THE UNIVERSITY OF HONG KONG
SOCIAL SCIENCES RESEARCH CENTRE
Director: Professor J. Bacon-Shone *(PhD Birmingham)*

香港大學
社會科學研究中心
主任: 白景崇教授

Baseline Survey of Public Attitudes on Privacy and Data Protection 2014

Main Report

Table of Contents

List of Figures

Executive Summary

Introduction

The Social Science Research Centre of The University of Hong Kong (SSRC) was commissioned by the Office of the Privacy Commissioner for Personal Data (PCPD) to conduct a survey of public attitudes on personal data privacy on a scientific basis between November and December 2014, so as to provide the PCPD with a useful reference to make informed decisions on strategies, educational and promotional plans/activities in the future, to provide the PCPD with information regarding public general awareness and perceptions on privacy data protection, and issues related to their everyday life.

Research Methodology

This study comprises a household telephone survey of the Hong Kong adult population and focus group interviews with the Hong Kong adult population. The household telephone survey was conducted by using Computer Assisted Telephone Interviews (CATI) and the sample of residential telephone numbers was generated from the latest English residential telephone directory by dropping the last digit, removing duplicates, adding all 10 possible final digits, randomising order, and selecting as needed. The target respondents were Cantonese, Putonghua or English speaking and aged 18 or above. A bilingual (Chinese and English) questionnaire was used to collect data. Fieldwork took place between 25th November and 17th December 2014. Sample sizes of 1,222 respondents were successfully interviewed. The contact rate was 30.6% and the overall response rate was 62.2%. The width of a 95% confidence interval was at most +/- 2.8% and weighting was applied in order to make the results more representative of the general population. Statistical tests were applied to investigate if there is any significant association between demographics and the response variables. Only the significant findings at the 5% level (2-tailed) are presented in the report.

4 focus group interviews with a total of 36 participants were conducted, designed to reflect different opinions of the general public:

i. People aged between 18 and 40 (males and females);

ii. People aged 41 and above (males and females);
iii. People with lower education level i.e. secondary education or below (males and females); and
iv. People with higher education level i.e. post-secondary education or above (males and females).

Key Findings of the Survey

The household telephone survey respondents were weighted by age and gender to match the Hong Kong population data compiled by the Census and Statistics Department (C&SD) for mid 2014.

Privacy attitudes about the use of ID cards

From the results of the household telephone survey, around 30% of respondents did not mind legitimate, justified use of ID card information at all, while nearly 40% did mind clearly unjustified use of ID card information.

Privacy attitudes to providing different types of personal data

From the results of the household telephone survey, few respondents were very concerned about providing mobile phone number (even though it allows receiving advertising calls), occupation or full date of birth (even though it is often used for validation), but many expressed legitimate concern about providing personal income and ID card number.

Privacy for public registries, CCTV & loyalty cards

For the use of personal data made public by public registries, 13-15% of respondents had no concern and 18% had serious concern about the marriage and lands registry. For the ID card number and residential address of a company director, 28-35% had serious concern, again supporting that this information is seen as sensitive. For CCTV covering your doorway, 16% had no concern, while 23% had serious concern. 67% of respondents had serious concern and only 1-2% of respondents had no concern as regards provision of their or their friends/relatives names and addresses when applying for a loyalty card, suggesting that this is widely seen as invasion of privacy.

Misuse of personal data

From the results of the household telephone survey, nearly half (46%) of respondents had experienced misuse of their personal data in the last 12 months and the most common source of the problem was banks (57%), followed by telecom companies (32%), fitness/beauty centres (26%) and money lenders (17%). (Whereas in 2001 the most frequent sources were banks, real estate agents and telecom companies.)

Almost 11% of those who experienced misuse had made a complaint, while those who had not complained explained that the major reasons were that friends had provided the information (35%), or they were unwilling to involve the company staff (25%) responsible for the misuse.

For the notification of data leakage to data subjects and PCPD, all participants in the focus group interviews generally agreed that the data subjects and PCPD as well as the media should be notified immediately.

Awareness of the work of the PCPD

From the results of the household telephone survey, the majority of respondents (63%) were aware of the PCPD through mass media, with smaller proportions through the website/multimedia (19%), PCPD publications (15%) and the PCPD publicity programmes (7%). An overwhelming majority (86%) of respondents agreed or strongly agreed that PCPD has increased community awareness of personal data privacy issues after the Octopus Incident in 2010, with only 14% disagreeing/strongly disagreeing.

Naming the Organisations at Fault

Most of the participants in the focus group interviews agreed that PCPD publishing reports that name the organisation at fault was effective because it raised public awareness of personal data protection and most of them reported that their confidence or trust had decreased towards those companies against which PCPD had reported contraventions of the Personal Data (Privacy) Ordinance (PD(P)O).

Whether the current regulatory framework provides sufficient protection

From the results of the focus group interviews, only several participants aged 41 and above or with lower education level thought the current regulatory framework was sufficient to protect the public and many of them did not have any ideas about the regulatory framework. No participants with higher education level thought the current regulatory framework was sufficient to protect the public because they were concerned that the current situation was that people were forced to provide personal data and a lot of personal data could be found openly.

Aware of the consequences of non-compliance with the PD(P)O and what they expect the PCPD to do

From the results of the focus group interviews, most of the participants did not know the consequences of violating the PD(P)O.

Direct marketing and the PD(P)O amendment

From the results of the focus group interviews, only a few participants aged between 18 and 40 or with lower education level were aware that companies had to notify potential customers and get their consent first before using their personal data for direct marketing. However, most of the participants aged 41 or above or with higher education level were aware of this notification and consent requirement.

The minority of the participants in the focus group interviews knew that direct marketing calls could cover only the type of products that they agreed to, when giving approval to use their personal data for direct marketing.

Many participants in the focus group interviews knew that organisations could not transfer their personal data to a third party for use in direct marketing unless written consent has been obtained.

The majority of participants aged between 18 and 40 knew that they had the right to opt out from direct marketing even if they had opted in before. However, the majority of participants aged 41 and above did not know that they had the right to opt out.

The minority of participants in the focus group interviews had heard of the revision of the PD(P)O, including the enhanced protection for direct marketing. After a brief introduction of the PD(P)O amendment in force since 2013 about direct marketing,

the majority of participants believed that the PD(P)O amendment since 2013 was not sufficient to protect the public, because of limited enforcement powers.

Trustworthiness in handling complaints

The perceived trustworthiness of the PCPD (25%) edged out the Consumer Council (24%), and is the second most trusted agency after Independent Commission Against Corruption (33%). The respondents gave their perceived trustworthiness rating to the following six statutory agencies in handling complaints:

Consumer Council (rating as 9 or 10: 24.3% vs rating 5 or less: 30.0%)
Hong Kong Police Force (19.9% vs 42.5%)
The Ombudsman Hong Kong (19.7% vs 34.9%)
Equal Opportunities Commission (16.4% vs 38.1%)
Independent Commission Against Corruption (32.7% vs 23.4%)
Office of the Privacy Commissioner for Personal Data (25.0% vs 29.9%)

Privacy attitudes towards online activities

(a) Advertising and privacy

From the results of the household telephone survey, the majority of respondents (56%) would certainly not be prepared to pay $20 per month for email services like Gmail with the promise of no advertising at all, while only 6% would be certainly willing suggesting that most people are reluctant to pay for privacy protection.

(b) Facebook and privacy

From the results of the household telephone survey, the majority of respondents (56%) who have ever had a Facebook account use Facebook at least daily with only 18% rarely or never using their account. A strong majority (77%) of Facebook account users are aware of the privacy setting, of whom a strong majority (73%) have ever checked the settings, of whom nearly all (90%) have changed the settings. This suggests that people are now generally aware of the need of privacy protection in social networks and can act to protect themselves. (A privacy awareness survey on Facebook users conducted by the PCPD in 2013 found that over 80% of the respondents knew how to set access right to protect their personal data, but less than 40% did so.)

(c) Smartphones and privacy

From the results of the household telephone survey, an overwhelming majority (87%) of respondents use a smartphone of whom 95% have WeChat or a similar app installed, although 19% did not install it themselves. Only 72% of respondents with WeChat or a similar app installed were aware that it accesses all of the contacts on their smartphone, while a significant proportion (33%) thought the law should prohibit this.

Privacy tradeoffs

Most participants aged between 18 and 40 or with lower education level in the focus group interviews were not willing to provide their own or others' personal data for money or other benefits. Conversely, participants aged 41 or above or with higher education level were willing to provide their own personal data except ID number in exchange for benefit and benefit-in-kind, but not willing to provide others' personal data.

In summary, the results indicate that awareness of the PCPD, of privacy rights of individuals and their friends and trust in the PCPD are generally quite high and there is good awareness of the need to balance privacy rights differently in different situations. However, concerns about some current practices of public registries suggest public support for further action by the PCPD.

The widespread support for naming the organisations at fault suggests that the PCPD should make further use of this strategy in promoting compliance.

The general public seems unaware of how limited the enforcement powers of the PCPD are, suggesting a need for further education about this, which may increase support for additional powers, especially as better educated participants did not believe that the current regulatory framework was sufficient to protect the public.

The support for data leakage to be always reported to the PCPD suggests public support for making this a mandatory requirement.

People are much more likely to be aware of the privacy protection required on Facebook. However, with further advances in ICT such as the prevalent use of

mobile apps, the PCPD will need to continuously face the privacy and data protection challenges by stepping up efforts in enforcement as well as public education.

Chapter 1 Introduction

1.1 Background

The Privacy Commissioner For Personal Data ("PCPD") is an independent statutory body established to oversee the compliance of the Ordinance which is enacted to protect the personal data privacy rights of individuals and to provide for the regulation of the collection, holding, processing, security and use of personal data. The PCPD commissioned the Social Sciences Research Centre of the University of Hong Kong (HKUSSRC) to ascertain general public attitudes on personal data privacy on a scientific basis, so as to provide the PCPD with a useful reference to make informed decisions on strategies, educational and promotional plans/activities in the future, to provide the PCPD with information regarding public general awareness and perceptions on privacy data protection, and issues related to their everyday life.

1.2 Research Objectives

The objectives of the Study were:

(a) To assess the degree of sensitivity or importance people ascribe to different types of personal data
(b) To find out how people exercise their right under the Ordinance when they find their personal data being misused
(c) To find out public perception of PCPD's performance (public trust, efficiency, effectiveness)
(d) To assess the public awareness of the social media platform's privacy problem

Chapter 2 Research Methodology

2.1 Scope of Study

The scope of this study encompasses a household telephone survey of the Hong Kong adult population to cover the following issues:

- Privacy attitudes about the use of ID cards
- Privacy attitudes about providing personal data
- Privacy for public registries, CCTV & loyalty cards
- Misuse of personal data
- Awareness of the work of the PCPD
- Trustworthiness of PCPD in handling complaints
- Advertising and privacy
- Facebook and privacy
- Smartphones and privacy

The study also includes focus group interviews with the adult population covering the following issues:

- Enforcement powers of PCPD
  - Whether they are aware of any PCPD media briefing in the past
  - To assess their awareness and expectations of the role of the PCPD
  - Whether the participants are aware of the consequences of non-compliance with the Ordinance and what they expect the PCPD to do
  - To find out whether they think the current regulatory framework is sufficient to protect them
  - To find out whether the PCPD publishing investigation reports naming the organisation at fault, works effectively
- Direct marketing and the Personal Data (Privacy) Ordinance ("PD(P)O") amendment
  - To investigate whether they are aware that organisations are required to provide data subjects with notification (i.e. intention to use the personal data in direct marketing) and obtain their consent before using their personal data for direct marketing
  - To assess how they respond to direct marketers' notifications

- To investigate whether they know that the organisations can only promote products or services that he/she previously consented to (i.e. permitted class of marketing subject)
- To investigate whether they know that the organisations cannot transfer their personal data to third party (no matter for gain or not) for use in direct marketing unless written consent has been obtained
- To assess whether they are aware of their opt-out right
- To understand how people respond to direct marketers if they do not wish to receive promotional messages
- To investigate whether the PD(P)O amendment enforced in 2013 is sufficient

➢ Notification of data leakage to data subjects and PCPD
  - To identify their expectation as to whether PCPD or data subjects should be notified and when

➢ Dealing with organisations with "respect for privacy"
  - To what extent "respect for privacy" would be a factor in choosing a service or a product offered by an organisation
  - Whether PCPD issues investigation reports about organisations contravening the PD(P)O would affect their willingness to deal with those organisations
  - To identify their actions when they discover that their personal data has been misused
  - Refer to the Octopus case, whether they would consider using the anonymous Octopus card instead of a personalised card or one registered for Octopus rewards and the reasons not to consider.
  - Refer to the California Fitness case and assuming that they want some fitness training, whether the PCPD reporting their collection of ID card copies would affect their decisions about which fitness company to enrol with.

➢ Publicly available personal data
  - To investigate whether they search for information about another person via search engines online and the information is for personal interest or work related purpose
  - To investigate whether they expect their personal data to be found by others using search engines online

- To investigate their expectation of their personal data available in the public domain to be used indiscriminately
- To identify how they balance transparency, public interest, and privacy protection
- To investigate whether they understand the consequences of being part of a social network and whether they would ask for peers' consent before posting their personal data (e.g. photos)

➢ Privacy tradeoffs they would consider

- To assess their confidence to protect their personal data when purchasing from online shops and physical shops
- To what extent they are willing to compromise personal data protection in exchange for efficiency and convenience online
- Whether they are willing to compromise personal data protection (of their own, family and friends) in exchange for benefit and benefit-in-kind

➢ Facebook & Mobile Apps

- In general, whether they expect transparency about the collection and use of their information from Facebook and before installation of mobile apps, regardless of whether the information is personal data
- Whether they read and understand the information provided by apps prior to installation and the reasons for not doing this
- To investigate their views on the iOS and Android location requests

2.2 Organisation of the Report

The report is divided into Chapter 1, which contains the background, Chapter 2, which contains the research methodology, Chapter 3, which covers the household telephone survey, Chapter 4, which covers the focus group interviews, while Chapter 5 provides a summary of the integrated findings.

Chapter 3 Household Telephone Survey

3.1 Survey Research Methodology

3.1.1 Study Design and Target Respondents

The target population of this survey is randomly selected Hong Kong adults aged 18 or above.

3.1.2 Obtaining Ethical Approval

Ethical approval was obtained from the Human Research Ethics Committee for Non-Clinical Faculties of The University of Hong Kong prior to the commencement of the Study.

3.1.3 Pilot Study

A pilot study comprising 51 successfully completed interviews was conducted on 9th October 2014. Based on the feedback and comments from participants and the PCPD, the questionnaires and the logistics were fine-tuned for the main Study. Data collected from these pilot interviews are not included in this survey.

3.1.4 Data Collection

A total of 1,222 interviews were successfully completed between 25th November 2014 and 17th December 2014 via telephone survey using a Computer Aided Telephone Interview (CATI) system, calling between 6:30pm and 10:00pm. All interviewers studied the questionnaire instructions and successfully completed a practice interview before making phone calls. The supervisor reviewed the interviews to see whether the interviewers were employing proper question-asking and probing techniques and conducting the interview in a professional manner. General problems were also noted and instructions were clarified for every interviewer.

3.1.5 Quality Control

The following quality control measures were incorporated in the Study:

- The data collected were subjected to range checking and logical checking. Unclear and illogical answers were re-coded as invalid.
- Questionnaires with more than half of the questions unanswered were regarded as incomplete questionnaires and excluded from analysis.
- Any missing answers were excluded from analysis.
- Quality checking procedures were applied to at least 10% of the data collected prior to analysis and use, to ensure that the data were valid.

3.1.6 Response Rate

A total of 26,000 telephone numbers were attempted. However, 4,730 households were not available at that time, 600 households refused and 144 answered only part of the questionnaire. Ultimately, a total of 1,222 respondents were successfully interviewed by using the CATI in the survey. The overall contact rate was 30.6%[1] and response rate was 62.2%[2]. Table 3.1.6 shows the detailed breakdown of final telephone contact status.

Table 3.1.6 Final status of telephone phone numbers attempted

Type	Final status of contact	Number of cases
1	Success	1,222
2	Partial Case	144
3	Refusal	600
4	Not available	4,730
5	Business lines	1,227
6	Language problem	19
7	Problem (Aged under 18, etc)	7
8	Fax/data line	1,231
9	Disconnected number	10,305
10	Not answer	6,515
Total		**26,000**

[1] Contact rate = the number of answered telephone calls divided by the total number of calls attempted, sum of (type1 to 7)/ Total = (1222+144+600+4730+1227+19+7)/26000 = 30.6%.

[2] Response rate = the number of successful interviews divided by the sum of the numbers of successful interviews, partial cases and refusal cases, (type 1) / (type 1 + type 2 + type 3) = 1222/(1222+144+600)=62.2%.

3.1.7 Overall Sampling Error

The survey findings are subject to sampling error. For a sample size of 1,222, the maximum sampling error is + 2.8%[3] at the 95% level of confidence (ignoring clustering effects). In other words, we have 95% confidence that the population proportion falls within the sample proportion plus or minus 2.8%, based on the assumption that non-respondents are similar to respondents.

The table below serves as a guide in understanding the range of sampling error for a sample size of 1,222 before proportion differences is statistically significant.

95% Confidence Level
Maximum Sampling Error by Range of Proportion Response

	Proportion response				
Sample size (n=1,222)	**10%/90%**	**20%/80%**	**30%/70%**	**40%/60%**	**50%/50%**
Sampling error	± 1.7%	±2.2%	±2.6%	±2.7%	±2.8%

As the table indicates, the sampling error is at most 2.8% for a sample size of 1,222. This means that for a given question answered by the respondents, one can be 95 percent confident that the difference between the sample proportion and the population proportion is not greater than 2.8%.

3.1.8 Quality Control

All SSRC interviewers were well trained in a standardised approach prior to the commencement of the survey. All interviews were conducted by experienced interviewers fluent in Cantonese, Putonghua and English.

The SSRC engaged in quality assurance for each stage of the survey to ensure satisfactory standards of performance. At least 5% of the questionnaires completed by each interviewer were checked by the SSRC supervisors independently.

[3] As the population proportion is unknown, 0.5 is put into the formula of the sampling error to produce the most conservative estimation of the sampling error. The confidence interval width is:

$$\pm 1.96 \times \sqrt{\frac{0.5 * 0.5}{534}} \times 100\% = 4.2\%$$

3.1.9 Data Processing and Analysis

Weighting

Due to the differences between the respondents of this study and the population of Hong Kong, weighting factors were applied to adjust the data to match the age and gender distribution of the corresponding mid-year population for 2014 reported by the Census and Statistics Department of the HKSARG (C&SD). The differences in age and gender between the survey respondents and the population of Hong Kong in are shown in Table 2.2. The weighting factors are the ratio of the population of Hong Kong to the survey respondents in each gender and age group as shown in Table 3.1.7.

Table 3.1.7 Age & gender for this survey and mid 2014 population of Hong Kong

Age	This survey			Mid-year population for 2014 by C&SD		
	Male	Female	Total	Male	Female	Total
18-19	2.5%	2.5%	5.0%	1.4%	1.3%	2.7%
20-24	3.2%	4.1%	7.4%	3.5%	3.5%	7.0%
25-29	1.4%	3.6%	5.0%	3.6%	4.7%	8.3%
30-34	2.8%	3.3%	6.1%	3.8%	5.6%	9.4%
35-39	2.6%	4.0%	6.7%	3.7%	5.4%	9.0%
40-44	3.4%	6.5%	9.9%	3.9%	5.5%	9.3%
45-49	4.3%	5.5%	9.8%	4.2%	5.3%	9.5%
50-54	6.1%	8.9%	15.1%	5.0%	5.6%	10.6%
55-59	2.9%	5.3%	8.2%	4.7%	4.8%	9.5%
60-64	5.2%	5.7%	10.9%	3.7%	3.7%	7.4%
65-69	3.3%	4.2%	7.5%	2.6%	2.6%	5.2%
70-74	1.9%	2.3%	4.2%	1.8%	1.6%	3.4%
75-79	1.3%	1.1%	2.4%	1.6%	1.8%	3.4%
80-84	1.2%	0.5%	1.8%	1.2%	1.5%	2.7%
85+	0.1%	0.1%	0.2%	0.8%	1.7%	2.5%
Total	42.4%	57.6%	100.0%	45.3%	54.7%	100.0%

Descriptive Statistics

Descriptive statistics are used to summarise the findings of the Study and they are reported in frequency, percentages, means and standard deviations (SD), wherever appropriate. Some percentages might not add up to the total or 100% because of rounding. Moreover, the sample bases for each question might vary due to missing answers.

Statistical Tests

Three types of statistical tests, namely Pearson chi-square test, Kruskal-Wallis test and Spearman's rank correlation are used for sub-group analysis in this Study. When both variables are nominal, the chi-square test was used. When one variable is nominal and the other is ordinal, the Kruskal-Wallis test is adopted. When both variables are ordinal, rank correlation is used. The statistical software, SPSS for Windows version 20.0, was used for performing all statistical analyses. All significance testing was run at 5% significance level (2-tailed test). The full results for the statistical tests can be found in Appendix B.

Table 2.3 Weighting factors by age & gender

Age	Male	Female
18-19	0.545192	0.536529
20-24	1.06853	0.857555
25-29	2.566013	1.301648
30-34	1.340258	1.683074
35-39	1.393578	1.331023
40-44	1.130703	0.844475
45-49	0.970612	0.965751
50-54	0.81657	0.628465
55-59	1.627748	0.917551
60-64	0.711083	0.657846
65-69	0.785853	0.622133
70-74	0.916857	0.719431
75-79	1.228694	1.673271
80-84	0.972294	2.812195
85+	9.581615	19.10827
Refuse to answer	1	1

3.1.10 Final Questionnaire

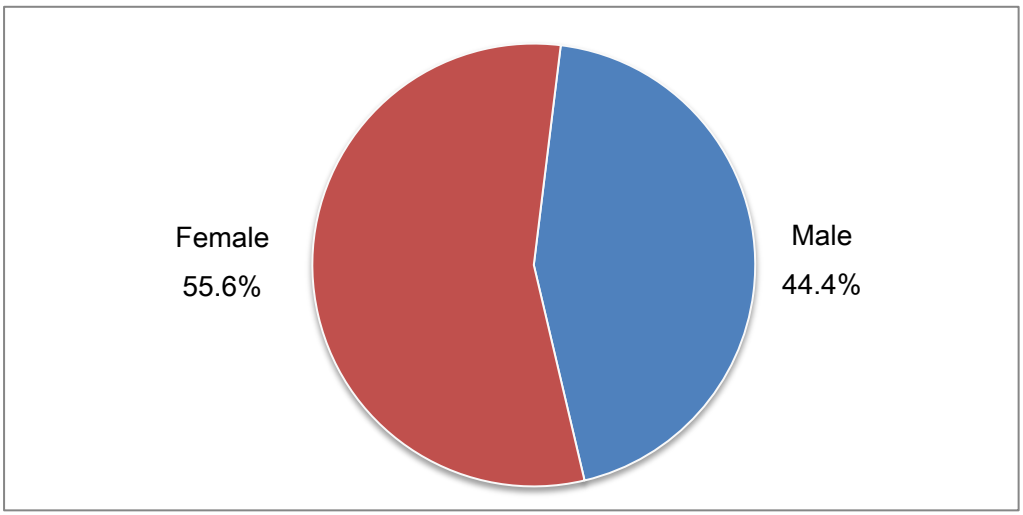
The final questionnaire can be found in Appendix A. It covers all the research objectives using practical situations that the general public should be able to evaluate from a privacy perspective.

3.2 Finding from the Household Telephone Survey

3.2.1 Demographic profile of respondents

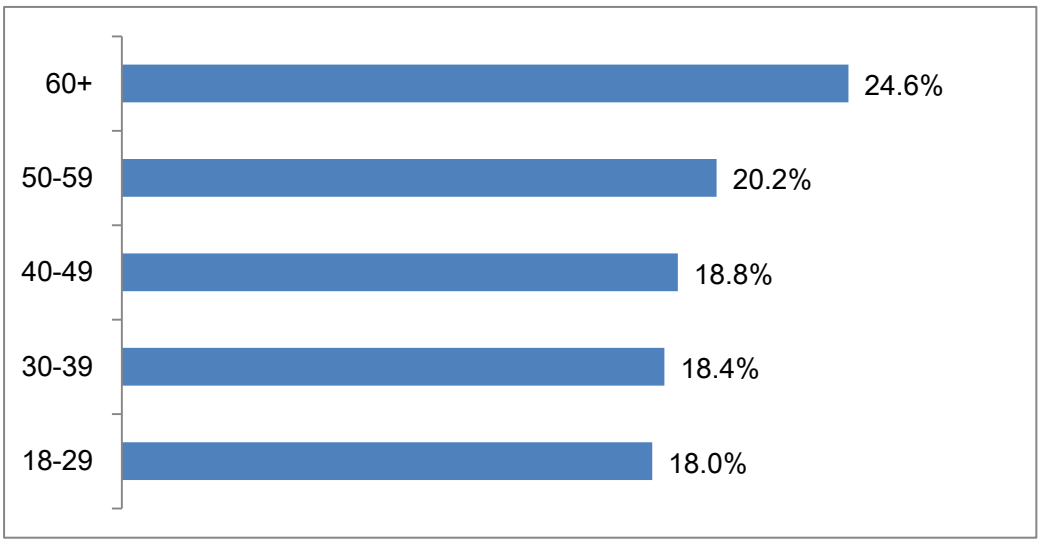
Figures 3.2.1.1-3.2.1.4 show the gender, age, education and personal income profile of respondents. Gender and age perfectly reflect the population profile because of the weighting by gender and age mentioned in Chapter 2.

Figure 3.2.1.1 Gender of respondents



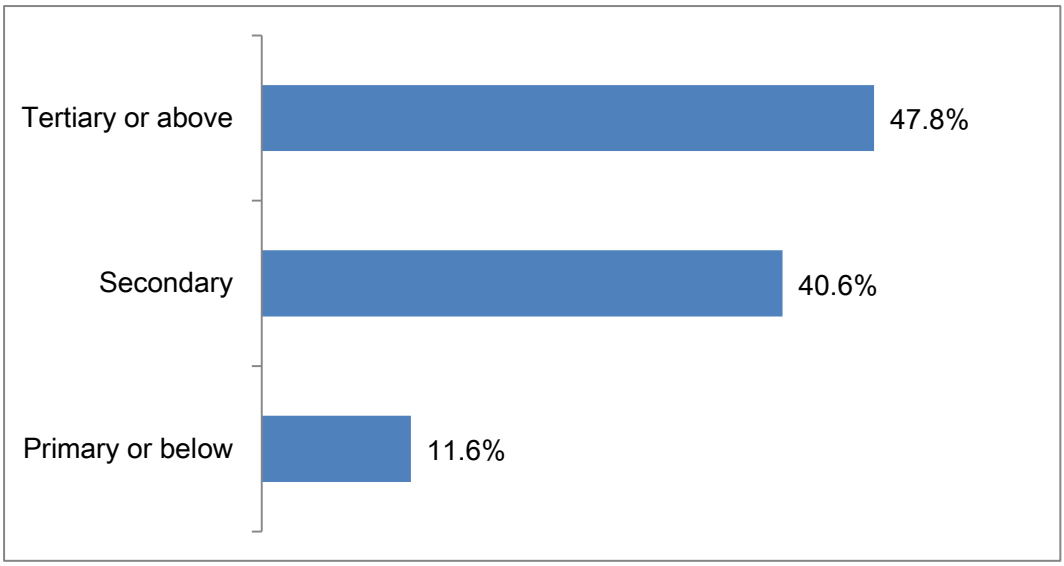
(Base: All respondents = 1,222)

Figure 3.2.1.2 Age of respondents



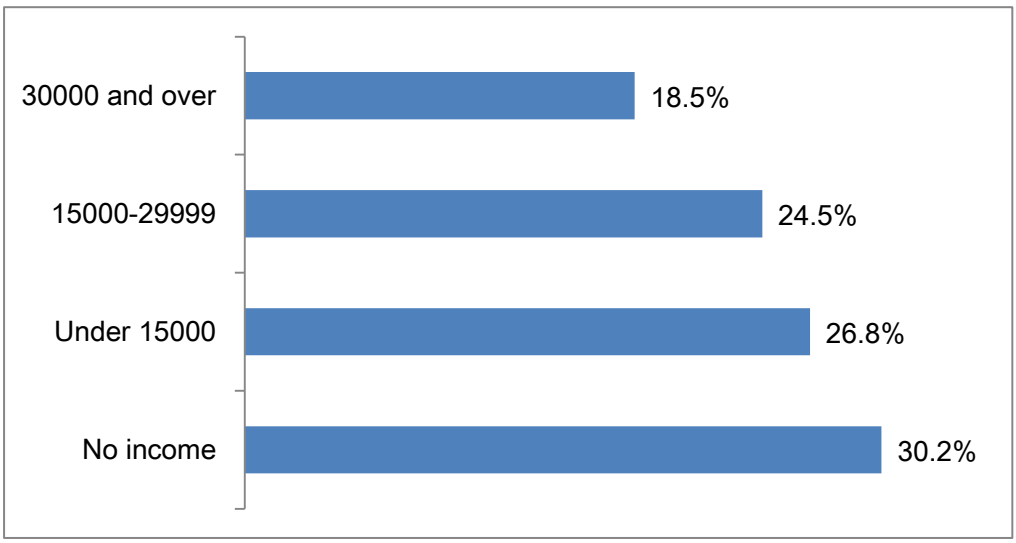
(Base: All respondents excluding "Don't know" and "Refuse to answer" = 1,141)

Figure 3.2.1.3 Education level of respondents



(Base: All respondents excluding "Refuse to answer" = 1,212)

Figure 3.2.1.4 Monthly personal income of respondents



(Base: All respondents excluding "Don't know" and "Refuse to answer" = 1,124)

3.2.2 Privacy attitudes about the collection and use of ID card details, numbers and copies

Figure 3.2.2.1 summarises responses to a series of questions about privacy attitudes about the collection and use of ID card details, numbers and copies in different situations. In each situation, respondents were asked how much they mind, on a scale from 0-10 where 0 means they do not mind at all and 10 means they would mind enough to make a complaint.

The situations presented were:

a) Their ID card details are noted down by a police officer when he stops them in the street
b) Their name and ID card number are noted down by a security guard in order to let them into a residential building as a visitor
c) Providing their ID card number to postman when collecting parcels
d) Providing their ID card number on a job application form
e) Providing their ID card copy when attending a job interview, after shortlisting, but before receiving a job offer
f) Providing their ID card number when enrolling for fitness club membership
g) Providing a copy of their ID card when enrolling for fitness club membership

As can be seen from the figure, providing ID card number to a postman or on a job application form or a police officer noting down the ID card details, which are all arguably legitimate and justified, raised the least concern, with about 30% of respondents stating that they did not mind at all and less than 10% of respondents minding enough to make a complaint.

For name & ID card number noted down by a security guard and providing an ID card copy before receiving a job offer, only about 12-15% of respondents did not mind at all and about 17% minded enough to make a complaint.

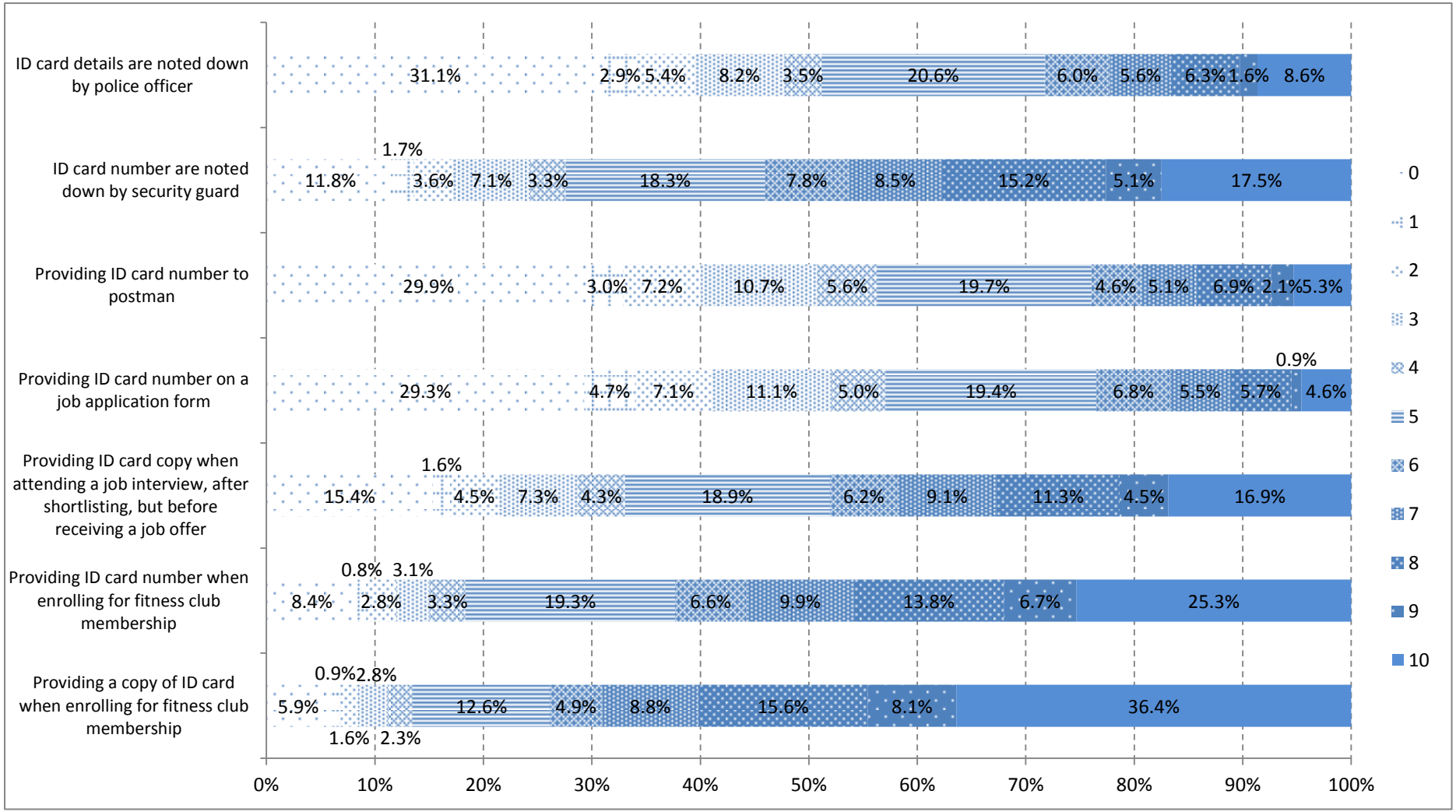
For providing ID card number when enrolling for fitness club membership, only 8% of respondents did not mind at all, while 25% minded enough to make a complaint.

Lastly, for providing a copy of ID card when enrolling for fitness club membership, which is clearly unjustified, only 6% did not mind at all, while 36% minded enough to make a complaint.

In summary, around 30% of respondents did not mind legitimate, justified use of ID card information at all, while nearly 40% did mind clearly unjustified use of ID card information.

There were some demographic differences in answers to these questions, with males, older and less educated respondents less concerned about the privacy implications of most situations.

Figure 3.2.2.1 Privacy attitudes about the collection and use of ID card details, numbers and copies



Base: All respondents excluding “No idea” and “Refuse to answer”

ID card details are noted down by police officer = 1210

ID card number are noted down by security guard = 1221

Providing ID card number to postman = 1210

Providing ID card number on a job application form = 1210

Providing ID card copy when attending a job interview, after shortlisting, but before receiving a job offer =1191

Providing ID card number when enrolling for fitness club membership = 1195

Providing a copy of ID card when enrolling for fitness club membership = 1184

3.2.3 Privacy attitudes to providing personal data

Figure 3.2.3 summarises responses to a series of questions about providing personal data in order to obtain a discount. In each situation, respondents were asked how much they mind, on a scale from 0-10 where 0 means they do not mind at all and 10 means they would mind enough to make a complaint.

The situations presented were providing:

a) Full residential address
b) Mobile phone number
c) ID card number
d) Personal income
e) Occupation
f) Date, month and year of birth

As can be seen from the figure, there was little concern about providing mobile phone number, occupation or full date of birth, with about 15-17% expressing no concern at all, while about 15-23% were concerned enough to make a complaint.

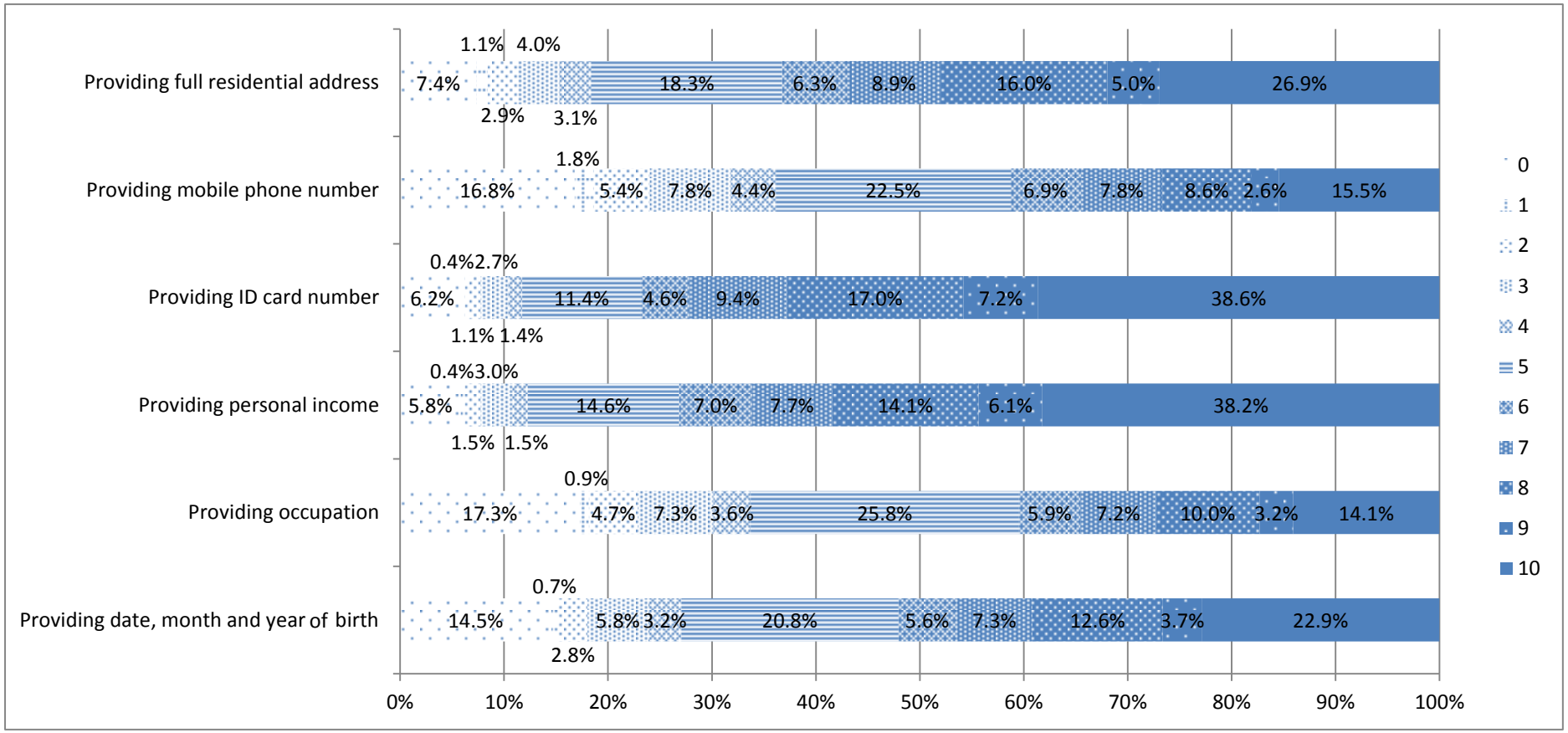
For providing full residential address, 7% expressed no concern at all, while 27% were concerned enough to make a complaint.

Lastly, for ID card number and personal income, only about 6% had no concern, while about 38% were concerned enough to make a complaint, suggesting that these were seen as sensitive personal data.

In summary, few respondents were very concerned about providing mobile phone number (even though it allows receiving advertising calls) occupation or full date of birth (even though it is often used for validation), but many expressed valid concern about providing personal income and ID card number.

There were some demographic differences in answers to these questions, with older, less educated respondents and those with higher personal income generally less concerned about providing their personal data in return for a discount.

