioner also took into account the following aggravating factors:

(a) the breach involved sensitive health-related personal data such as an individual's weight, height, and BMI; and

(b) the personal data of a total of 2,609 Actxa App users were potentially compromised or put at risk.

44 The Commissioner has carefully considered the relevant factors of this case and hereby directs the Organisation to pay a financial penalty of S$6,000 within 30 days from the date of the Commissioner's direction, failing which interest shall be payable on the outstanding amount of such financial penalty.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION