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

2017 Study Report on User Control over Personal Data in Customer Loyalty and Reward Programmes

18 December 2017

Table of Contents

I. Executive Summary

The Privacy Commissioner for Personal Data, Hong Kong (**PCPD**) participated in the Privacy Sweep of the Global Privacy Enforcement Network (**GPEN**) for the fifth consecutive year in 2017.

2. The theme of the global Privacy Sweep 2017 is "**User Control over Personal Information**". Twenty-four privacy enforcement authorities from around the world, including the PCPD, participated in the Privacy Sweep to evaluate the privacy practice of various sectors, mainly by conducting desktop review of the personal information collection forms, privacy policies and personal information collection statements.

3. During the Sweep period between 22 and 26 of May 2017, the PCPD examined **30 customer loyalty and reward programmes** selected from six sectors, i.e. retail, hotel, catering, airlines, cinema and gasoline.

4. The PCPD's major observations from the Sweep are summarised below:

A. **Lack of transparency**. Although all the customer loyalty and reward programmes examined had privacy policies in place, the policies generally lacked transparency because the terms used therein were too broad and vague.

B. **No meaningful consent.** Majority of the programmes obtained "bundled consent"[1] from customers during registration to use their data for multiple purposes. The customers usually did not have genuine choice.

C. **Lack of control over personal data.** Customers could not exercise effective control over their personal data because they were usually not provided with means to, for example, request for data deletion

[1] The consent given is "bundled" in such a way that customers could not give consent to the terms and conditions relating to the services subscribed for without also consenting to the use of their personal data for unrelated purposes.

and to object to data sharing and profiling. The rise of data broker's industry casts further doubt on where the data will end up in.

D. **Privacy risks relating to big data analytics[2] and profiling.** Many programmes indicated in their privacy policies their intention to use personal data for big data analytics, profiling and/or automated decision making, which would amplify the privacy risks, such as:

- excessive collection of personal data;
- re-identification of individuals from anonymous data; and
- revelation of details about an individual's intimate life.

5. The PCPD urges operators of customer loyalty and reward programmes to be frank with their customers about their privacy policies and practices, respect the customers' right to personal data privacy and provide the customers with control over their own personal data. The PCPD also advises individuals to think twice before joining customer loyalty and reward programmes, taking into consideration the privacy risks.

II. Objectives of the Sweep

6. GPEN was established in 2010 upon recommendation by the Organisation for Economic Co-operation and Development to foster cross-border co-operation among privacy regulators in an increasingly global market. The Privacy Sweep aims to:

- broaden public and business awareness of privacy rights and responsibilities;
- identify privacy concerns which need to be addressed; and
- encourage compliance with privacy legislation.

7. The Privacy Sweep 2017 aimed to examine privacy policies and practices of data users with a view to evaluating user controls over personal data. Thirty customer loyalty and reward programmes in Hong Kong are selected from six

[2] "Big data analytics" refers to the analysis of large volumes of data, i.e. big data, derived from a wide variety of sources to uncover patterns and connections of different matters and behaviours that might otherwise be invisible, and that might provide valuable insights.

sectors, i.e. retail, hotel, catering, airlines, cinema and gasoline, because of their popularity in the local market and their potential to collect substantial amount of personal data from large number of individuals.

III. Methodology of the Sweep

8. The PCPD conducted the Sweep by examining the following information of the customer loyalty and reward programmes:

- privacy policies;
- personal information collection forms; and/or
- personal information collection statements.

9. For the purpose of this report, privacy policy and personal information collection statement are collectively referred to hereinafter as "privacy policy".

IV. The Global Sweep Results

10. Twenty-four privacy enforcement authorities around the world, including the PCPD, examined the privacy policies and practices of 455 data users in various sectors including retail, finance & banking, travel, social media, gaming/gambling, education and health. Major observations from the global Privacy Sweep are listed below.

- Privacy policies and practices across the various sectors tended to be vague, lacked specific details and often contained generic clauses.
- Majority of the organisations failed to inform users/customers what would happen to their information once it had been collected.
- Organisations were generally quite clear on what information they would collect from users/customers.
- Organisations generally failed to specify with whom personal data would be shared.

- Many organisations failed to address the security aspect of the data collected and held. It was often unclear in which country data was stored or whether any safeguards were in place.
- Just over half of the organisations examined made reference to how users/customers could access the personal data held about them.

V. The PCPD's Sweep Results

11. The privacy policies and practices of the customer loyalty and reward programmes examined may change over time. Hence, the PCPD's Sweep results only represent the position as of May 2017.

12. PCPD's observations are largely in line with the global ones as discussed above. Major observations by the PCPD during the Sweep are summarised under the following four headings:

- lack of transparency;
- no meaningful consent;
- lack of control over personal data; and
- privacy risks relating to big data analytics and profiling.

A. Lack of transparency

13. The PCPD found that all 30 customer loyalty and reward programmes (100%) had privacy policies and 29 of them (96.67%) were easy to locate.

14. However, many privacy policies lacked clarity because broad and vague descriptions were used. For example:

- some privacy policies gave vague descriptions of the classes of persons with whom personal data would be shared, such as "*our parent companies*", "*any of our subsidiaries*", "*corporation in connection with the company*", and "*business partners who provide administrative, telecommunications…or other services to any of [our affiliates]*";

- some purposes of personal data collection stated in the privacy policies were described in broad and vague terms, such as "*to better marketing strategy and make our service more relevant to each member*"; "*for the use by any of our subsidiaries, associate companies and/or business associates in connection with…any other travel related services and offers such companies and associates may offer from time to time.*"
- five privacy policies (16.67%) did not specify what personal data would be collected, making it difficult for customers to understand clearly the extent of data collection; and
- three privacy policies (10%) did not specify whether personal data would be disclosed to third parties.

B. No meaningful consent

15. All 30 programmes (100%) required customers to agree to their privacy policies in order to proceed with the applications. By agreeing to the policies, the customers gave bundled consent to all uses[3] of their personal data stated therein. In other words, customers were deemed to have agreed to all purposes of use as stated therein, even if some were not related to the operation of the programmes, such as "*facilitate matching for whatever purpose with other personal data*".

16. Business enterprises or organisations tended to draft the privacy policies broadly to cover every eventuality and with no granular options. Customers could only take it or leave it. Hence, many customers might skip the privacy policies and give consent right away. Without genuine choice, there could not be meaningful consent. As a result, customers may be surprised or even feel aggrieved when they learn that their personal data were used in a way beyond their expectation. This would probably damage the reputation of the programme operators.

[3] Except for the use of personal data in direct marketing activities, of which customers were generally allowed to opt out during or after registration.

C. Lack of control over personal data

Right to request deletion of personal data

17. The Personal Data (Privacy) Ordinance (**Ordinance**) does not provide individuals with the right to request deletion of their personal data, but only requires data users to erase personal data when the original purposes (including the directly related purposes) of collection are fulfilled[4]. However, as a good practice, data users should provide effective means for individuals to request deletion of their personal data when the individuals intend to end the contractual or other relationship with the data users, unless the data users have strong reasons to retain the same which override the data subjects' right to personal data privacy.

18. However, the Sweep showed that 22 programmes (73.33%) did not provide customers with any information on how to delete their personal data. Twenty-six programmes (86.67%) did not mention about the retention period of personal data in general and 25 programmes (83.33%) did not explain the retention period of data in relation to dormant or inactive accounts.

Right to object to sharing of personal data and profiling

19. Many operators of the customer loyalty and reward programmes obtained consent from customers in a way that bundled with other extensive processing of their personal data which are unrelated to the services offered to customers in the programmes. As a good practice, and in order to provide customers with control over their personal data, data users should allow and provide effective means to customers to opt out from processing activities which are not necessary for the operation of the customer loyalty programmes, such as sharing of personal data for market research, analytics and profiling of customers. "Profiling" refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular

[4] Section 26(1) of the Ordinance stipulates: "*A data user must take all practicable steps to erase personal data held by the data user where the data is no longer required for the purpose (including any directly related purpose) for which the data was used unless- (a) any such erasure is prohibited under any law; or (b) it is in the public interest (including historical interest) for the data not to be erased.*"
Data Protection Principle 2(2) of the Ordinance stipulates: "*All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data is or is to be used.*"

to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements[5].

20. Among 28 programmes (93.33%) which indicated the intention to share personal data with third parties, and 29 programmes (96.67%) which indicated that the personal data collected would be used in profiling or related activities, only 1 (3.57%) and 0 (0.00%) programmes respectively provided means for an individual to opt out from these sharing or processing. This indicated a lack of control by individuals over their own personal data.

D. Privacy risks relating to big data analytics and profiling

21. Most of the customer loyalty and reward programmes (29 or 96.67%) indicated in their privacy policies that they intended to use customers' personal data for research, analytics and/or profiling in order to provide customers with, for example, personalised marketing, services or products. Although customers may benefit by receiving more customised advertisements, services or products, the privacy risks involved must not be ignored. For example, big data analytics and profiling require enormous amount of data in order to generate useful insights and build comprehensive profiles of individuals. This may lead to excessive collection and amassment of personal data. Also, by aggregating and analysing data from various sources, anonymous individuals may be re-identified, and intimate lives of individuals may be revealed.

22. Indeed, predictions and inferences about customers produced by big data analytics and profiling can be surprising and privacy-intrusive. Earlier, a U.S. retailer analysed customers' shopping habits and accurately guessed that a teenage girl was pregnant before her father knew about it[6].

23. Big data analytics and profiling rely on correlations, as opposed to causalities, in discovering patterns and identifying trends. As a result, the inference about an individual derived from big data analytics and profiling may be inaccurate or unfair. For example, by coincidence, an individual might habitually

[5] See the definition in Article 4(4) of the General Data Protection Regulation of the European Union.

[6] The New York Times Magazine, "How Companies Learn Your Secrets" (16 February 2012): http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp

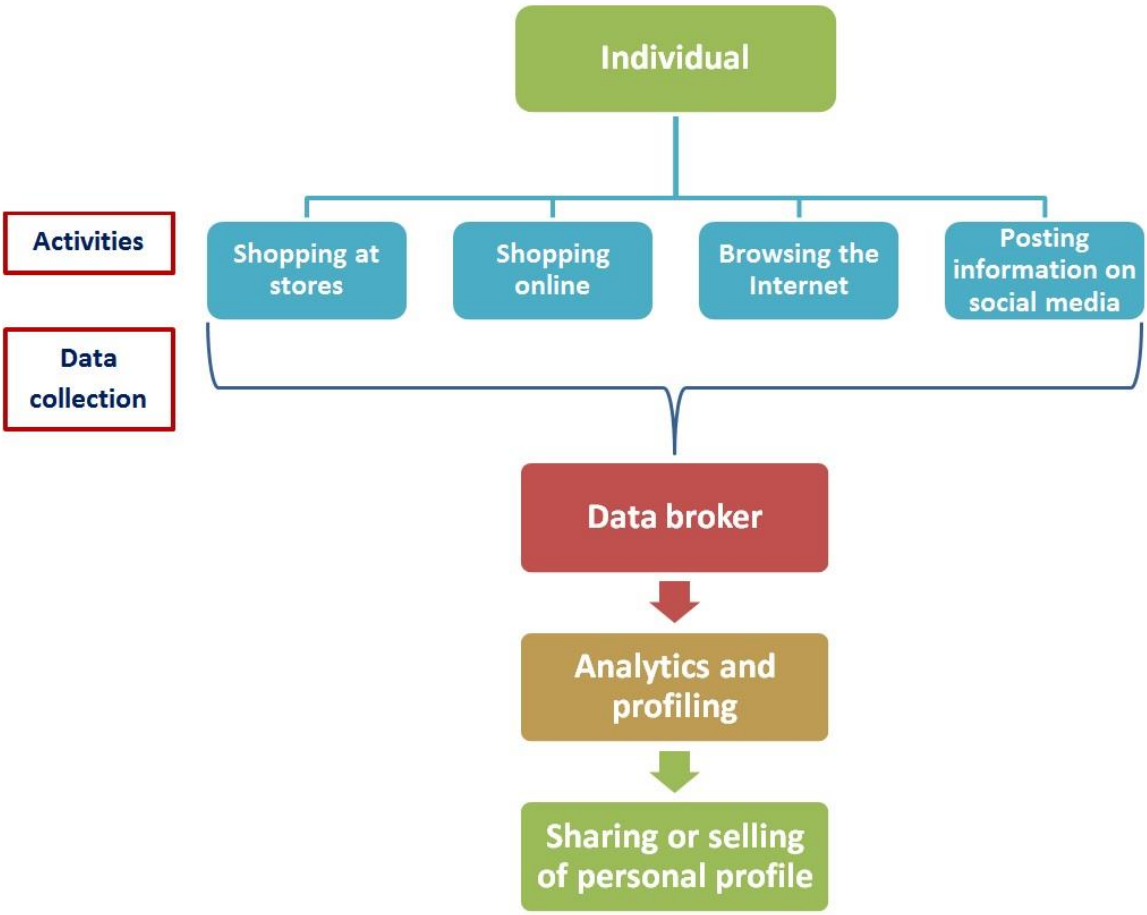
shop at stores frequented by people deemed by credit card companies to have a poor repayment history; however, it may well be incorrect or unfair for the individual's credit card company to lower his credit score and credit limit by this reason alone[7].

24. The rise of data broker industry may magnify the privacy risks above. According to a report by the Federal Trade Commission of the U.S.[8], data brokers are companies which collect personal information from a wide variety of sources and then resell the same to businesses, often without customers' knowledge and consent, and operate with low transparency. To make the data appealing to buyers, data brokers may engage analytics to profile customers into different categories. Data are usually sold to third parties for marketing, fraud detection, people search and other purposes. Without knowing that their personal data would be transferred to data brokers or other third parties for other purposes, individuals may well be deprived of their right to exercise control over their personal data, and may be subject to unfair or discriminatory treatments ignorantly.

[7] Financial Times, "Big data: Credit where credit's due" (5 February 2015): https://www.ft.com/content/7933792e-a2e6-11e4-9c06-00144feab7de

[8] U.S. Federal Trade Commission, "Data Brokers – A Call for Transparency and Accountability" (May 2014): https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Profiling of an individual



25. Having considered the very broad and vague terms used in their privacy policies, the operators of the customer loyalty and reward programmes might have failed to communicate to customers effectively on the transfer or even sale of their personal data to data brokers. The customers may well be caught by surprise when they learn about the disclosure of their personal data to unknown parties for uses in unexpected purposes, or even to their detriment.

VI. Conclusions and Recommendations

26. To conclude, the PCPD noted that the privacy policies of the examined programmes had low transparency which did not facilitate customers' understanding of privacy practices. Customers were unable to provide meaningful consent to the collection and use of their personal data. They were unable to

exercise effective control over their personal data in aspects of data deletion, data sharing and profiling either.

27. The PCPD recommends operators of customer loyalty and reward programme to improve their privacy practices in the following ways:

- **Transparency**: Provide a privacy policy which is precise, concise and easy to understand. Avoid using obscure and legalese language.

- **Avoidance of surprises**: Explain to customers frankly and clearly the types of data to be collected. Specify the purposes of collection. Identify clearly the parties to whom personal data may be shared.

- **Respect**: Provide customers with granular options (as opposed to bundled consent) regarding the collection and use of their personal data. If possible, allow customers to opt out from certain use (including profiling) or sharing of their personal data.

- **Accountability and ethics**: Take into account the reasonable expectation of customers, as well as the privacy risk and potential harm (including physical, financial and psychological) to the customers, when deciding on the use (including disclosure) of the customers' personal data.

28. The PCPD also reminds individuals to read the privacy policy carefully to understand the possible use and sharing of their data, and assess the related privacy risks before joining any customer loyalty and reward programmes.

Appendix - The Sweep Statistics

1.	Do the programmes have privacy policies?	Number	Percentage
	Yes	30	100%
	No	0	0%

2.	Among the programmes which have privacy policies in Q1 above (total 30), are the policies easy to locate?	Number	Percentage
	Yes	29	96.67%
	No	1	3.33%

3.	Do the privacy policies specify what personal data will be collected?	Number	Percentage
	Yes	25	83.33%
	No	5	16.67%

4.	Do the programmes specify whether personal data will be disclosed to third parties?	Number	Percentage
	Yes	27	90%
	No	3	10%

5.	What types of personal data are collected from customers?	Collect (Both voluntary and mandatory)		Not Collect	
		Number	Percentage	Number	Percentage
	Name	30	100%	0	0%
	Username	3	10%	27	90%
	Address	21	70%	9	30%

5.	What types of personal data are collected from customers?	Collect (Both voluntary and mandatory)		Not Collect	
		Number	Percentage	Number	Percentage
	Phone number	28	93.33%	2	6.67%
	Email Address	30	100%	0	0%
	Gender	27	90%	3	10%
	Nationality	9	30%	21	70%
	Education Level	5	16.67%	25	83.33%
	Occupation	8	26.67%	22	73.33%
	Marital Status	8	26.67%	22	73.33%

6.	Do the programmes provide any instructions on how to delete personal data?	Number	Percentage
	Yes	8	26.67%
	No	22	73.33%

7.	Do the programmes mention the retention period of personal data?	Number	Percentage
	Yes	4	13.33%
	No	26	86.67%

8.	Do the programmes provide retention policies for dormant/inactive accounts?	Number	Percentage
	Yes	5	16.67%
	No	25	83.33%

9.	Do the programmes make reference to the sharing of personal data?	Number	Percentage
	Yes	28	93.33%
	No	2	6.67%

10.	Among the programmes which make reference to the sharing of personal data in Q9 above (total 28):	Number	Percentage
	Programmes that share personal data for both direct marketing and non-direct marketing purposes	27	96.43%
	Programme that share personal data for direct marketing purpose only	0	0%
	Programme that share personal data for non-direct marketing purpose only	1	3.57%

11.	Among the programmes which make reference to the sharing of personal data in Q9 above (total 28), do they mention with whom the data will be shared?	Number	Percentage
	Yes	18	64.29%
	No	10	35.71%

12.	Among the programmes which make reference to the sharing of personal data in Q9 above (total 28), do they mention the purpose of data sharing?	Number	Percentage
	Yes	24	85.71%
	No	4	14.29%

13.	Among the programmes which share data for non-direct marketing purposes in Q10 above (total 28), do they provide means for customers to opt out from sharing?	Number	Percentage
	Yes	1	3.57%
	No	27	96.43%

14.	Do the programmes mention about the intention to use collected personal data for profiling?	Number	Percentage
	Yes	29	96.67%
	No	1	3.33%

15.	Among the programmes which mentioned about the intention to use collected personal data for profiling in Q14 above (total 29), do they provide means for customers to object to profiling?	Number	Percentage
	Yes	0	0%
	No	29	100%

16.	Do the programmes mention whether any decisions affecting the customers may be made by automated means (i.e. automated decision making)?	Number	Percentage
	Yes	10	33.33%
	No	20	66.67%