Figure 3.2.3 Privacy attitudes to providing personal data



Base: All respondents (excluding “No idea” and “Refuse to answer”)

Providing full residential address = 1,218

Providing mobile phone number = 1,195

Providing ID card number = 1,217

Providing personal income = 1,205

Providing occupation = 1,207

Providing date, month and year or birth = 1,218

3.2.4 Privacy for public registries, CCTV & loyalty cards

Figure 3.2.4 summarises responses to a series of questions about privacy attitudes towards invasion of privacy due to collection and use of personal data by public registries, CCTV and loyalty cards. In each situation, respondents were asked how much they mind, on a scale from 0-10 where 0 means they do not mind at all and 10 means they would mind enough to make a complaint.

The situations presented were:

a) Marriage registry shows occupation of the marrying parties for 3 months publicly
b) Lands registry shows registered owners to anyone
c) Companies registry shows ID card number of directors to anyone
d) Companies registry shows residential address of directors to anyone
e) CCTV showing your doorway
f) Friends provide their name/address to apply for loyalty card without prior agreement
g) They provide their friends'/relatives' name/address to apply for loyalty card without their prior agreement

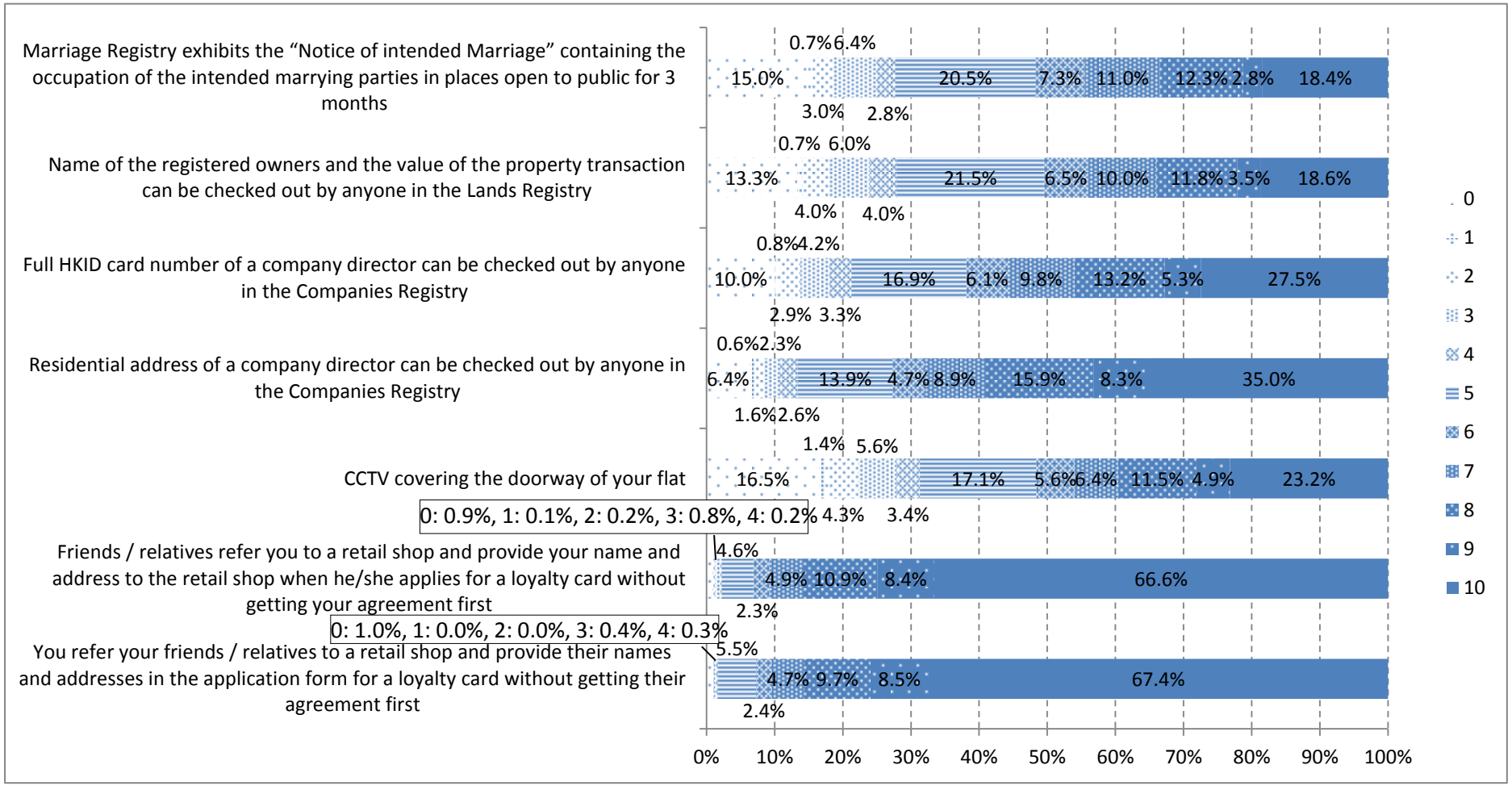
For the registries, 13-15% of respondents had no concern and 18% had serious concern for the marriage and lands registry. For the ID card number and residential address of a company director, 6-10% had no concern, and 28-35% had serious concern, again supporting that this information is seen as sensitive.

For CCTV covering their doorway, 16% had no concern, while 23% had serious concern.

For providing names and addresses of friends/relatives when applying for a loyalty card, 67% had serious concern and only 1-2% had no concern regardless of whether it was themselves or their friends/relatives doing the application, suggesting that this is widely seen as invasion of privacy.

There were some demographic differences for these questions, with male, less educated and older respondents and those with higher personal income less concerned generally about privacy invasion.

Figure 3.2.4 Privacy for public registries, CCTV & loyalty cards



Base: All respondents (excluding “No idea” and “Refuse to answer”)

Marriage Registry exhibits the “Notice of intended Marriage” containing the occupation of the intended marrying parties in places open to public for 3 months = 1,171

Name of the registered owners and the value of the property transaction can be checked out by anyone in the Lands Registry = 1,200

Full HKID card number of a company director can be checked out by anyone in the Companies Registry = 1,198

Residential address of a company director can be checked out by anyone in the Companies Registry = 1,184

CCTV covering the doorway of your flat = 1,214

Friends / relatives refer you to a retail shop and provide your name and address to the retail shop when he/she applies for a loyalty card without getting your agreement first = 1,221

You refer your friends / relatives to a retail shop and provide their names and addresses in the application form for a loyalty card without getting their agreement first = 1206

,

3.2.5 Misuse of personal data

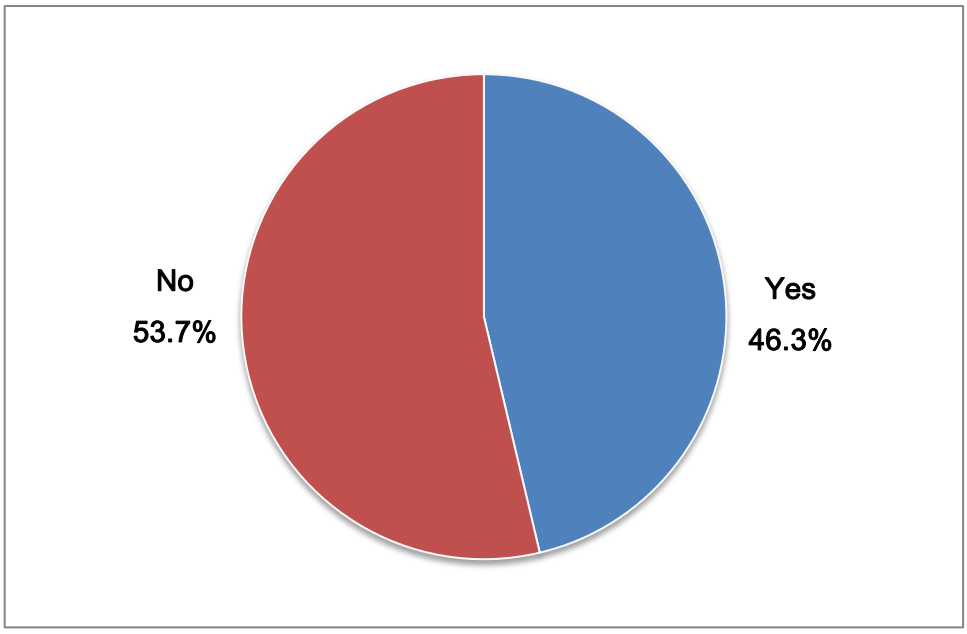
Figure 3.2.5.1 shows that nearly half (46%) of respondents had experienced misuse of their personal data in the last 12 months. As shown in Figure 3.2.5.2, the most common source of the problem was transactions with banks (57%), followed by telecom companies (32%), fitness/beauty centres (26%) and money lenders (17%), whereas in 2001 the most frequent sources were banks, real estate agents and telecom companies.

Respondents aged 30-39, with higher education and higher personal income were more likely to report that they had personal experience of misuse of their personal data.

As seen in Figure 3.2.5.3, 11% of those who experienced misuse had made a complaint, while of those who had not complained, the major reasons (Figure 3.2.5.4) were that friends had provided the personal data that had been misused (35%), (even though, as seen in 3.2.4, many respondents did not think friends should provide personal data for loyalty cards) or they were unwilling to involve the staff of the company responsible (25%).

