PCPD HK 20 PCPD.org.hk est.1996
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

2016 Study Report on

The Privacy Policy Transparency of Fitness Bands

January 2017

Table of Contents

Introduction

The Privacy Commissioner for Personal Data, Hong Kong (the "**PCPD**") is a member of the Global Privacy Enforcement Network (the "**GPEN**")[1], and participates in the Sweep exercise coordinated by the GPEN for the fourth consecutive year.

2. This year, 25 privacy enforcement authorities ("**PEAs**") from around the world, including the PCPD, participated in the Sweep to examine how well manufacturers and providers of Internet of Things ("**IoT**") devices communicated privacy-related matters to users.

3. The theme of the 2016 Sweep is "The Internet of Things – with a focus on Accountability". IoT is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment[2]. Typical examples of IoT devices include smart TVs[3], smart meters[4] and wearables[5]. IoT devices have significantly improved people's lives and created business opportunities. However, IoT devices have also triggered privacy concerns because they have the ability to collect, analyse and generate data about their users, and share the data with third parties without the users' knowledge.

4. Participating PEAs were allowed to choose the type of IoT devices they wish to examine, taking into consideration local conditions and interests, etc. In view of product availability and increasing popularity, the PCPD decided to select locally manufactured fitness bands for the Sweep. The PCPD examined five

[1] The GPEN was established in 2010 to foster international cooperation on enforcement of privacy laws. As of 31 July 2016, GPEN comprises 63 privacy enforcement authorities from 47 countries around the world.

[2] Source: Gartner IT glossary at www.gartner.com/it-glossary/internet-of-things/

[3] Smart TVs are TVs that may be connected to the Internet and have browsing function. Apart from allowing viewers to browse the Internet like a computer, smart TV may be used to play TV/movies available in the Internet, install and run apps (informational, social media etc.) specifically written for them.

[4] Smart meters are utility meters that can be read remotely by wired or wireless technology, and may provide granular reading (e.g. minute-by-minute) and recording of utility consumption.

[5] Wearables are devices that may be worn by individual to monitor their physical activities or physiological conditions (e.g. fitness bands, blood pressure/heart beat trackers) or as an extension of their smartphones (e.g. smart watches, Google glass-type of devices).

locally manufactured fitness bands and the supporting mobile applications ("**apps**"). In addition, a popular fitness band manufactured by a well-known US company, Fitbit, and its mobile app were also examined for comparison purpose.

5. The PCPD found that fitness bands and their mobile apps might collect sensitive personal data and pose privacy risks to their users. However, manufacturers of fitness bands were found not to have provided sufficient privacy communications to allow users to assess the privacy impact and to take steps to protect their personal data.

6. As a follow-up and lesson learnt from the exercise, recommendations were developed to advise manufacturers of fitness bands on how to enhance privacy communications and improve the handling of personal data. Pieces of advice were also provided to the users of fitness bands on how to protect their own personal data when using.

Operation of Fitness Bands

7. A fitness band is an electronic sensor worn on the wrist of the user for tracking the daily activities, e.g., distance walked, calories burnt, duration and quality of sleep, and some of them have the ability to read the physiological signals, e.g., heart rate, and even collect the physical location of their users through GPS. Generally, fitness bands do not operate on their own but in conjunction with the supporting mobile apps. A fitness band may collect personal data of its user when the data is:

7.1. submitted by the user during registration (e.g., name, age, weight, height);

7.2. collected by the fitness band during use (e.g., distance walked, duration of sleep); and

7.3. collected by the supporting mobile app through the latter's direct access to the data in user's smartphone (e.g., physical location of the user).

Objectives of the Sweep on Fitness Bands

8. The PCPD notes that fitness bands and similar IoT devices are increasingly popular in Hong Kong. More businesses, including start-ups, may enter the market in future[6]. By participating in the Sweep, the PCPD aims to:

8.1. explore the privacy challenges and implications brought by fitness bands and IoT devices generally;

8.2. raise the privacy awareness of the manufacturers of fitness bands and IoT devices, and promote compliance with the Personal Data (Privacy) Ordinance (the "**Ordinance**");

8.3. educate users of fitness bands and IoT devices on how to protect their personal data;

8.4. identify areas of concern for future privacy education, promotion and enforcement; and

8.5. share the results and findings of the PCPD with other PEAs to foster cross-border privacy enforcement and knowledge-sharing.

Selection of Fitness Bands

9. Each PEA participating in the Sweep was free to choose the type(s) and number of IoT devices to be studied, based on its own strategic focus and domestic conditions. The objective of the global Sweep exercise was to assess how the manufacturers of the IoT devices communicated privacy-related matters to their users. Through enquiries with the manufacturers of fitness bands, the PCPD further explored the security measures adopted by them for protecting users' personal data.

10. The PCPD decided to examine fitness bands because of their increasing popularity in Hong Kong. The PCPD further limited the scope to locally manufactured fitness bands such that any follow-up actions or recommendations derived from the Sweep would be applicable to them.

[6] The US research company Gartner, Inc. forecasted that in 2016, 34.97 million fitness bands (known as "wristbands" in Gartner's report) will be sold worldwide, which would be an increase of 16 percent from 2015. Gartner also forecasted that the growth in fitness band sale would accelerate in 2017, with 44.1 million units of sale worldwide expected, which represents an increase of 26 percent from 2016. For details, see www.gartner.com/newsroom/id/3198018

11. Generally, fitness bands can work with both Android and iOS smartphones, and hence their corresponding fitness band apps would normally be available in both the Google Play and the AppStore.

12. The PCPD found and selected the locally manufactured fitness bands using the following strategies:

12.1. given that fitness bands needed to work with a mobile app, the category of "fitness and health" in Google Play app store was chosen as the starting point, and more than 1,000 mobile apps were checked to see whether they were associated with fitness bands, and if so, whether they were manufactured by Hong Kong companies and were available in the Hong Kong market;

12.2. the following websites were also searched to identify fitness bands, or manufacturers or mobile apps that would be associated with fitness bands:

12.2.1. a Hong Kong price-comparison site for electronics "gadgets";

12.2.2. list of websites and participants of the Hong Kong Electronic Fair 2016 (Spring Edition) which was organised by the Hong Kong Trade and Development Council;

12.2.3. the Hong Kong ICT Awards on mobile apps as organised by the Wireless Technology Industry Association and steered by the Office of the Government Chief Information Officer; and

12.2.4. Internet search of potential manufacturers and fitness bands.

13. Eventually, the PCPD identified and acquired five locally manufactured fitness bands for examination.

14. For the purpose of benchmarking, the PCPD selected one fitness band manufactured by a popular US fitness band company for comparison.

15. The list of selected fitness bands and mobile apps is at **Appendix A**.

Examination of Selected Fitness Bands and Mobile Apps

16. The PCPD conducted the Sweep between 11 April and 16 June 2016 as follows:

16.1. purchased the selected fitness bands (five local and one US) and familiarised with their functions and features with both Android and iOS smartphones;

16.2. read through the privacy statements and user guides of the fitness bands contained in their product packages, mobile apps and/or websites of the manufacturers with a view to answering a set of predefined questions (see paragraph 17); and

16.3. made enquiries with the respective manufacturers with a set of predefined questions (see paragraph 20).

17. The purpose of the Sweep was to assess how well privacy-related matters were communicated to users, and the following predefined questions set by the GPEN were used by all participating PEAs:

17.1. Did the fitness band have a privacy policy? If so, was the privacy policy specific to the fitness band or generic?

17.2. Did the privacy policy (if available) indicate what personal data would be collected by the fitness band and mobile app, and for what purposes?

17.3. Did the privacy policy (if available) identify the potential transferees of the users' personal data?

17.4. Were users informed about the storage location of the personal data collected, the methods of storage and transmission of the data, and the security measures taken to protect the data?

17.5. Were users asked or reminded to change the default privacy settings of the fitness band and mobile app?

17.6. Were users told how to delete their personal data from the fitness band and mobile app?

17.7. Were users provided with the contact details of the fitness band manufacturer for making enquiries about privacy-related matters?

17.8. Did the fitness band manufacturer provide timely and detailed response to the PCPD's enquiries?

18. The original questionnaire predefined by the GPEN for this Sweep purpose is at **Appendix B**.

19. As some of these indicators required subjective judgments of the examining officers concerned, each fitness band was examined by two officers to ensure the objectiveness of the assessment. Any variance in the results produced by the two examining officers were discussed and reconciled. This arrangement also helped replicate the typical experience of the general users.

20. In addition to examining the fitness band, apps and website, written and verbal enquiries were made by the PCPD with the device manufacturers. The questions asked include the following:

20.1. What personal data of the users is collected by the fitness bands and the mobile apps?

20.2. Is the users' personal data stored in the fitness bands, the connected mobile phones, the manufacturers' servers or anywhere else?

20.3. Is the users' personal data stored and transmitted between devices in encrypted form?

20.4. Will the manufacturers share or transfer the users' personal data to other parties?

20.5. How can the users delete, extract and export their personal data from the fitness bands, the mobile apps and the manufacturers' servers?

20.6. Have the manufacturers conducted any risk assessment to identify potential privacy risks associated with the fitness bands?

21. Among the six manufacturers enquired by the PCPD, four local manufacturers provided partial responses.

22. The examination results of the five locally manufactured fitness bands were compared to those of the US fitness band. Not all answers produced significant results, but where they did, they were elaborated below.

Global Sweep

23. Globally 25 PEAs examined 314 IoT devices. The distribution of types of devices is as follows:

Type of devices	**Number of PEAs that examined the devices(a PEA may examine more than one type of device)**
Connected medical/health devices (e.g. blood pressure monitors, sleep monitors)	11
Fitness wearables	10
Household aids	6
Smart TVs	2
Smart meters	2
Usage Based Insurance devices	1
Connected toys	1
Connected cars	1

24. Based on the predefined questions set by the GPEN, five indicators were reported by participating PEAs:

24.1. number of devices that failed to explain to users on how their personal data is collected, used and disclosed;

24.2. number of devices that failed to explain to users on how the data collected by the device is stored and protected against data leakage;

24.3. number of manufacturers that failed to provide users with easily identifiable contact details for privacy-related matters;

24.4. number of devices which did not explain how a user can erase their personal data from the device; and

24.5. number of manufacturers that failed to provide a timely, adequate and clear response upon enquiry.

Results and Findings

25. It should be noted that the firmware of the fitness bands, as well as their mobile apps and the manufacturers' websites may be constantly evolving and going through changes and updates. Hence, the results and findings in this study report should only be taken as representing the positions of the selected fitness bands, the mobile apps and the websites at the particular time of the Sweep between April and June 2016.

26. Moreover, the Sweep was a coordinated research exercise and was not a compliance check or formal investigation. Therefore it is not appropriate for the PCPD to disclose the specific results and findings for each individual fitness band. The results and findings set out below are therefore aggregated in nature.

27. In each category of items below, the findings of the local fitness bands would be presented first, followed by how the US fitness band had behaved. In addition and where appropriate, the findings of the local fitness bands would also be compared with the five global indicators reported from the other 24 PEAs. However, readers need to be reminded that not all PEAs have examined fitness bands, so the comparison is between Hong Kong fitness bands and global IoT devices examined.

Notable results and findings of the Sweep

<u>Privacy policy</u>

28. Only two out of five local fitness band manufacturers (40%) provided privacy policies to users in their websites or the supporting mobile apps, and only one (20%) such privacy policy was specific to the fitness band. The other privacy

policy was related only to the collection of information by the manufacturer's website.

29. Only the manufacturer with specific privacy policy for fitness bands indicated to users the types of personal data to be collected (e.g., email address, date of birth, height, weight), and the collection purposes. The other four local manufacturers did not provide any information on this aspect.

30. In comparison, the US manufacturer provided users with privacy policy on the supporting mobile app which was specific to fitness bands. In the privacy policy, the US manufacturer explained to users the types of personal data to be collected and the collection purposes.

31. Globally, the majority of IoT devices examined did not provide users with privacy policies specific to the devices. They tended to provide examples of data that might be collected rather than listing every data to be collected in their privacy policies.

32. Summary of findings in relation to privacy policy:

	Five local fitness bands	**US fitness band**	**Global IoT devices (314 devices/companies)**
Devices with privacy policies provided	2 (40%)	Yes	41% (Devices that adequately explained to users on how their personal data is collected, used and disclosed)
Information provided in the privacy policies on the types of information to be collected	1 (20%)	Yes	

33. The lack of transparency might not allow a user to ascertain the full extent of data collection. A user might be taken by surprise when some data items which he did not expect to be collected were later found to have been collected. In

addition, a user would not be able to make an informed choice if he wanted to purchase a privacy-friendly fitness band.

Collection of personal data during registration on the mobile apps and use

34. All local fitness bands collected, during the registration on the mobile apps, certain personal data of a user, such as his name, telephone number, email address, date of birth/age, weight and height, either on a mandatory or a voluntary basis. However, the type and amount of personal data collected by each fitness band varied. For example, some fitness bands sought to collect a user's telephone number and email address, while others did not. This might indicate that telephone number and email address are not necessary for the proper functioning of the fitness band, and hence should not be collected or should be made optional.

35. All the six fitness bands (including the US fitness band) collected a user's health/fitness information during use. Data collected might include calories intake, calories burnt, heart rate, time of sleep, sleep movements and walking distance, etc. Collecting such data is probably necessary because it is directly related to the function of the fitness bands, i.e., monitoring the activities and fitness of the user.

36. The supporting mobile apps also had access to the data and functions of a user's smartphone, such as reading location data, pictures, text messages and social media accounts, controlling the cameras of the smartphone, etc. The extent of access by the same app may vary with its Android and iOS versions.

37. By the design of iOS operating system, opt-in consent by a user was required before a mobile app was able to access users' data. On the other hand, for a smartphone running Android operating system, a mobile app can get access to the data by simply notifying the user before installation of the app. However, for smartphones running Android version 6.0 or above, users may remove certain access rights of the apps after installation.

38. It was noted that the apps of some fitness bands running Android system obtained certain access rights to users' smartphones by default, but the apps of the same fitness bands running iOS system did not request for such access. For example, the app of one local fitness band running Android system obtained access to location data and had control of the smartphone's camera by default.

However, these access rights were not requested by the same app running iOS system when the PCPD's officers used the app and the fitness band. This indicated that some fitness band manufacturers might have obtained too much access rights to the users' smartphones by default which were unnecessary for the proper functioning of the fitness bands and the apps.

39. Globally, the IoT devices examined also collected different types of personal data from users, including name, email address, date of birth/age, address, phone number, weight, height, medical details, location data, pictures and unique device identifiers, either on a mandatory or a voluntary basis. Similar to the findings of the local fitness bands, concerns were raised as to whether certain types of data such as date of birth and location data were necessary for the proper functioning of the devices.

40. Summary of findings in relation to personal data collection:

	Five local fitness bands	**US fitness band**	**Global IoT devices (314 devices/companies)**
Requesting users to provide personal data during registration	5 (100%)	Yes	Information collected: • Name – 84% • Email – 83% • Date of birth/age – 64% • Location – 68% • Phone number – 55% • Photograph/video/audio file – 41% • Unique device identifier – 61%
Obtaining access to data and/or functions of users' smartphones during use	5 (100%)	Yes	

41. It should be noted that when the data collected during an user's registration and during use was combined, not only the user's identity but also his intimate information, such as the health conditions, the habits and the lifestyle of the user could be extracted by the manufacturer. Manufacturers should minimise the amount of data to be collected and whenever possible collect the least privacy intrusive data (e.g., collect "nickname" instead of full name; collect age/year of birth instead of full date of birth).

42. The PCPD noted that one fitness band minimised the personal data collection during users' registration by asking users to only voluntarily provide the necessary data, such as name, gender, age, weight, height and stride length to enable the proper functioning of the fitness band. There is no other field in the app for users to submit further information, like email address and telephone number. This is a good example of "Privacy by Design[7]", because fitness band users may normally have a tendency to fill up as many fields as appeared in a data collection form. To minimise data collection, the preferred way is to remove the unnecessary data collection fields from a form, rather than to make the fields optional.

Transfer of personal data to third parties

43. Only two local fitness bands (40%) stated in their privacy policies their intention of transferring users' personal data to third parties (such as affiliates, agents and partners) and explained the purposes of such transfer (such as provision of services to users), but stopped short of mentioning the types of data to be transferred. For the remaining three local fitness bands (60%), no information on this aspect was provided.

44. In comparison, the US manufacturer explained to users in its privacy policy that it would transfer personal data to third parties (such as strategic partners and service providers). It also specified under what circumstances the personal data may be transferred (e.g., for order fulfilment, compliance with law and regulation, etc.). However, the US manufacturer also failed to mention the types of personal data to be transferred to third parties.

45. No figure on this aspect was provided in the global Sweep results.

[7] Privacy by Design is an approach to ensure that privacy consideration is built in right from the beginning of any design. This approach ensures privacy is embedded into the design specifications of technologies, business practices and physical infrastructures. Privacy concerns are to be anticipated and assessed before a system is to be implemented. Privacy risks should be prevented before they materialise.

46. Summary of findings in relation to transparency of the intended transfer of personal data:

	Five local fitness bands	**US fitness band**
Disclosure on recipient of transferral:		
- *in the privacy policies*	0 (0%)	Yes
- *upon enquiries by the PCPD*	2 (40%)	No response
Disclosure on the types of information to be transferred to third parties:		
- *in the privacy policies*	0 (0%)	No
- *upon enquiries by the PCPD*	1 (20%)	No response

47. If users are not informed of the types of personal data to be transferred and the classes of potential recipients, they cannot make informed decision on what personal data should/could be disclosed to fitness band manufacturers.

Storage of personal data

48. None of the five local fitness bands (0%) provided sufficient information in their privacy communications to users in respect of where their data would be stored, or whether third parties would be employed to store the data.

49. The PCPD obtained further information about storage of users' personal data by making enquiries with the manufacturers. Two (40%) local manufacturers stated that they employed third parties to store the data in Mainland China and Singapore respectively, and remaining three (60%) local manufacturers either did not respond or did not sufficiently address our questions.

50. In comparison, the US manufacturer stated in its privacy policy that the personal data would be stored in the US, but did not mention whether third parties were engaged to store the data.

51. Globally, the majority of IoT devices examined did not explain to users in their privacy policies on how personal data was stored. Even if data storage was mentioned, the privacy policies rarely explained to users the storage location, period of data retention and in what form of data was stored (e.g., in a cloud).

52. Summary of findings in relation to storage of personal data:

	Five local fitness bands	**US fitness band**	**Global IoT devices (314 devices/companies)**
Disclosure of storage location:			
- *in the privacy policies*	0 (0%)	Yes – in US	32%
- *upon enquiries by the PCPD*	2 (40%)	No response	No figure available
Disclosure of third party storage:			
- *in the privacy policies*	0 (0%)	No – no information on disclosure	32%
- *upon enquiries by the PCPD*	2 (40%)	No response	No figure available

<u>Safeguard of personal data</u>

53. None of the five local fitness bands (0%) provided sufficient information in their privacy communications to users in respect of whether the data would be protected (e.g., by encryption) in storage and transmission. Only one local fitness band (20%) committed to use security safeguards to protect users' personal data in its privacy policy, but details of the security measures were not given.

54. The PCPD obtained further information about safeguard of users' personal data by making enquiries with the manufacturers. Two (40%) local manufacturers responded that they did not apply encryption to data in storage and transmission, of which one (i.e., the one committed to using security safeguards to protect users' personal data in its privacy policy) stated that it used other means to protect the

personal data (e.g., requiring password to login to the app); one (20%) local manufacturer submitted that encryption was adopted for data in storage and transmission between the smartphone and the manufacturer's server; the remaining two (40%) either did not respond or did not sufficiently address our questions.

55. In comparison, the US manufacturer stated in its privacy policy that it used "*a combination of firewall barriers, encryption techniques and authentication procedures*" to protect the personal data of users.

56. Globally, 51% of the IoT devices examined informed users about how their personal information was being safeguarded and what was being done to prevent unauthorised users from accessing the data (e.g., passwords protections or authentication questions). It appeared that the transparency of local fitness bands was below global average in this regard.

57. Summary of findings in relation to safeguard of personal data:

	Five local fitness bands	**US fitness band**	**Global IoT devices (314 devices/companies)**
Commitment on safeguarding collected information:			
- *in the privacy policies*	1[8] (20%)	Yes	51%
- *upon enquiries by the PCPD*	1[9] (20%)	No response	No figure available

[8] This manufacturer reaffirmed in its response to the PCPD's enquiry that security safeguard was used.

[9] This manufacturer did not commit to security safeguard in its privacy policy.

	Five local fitness bands	**US fitness band**	**Global IoT devices (314 devices/companies)**
Encryption deployed to protect information:			
- *in the privacy policies*	0 (0%)	Yes	No figure available
- *upon enquiries by the PCPD*	1 (20%)	No response	No figure available

58. Given the sensitivity of the personal data collected by fitness bands, users normally would expect stronger safeguards to be offered by the manufacturers. Moreover, the legal protection on personal data varies with jurisdictions. Therefore, the lack of transparency on data storage and data security may undermine users' confidence in choosing the devices, which may be exacerbated in a place, like Hong Kong, where the privacy awareness of the public is high.

Privacy impact assessment

59. The PCPD wrote to the fitness band manufacturers to enquire whether any privacy impact assessment was conducted to identify potential privacy risks associated with the fitness bands. Only one (20%) local manufacturer stated that they had conducted the assessment, while another one (20%) stated that it would conduct the assessment in future. The remaining three (60%) either did not respond or did not sufficiently address our question.

60. The US manufacturer did not mention about privacy impact assessment in its privacy policy, nor did it respond to the PCPD's enquiry on the question.

61. No figure on this aspect was provided in the global Sweep results.

62. Summary of findings in relation to privacy impact assessment:

	Five local fitness bands	**US fitness band**
Conducting privacy impact assessment	1 (20%)	No response

63. In the absence of privacy impact assessment, the manufacturers may be unable to identify the privacy risks of their fitness bands systematically. As a result, they may not be able to implement adequate privacy safeguards.

Deletion of personal data

64. None of the five (0%) local manufacturers told users how to erase their personal data collected by the fitness bands and the mobile apps. Only one (20%) local manufacturer provided users with an email address in its privacy policy to which data erasure request could be sent. Another local manufacturer, in response to the PCPD's enquiry, stated that users might contact them for erasure of data in the band, the app, and/or in storage. The remaining local manufacturers either did not provide means for users to erase personal data, or did not respond to the PCPD's questions. Generally, users were not given a convenient way to erase their personal data.

65. In comparison, the US fitness band stated in its online user handbook that all users' personal data stored in the fitness band would be erased if the band was linked to another user account. It also provided an email address in its privacy policy for fitness band users to make requests for data erasure.

66. Globally, only 28% of the IoT devices examined explained to users in their privacy policies how to erase their personal data from the devices/mobile apps. In some cases, data erasure processes were complicated. Similar to the findings of local fitness bands, there was insufficient information provided to users on erasure of personal data.

67. Summary of findings in relation to erasure of personal data:

	Five local fitness bands	**US fitness band**	**Global IoT devices (314 devices/companies)**
Information on how to erase information collected:			
- *in the privacy policies*	1 (20%)	Yes	28%
- *upon enquiries by the PCPD*	1[10] (20%)	No response	No figure available

68. The primary purpose of collecting personal data by fitness bands is to allow users to gain insight into their own fitness condition, instead of the use by the manufacturers. Therefore, the users should have the right to control the retention and erasure of their own personal data. The lack of information on data erasure undermines the users' rights.

Change of default settings

69. None of the five local manufacturers (0%) reminded users to examine and change the default privacy settings of the fitness bands and the mobile apps. For the US manufacturer, it explained in its privacy policy about the types of information in the user accounts to be shared by default with the public and with the users' "friends". It also informed users that they might change the privacy settings in its website anytime.

70. No figure on this aspect was provided in the global Sweep results.

[10] The one responded to PCPD's written enquiry that fitness band users may contact them for personal data deletion is a different one from the fitness band that has provided an email address in its privacy policy for receiving deletion requests.

71. Summary of findings in relation to change of default settings:

	Five local fitness bands	**US fitness band**
Reminder in the privacy policies on changing default settings regarding privacy	0 (0%)	Yes

72. We noted that the mobile apps running Android system might obtain too much access rights to the smartphone data by default (see paragraph 38 above). The apps may also disclose users' personal data to their "friends" or other users beyond their expectations. Therefore, users should examine the privacy settings, and disable the unnecessary/unwanted access rights and information-sharing functions.

Contact details for enquiry about privacy-related matters

73. Only two (40%) local manufacturers provided contact information (i.e., email addresses) to users for enquiring about privacy-related matters.

74. Similarly, the US manufacturer also provided email address to users for enquiring about privacy-related matters.

75. Globally, 62% of the IoT devices provided contact details to users for raising privacy concerns. It appeared that the transparency of local fitness bands was below global average in this regard.

76. Summary of findings in relation to contact information:

	Five local fitness bands	**US fitness band**	**Global IoT devices (314 devices/companies)**
Contact information provided to users in the privacy policies for privacy-related matters	2 (40%)	Yes	62%

77. Without providing contact details to users, users cannot clarify privacy-related matters and exercise their data access and correction rights, which may lead to privacy-related complaints and dissatisfaction about the company and in turn affect its reputation.

Summary on notable results and findings

78. Overall, the US fitness band performed better than the local fitness bands in terms of privacy communications because the manufacturer of the US fitness band:

78.1. provided privacy policy specific to the devices to explain the types of personal data to be collected and the collection purposes;

78.2. explained the circumstances under which personal data might be transferred to third parties;

78.3. explained (though very briefly) the security measures for protecting personal data;

78.4. provided means for users to erase their personal data; and

78.5. stated contact information for users to get in touch for privacy-related enquiries.

79. The local fitness bands' performance appeared to be below the global average for IoT devices in some areas of the privacy communications, such as the communication in relation to safeguard of personal data and the provision of contact details for enquiry about privacy-related matters. However, it should be noted that the comparison between Hong Kong's and the global Sweep results may not be conclusive because Hong Kong's results only represented the performance of fitness bands, while the global results represented the performance of a variety of IoT devices.

Conclusions and Recommendations

80. Fitness bands may collect sensitive personal data of their users and pose privacy risk to users if the data is misused or leaked. Sufficient information should therefore be provided to users to alert them about the privacy risk. Adequate safeguards for the personal data should also be deployed by the manufacturers. However, the Sweep revealed the deficiency in privacy and security communications provided by the local manufacturers.

81. To increase the transparency and safeguards in handling of personal data, the PCPD recommends fitness band manufacturers to:

81.1 provide privacy policy to users by using simple language, and help users locate important information in privacy policy easily (e.g., by dividing privacy policy into different sections and adding headings to each section);

81.2 state clearly 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;

81.3 adopt "Privacy by Design" in minimising data collection; incorporating sufficient security safeguards for personal data in transmission and in storage; and adopting the least privacy intrusive default settings for the fitness bands and the mobile apps;

81.4 offer opt-out choice if the supporting mobile apps would access data in smartphones that is not directly relevant to the main purpose of the fitness band (e.g., location, contact list, etc.);

81.5 provide clear instructions to users for erasing their personal data stored in the fitness band, in the smartphone and in the remote storage (e.g., the backend servers of the manufacturers and sports-related social networks where appropriate); and

81.6 provide contact information (e.g., contact person, telephone number, email address, office address) for users to pursue privacy-related matters, and provide timely responses to users to address their privacy concerns.

82. Users of fitness bands should also play a role in protecting their personal data privacy. The PCPD recommends users to:

82.1. carry out research on personal data privacy impact before purchase of fitness bands, ascertaining the types and extent of personal data to be collected by the manufacturers and the supporting mobile apps, the intended uses of the personal data collected and the safeguards in place;

82.2. use pseudonyms for account registration whenever possible;

82.3. set up dedicated accounts (e.g., dedicated email accounts) for fitness bands, and avoid linking the fitness band accounts with social media accounts whenever possible;

82.4. review the default settings of the fitness bands and the mobile apps, and turn off unnecessary function (e.g., location data access) where possible;

82.5. patch the firmware of the fitness bands and update the mobile apps timely to enhance security; and

82.6. purge the data in the fitness bands before disposal/resale.

83. Based on the results and findings of this Sweep exercise, the PCPD has released the Infographic entitled “Protect, Respect Personal Data – Smart Use of Internet of Things[11]” to remind users on how to protect their personal data privacy when using IoT devices.

[11] See https:// www.pcpd.org.hk/english/resources_centre/publications/surveys/files/sweep2016_e.pdf

Appendix A – List of Selected Fitness Bands and Mobile Apps

Fitness band	Mobile app	Manufacturer	Download date and version of mobile app	
			Android	iOS
Local fitness bands				
innoBand-D	innoBand	3 N Half Limited	12 April 2016 v.1.1.6	13 April 2016 v.1.4.1
iHeHa Dao	HeHa	Heha Digital Health Limited	11 April 2016 v.2.5.0	13 April 2016 v.2.5.0
Archon Touch Fitness Wristband	Archon	Millennium Pacific Concept Limited	27 April 2016 v.3.4.60	13 April 2016 v.3.1.62
Digicare ERI Fitness Activity Tracker	DigiCare	DigiCare Technology Limited	14 April 2016 v.1.7.4	13 April 2016 v.3.1.2
ELAH BT-009	MyWay Fit	R.E.A.C. Electronic Company Limited	17 May 2016 v.3.3.60	17 May 2016 v.1.3.4
US fitness band				
Fitbit Alta	Fitbit	Fitbit, Inc.	12 May 2016 v.2.24	12 May 2016 v.2.21.1(488)

Appendix B – Questionnaire of the Sweep

Basic info Device type	Wearable ☐ Health-related device ☐ Smart TV ☐ Appliance ☐ Smart meter ☐ Connected car ☐ Other ☐ Please state													
Device/ company details	Device name:	Name of organisation:	Sector:	Relationship of org to device:	Country of relevant company:									
Collection, use & disclosure of data	Does the website/app have a privacy policy? ☐Y ☐N Do privacy communications indicate what personal information is collected by the device? ☐Y ☐N Are privacy communications specific to the device? ☐Y ☐N Do privacy communications state that personal information is disclosed to other companies and for what purpose? ☐Y ☐N ☐ Don’t know If the company does share information with other companies, is the user told *which* companies? ☐Y ☐N ☐N/A Are users told to change the default settings for the device? ☐Y ☐N How do users consent to the collection of their personal data? ☐ Through literature ☐ On the device itself ☐ During registration ☐ Other ……………………. ☐ Don’t know													
Information collected	**During registration**									**During use**				
	Name	User name	Address	Phone number	Email address	DOB/ age	Weight/ height	Medical details (e.g. diabetic)	Other (please state)	Location	Health/ Fitness info (e.g. heartrate)	Photo/ Video/ Audio file	Unique device ID	Other (please state)
Mandatory **O**ptional **N**ot **C**ollected	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC
Explanation for how info is used	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N
Storage of information and safeguards	Do privacy communications make reference to the *storage* of personal information collected by the device? ☐Y ☐N Is personal information stored and/or transferred in an *encrypted* form? ☐Y ☐N ☐Don’t know Do privacy communications mention the use of security safeguards to keep unauthorised users from accessing the device or data? (e.g. password protections or authentication questions?) ☐Y ☐N													

Storage of information and safeguards	Is the data stored in the same country as the manufacturer/relevant data controller? ☐Y ☐N ☐Don’t know Does the company use third parties to store data? ☐Y ☐N ☐Don’t know (***If company is contacted directly***) Did the company conduct any risk assessment procedures to identify potential privacy risks associated with the device? ☐Y ☐N ☐Don’t know				
Contact information	Do privacy communications include contact details to allow a user to contact the company about privacy related matters? ☐Y ☐N				
Deleting personal information	How many steps are required to delete personal information from the device? .... Are deletion instructions clear and easy to follow? ☐Y ☐N ☐N/A If a user sells their device, does the company provide tools to help clear the device of personal data? ☐Y ☐N ☐Don’t know If a user loses their device, are tools available to delete/remove personal data from the device (i.e. remote wiping)? ☐Y ☐N ☐Don’t know				
OPTIONAL **DC response**	Did the data controller respond within the deadline? ☐Y ☐N Did the response address all questions? ☐Y ☐N Was the response clear and easy to understand? ☐Y ☐N				
INDICATOR Based on the above responses	1) Do privacy communications adequately explain how PI is **collected, used** and **disclosed**?	2) Are users fully informed about how personal information collected by the device is **stored** and are there **safeguards** to prevent loss of data?	3) Do privacy communications include **contact details** for individuals wanting to contact the company about a privacy-related matter?	4) Do privacy communications explain how a user can **delete** their information?	5) Did the data controller provide a **timely**, **adequate** and **clear** response?
RESPONSE Answer: Y or N (see advice below)					
Comments: Any positive observations identified during the Sweep (in relation to the communication of privacy information to customers) – whether related to the questions or not.			Any additional concerns identified during the Sweep – whether related to the questions or not.		