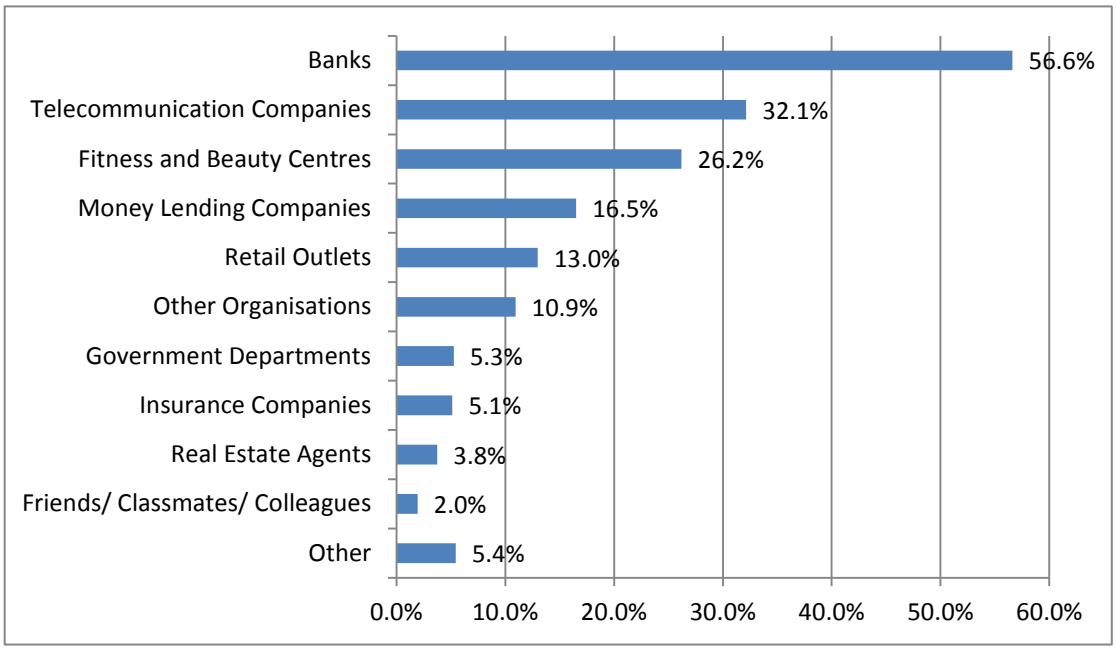
Among respondents who had experienced misuse, those with higher education were much more likely to have made a complaint than those with less education.

Figure 3.2.5.1 Misuse of personal data in the last 12 months



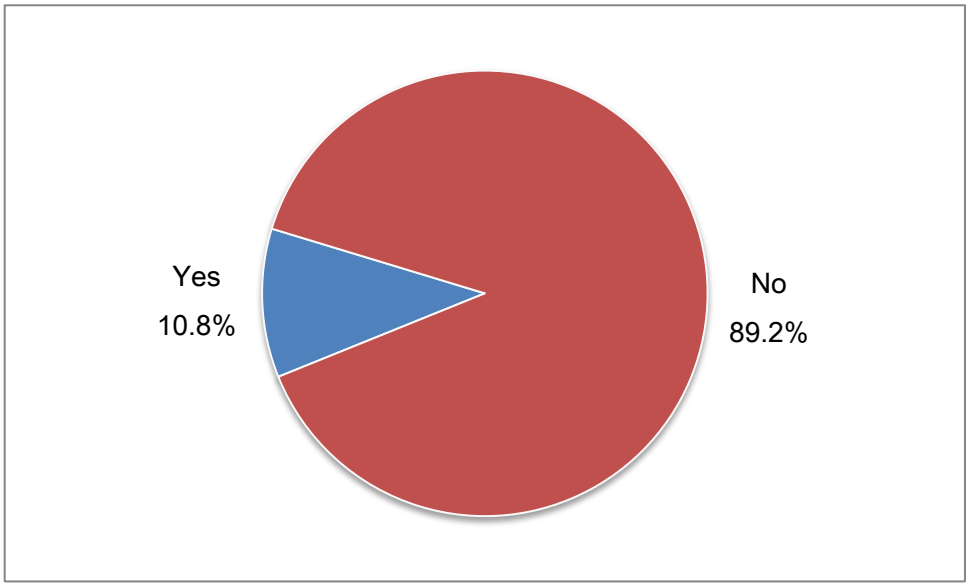
(Base: All respondents excluding "Don't know" and "Refuse to answer" = 1,190)

Figure 3.2.5.2 Organisation responsible for the misuse of personal data



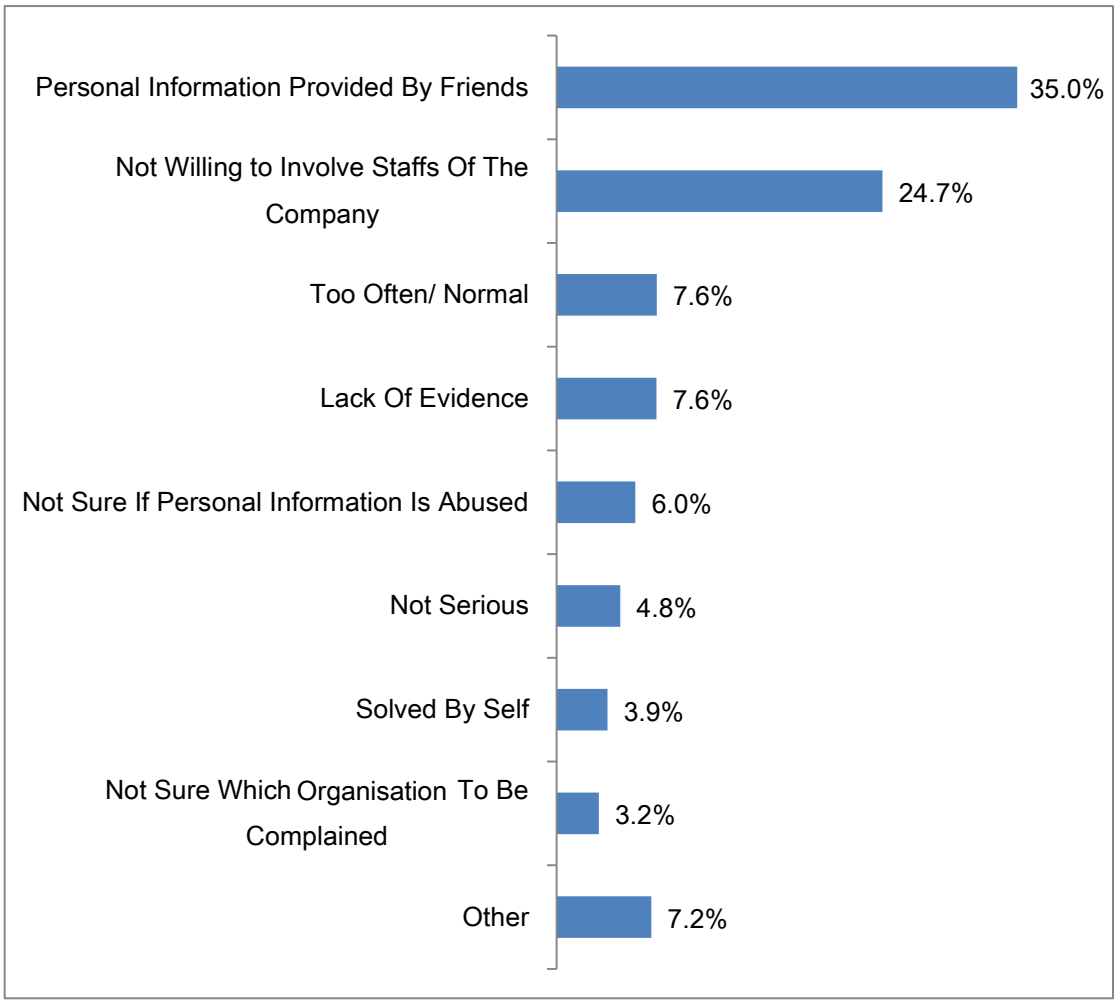
(Base: The respondents who personally experienced misuse of personal data excluding "Don't know" and "Refuse to answer" = 451)

Figure 3.2.5.3 Make a complaint about personal data being misused



(Base: The respondents who personally experienced misuse of personal data excluding "Don't know" and "Refuse to answer" = 551)

Figure 3.2.5.4 Reason for not lodging a complaint



(Base: The respondents who personally experienced misuse of personal data excluding "Don't know" and "Refuse to answer" = 484)

3.2.6 Awareness of the work of the PCPD

As shown in Figure 3.2.6.1, the majority of respondents (63%) were aware of the PCPD through mass media, with smaller proportions aware through the website/multimedia (19%), PCPD publications (15%) and the PCPD publicity programmes (7%), whereas in 2001 the major channels were mass media, publicity programmes and guidance materials.

There were demographic differences in awareness of the PCPD through different channels, with males, those aged 50-59, higher education and higher personal income more aware through mass media. Females and those aged 30-39 were more aware through PCPD publications, while those with higher personal income were more aware through the PCPD website and females were more aware through PCPD publicity programmes.

Figure 3.2.6.2 shows that an overwhelming majority of respondents (86%) of respondents agreed or strongly agreed that PCPD has increased community awareness of personal data privacy issues after the Octopus Incident in 2010, with only 14% disagreeing/strongly disagreeing.

Respondents with higher education and higher personal income were more likely to agree that PCPD had increased community awareness.

Figure 3.2.6.1 Awareness of the work of the PCPD

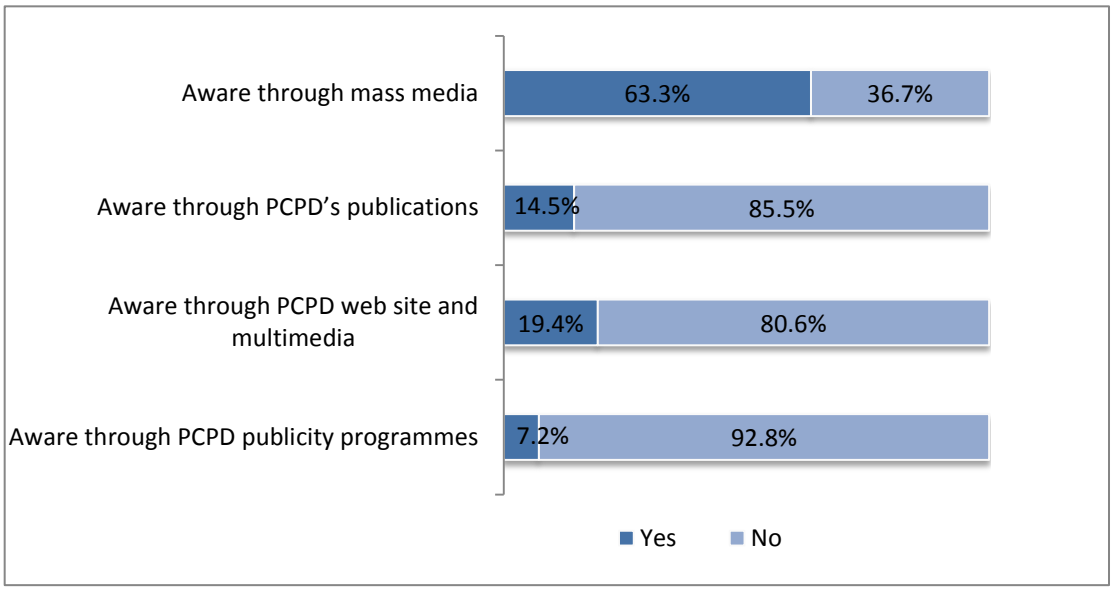
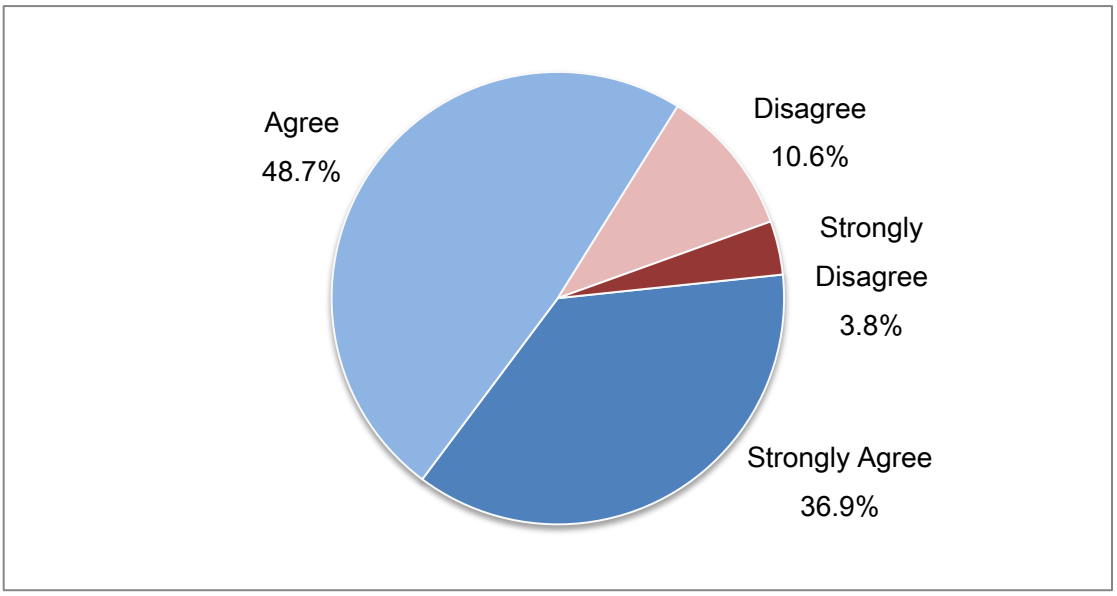


Figure 3.2.6.2 PCPD has increased community awareness of personal data privacy issues after the Octopus Incident in 2010



(Base: All respondents excluding "Don't know" and "Refuse to answer" = 1,148)

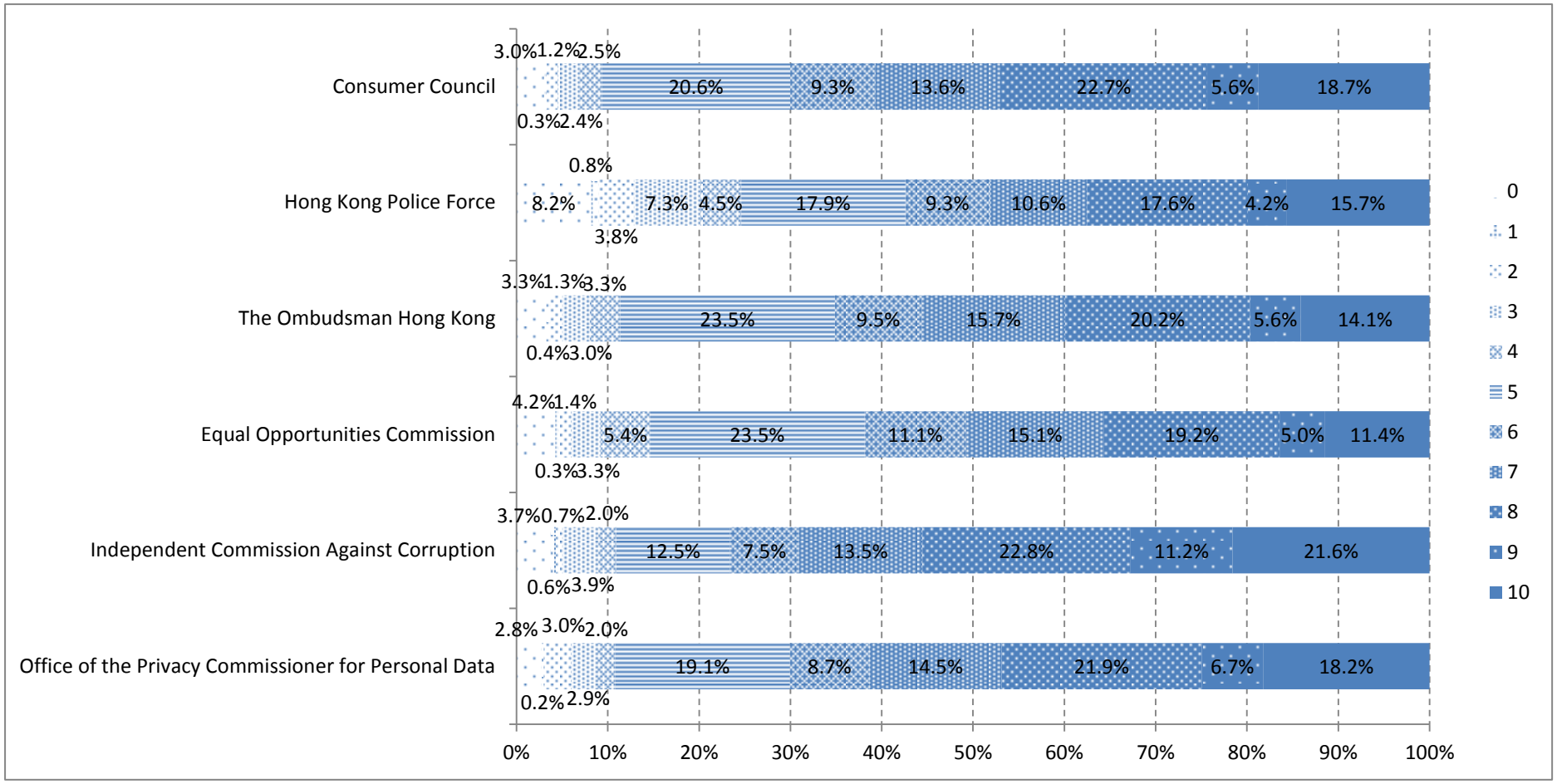
3.2.7 Trustworthiness in handling complaints

Figure 3.2.7 shows a comparison of the perceived trustworthiness of different statutory agencies handling complaints using a scale from 0 (no trust) to 10 (complete trust). Independent Complaints Against Corruption (ICAC) is clearly the most trusted agency with 33% rating it as 9 or 10, while PCPD (25%) edged out the Consumer Council (CC)(24%), while the HK Police Force (HKPF) and Ombudsman tied at 20%, with the Equal Opportunities Commission (EOC) still having 16% rating as 9 or 10. From the opposite perspective, ICAC had the smallest percentage rating it as 5 or less (24%), with PCPD and CC tied at 20%, followed by the Ombudsman (35%), EOC (38%) and HKPF (43%). [4]

Respondents with lower education had lower trust in the PCPD handling of complaints.

[4] Note: the survey was conducted after Occupy Central, which may explain the lower ratings for HKPF

Figure 3.2.7 Comparison of Trustworthiness when handling complaints



Base: All respondents (excluding “Difficult to say”, “No idea” and “Refuse to answer”)

Consumer Council = 1177

Hong Kong Police Force = 1197

The Ombudsman Hong Kong = 1080

Equal Opportunities Commission = 1127

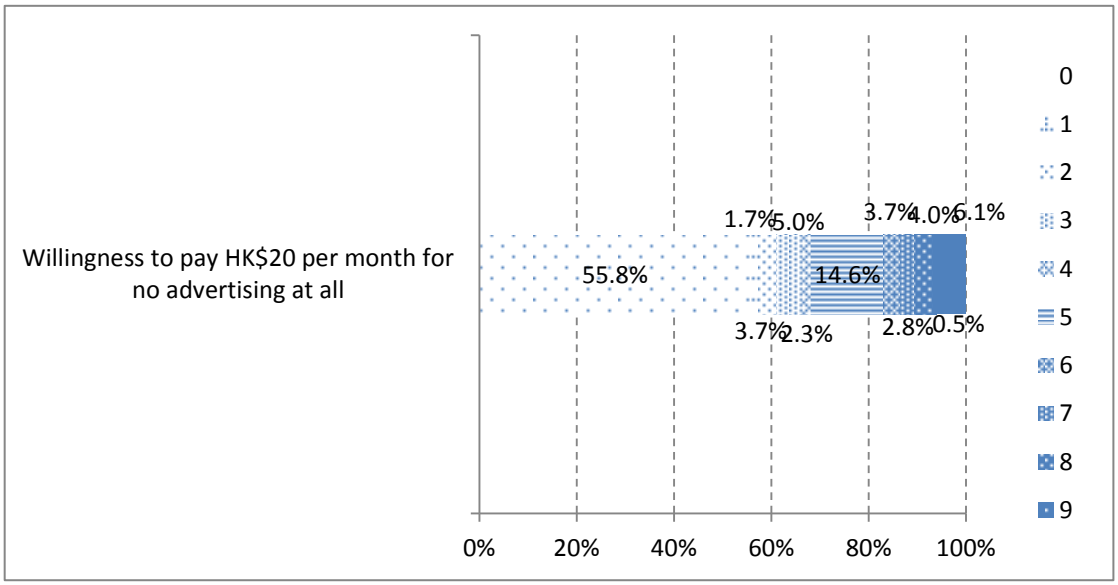
Independent Commission Against Corruption = 1184

Office of the Privacy Commissioner for Personal Data = 1131

3.2.8 Privacy Attitudes For Online Activities

Figure 3.2.8.1 shows the majority of respondents (56%) would certainly not be prepared to pay $20 per month for email services like Gmail with the promise of no advertising at all, while only 6% would be certainly willing, suggesting that most people are reluctant to pay for privacy protection.

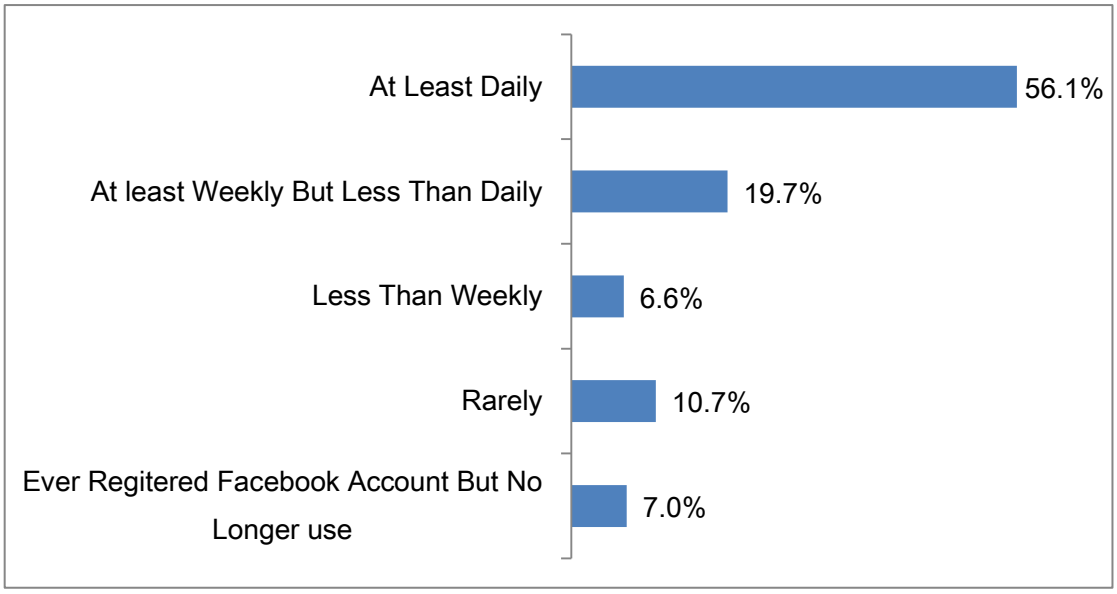
Figure 3.2.8.1 Willingness to pay HK$20 per month for no advertising at all



Base: All respondents (excluding “Difficult to say”, “No idea” and “Refuse to answer”) = 112

Figure 3.2.8.2 shows that the majority of respondents (56%) who have ever had a Facebook account use Facebook at least daily with only 18% rarely or never using their account. Younger and better educated respondents were much more likely to be daily users.

Figure 3.2.8.2 Frequency of use Facebook

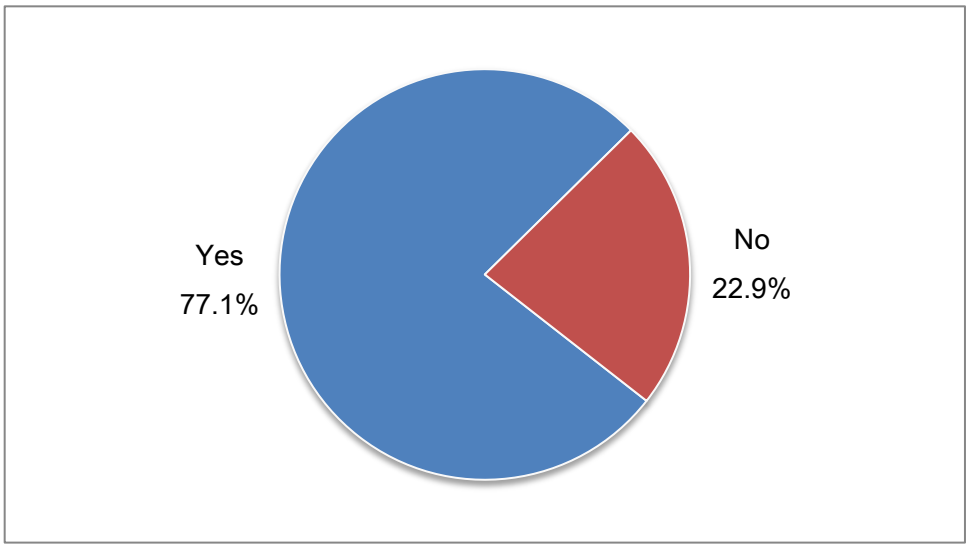


(Base: All respondents excluding "No Facebook account" = 885)

Figure 3.2.8.3 shows that a strong majority (77%) of Facebook account users are aware of the privacy setting, of whom a strong majority (73%) have ever checked the settings, of whom nearly all (90%) have changed the settings.

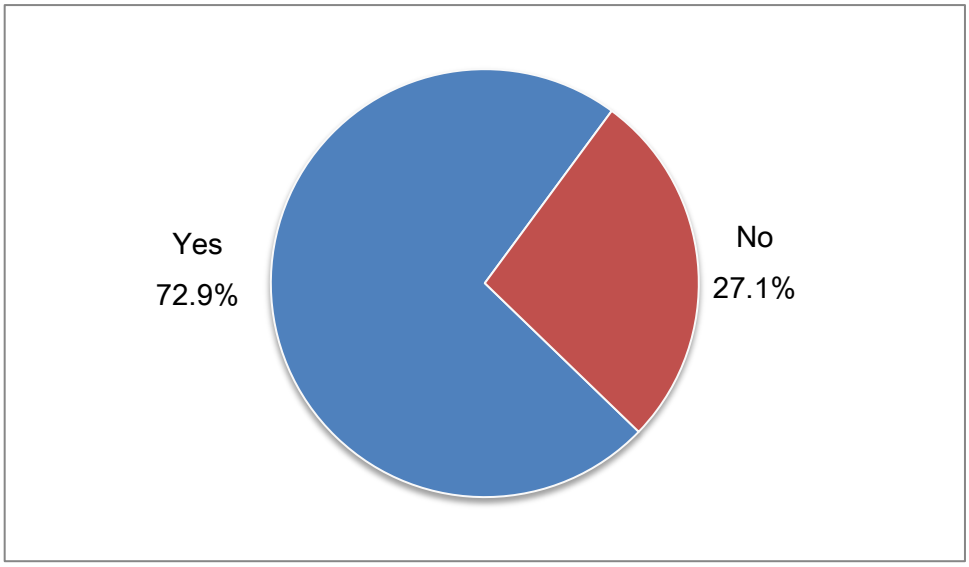
Younger and better educated respondents were much more likely to be aware of, to have checked and to have changed the privacy settings in Facebook.

Figure 3.2.8.3 Awareness of privacy setting in Facebook



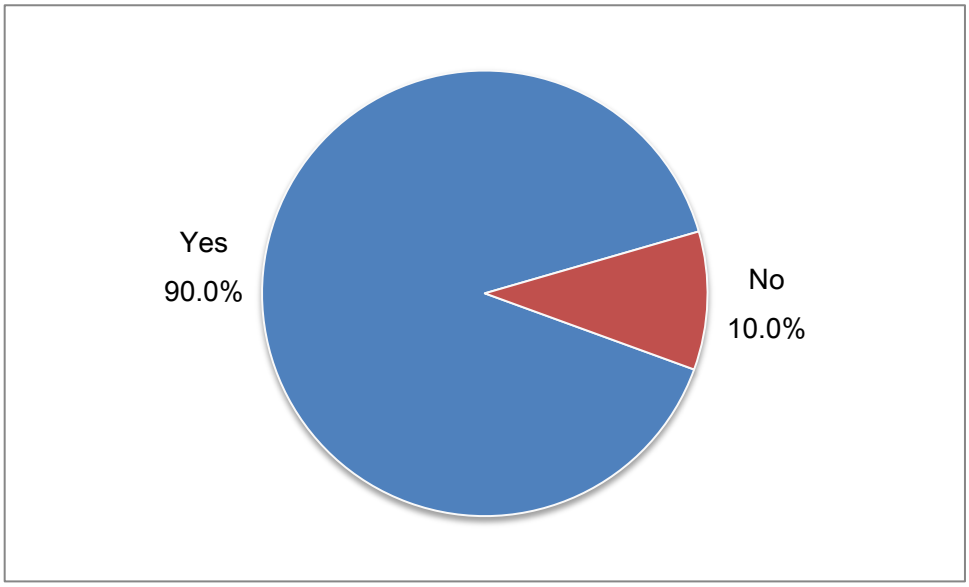
(Base: All respondents have Facebook account = 885)

Figure 3.2.8.4 Ever checked the privacy setting in Facebook



(Base: All respondents have Facebook account and aware privacy setting in Facebook= 684)

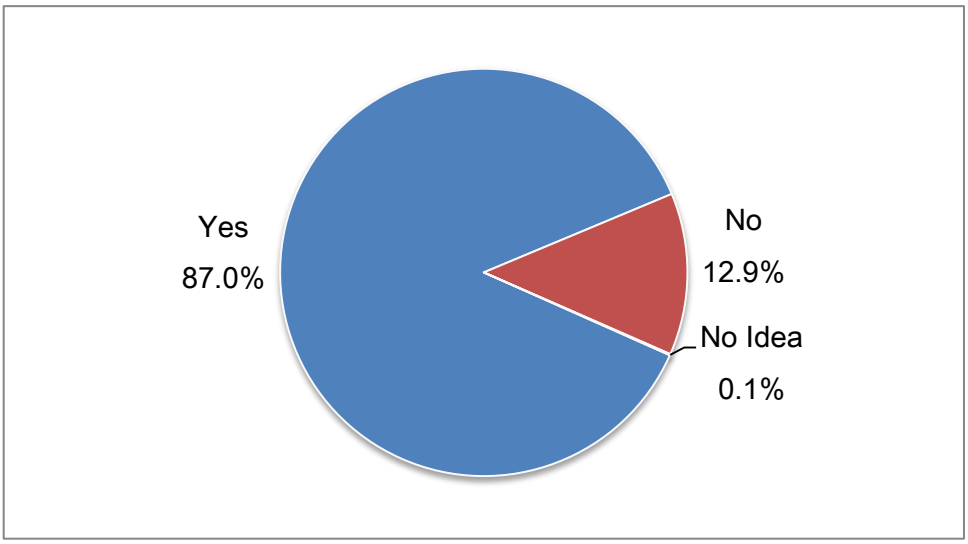
Figure 3.2.8.5 Ever changed the privacy setting in Facebook



(Base: All respondents have Facebook account and checked setting in Facebook= 496)

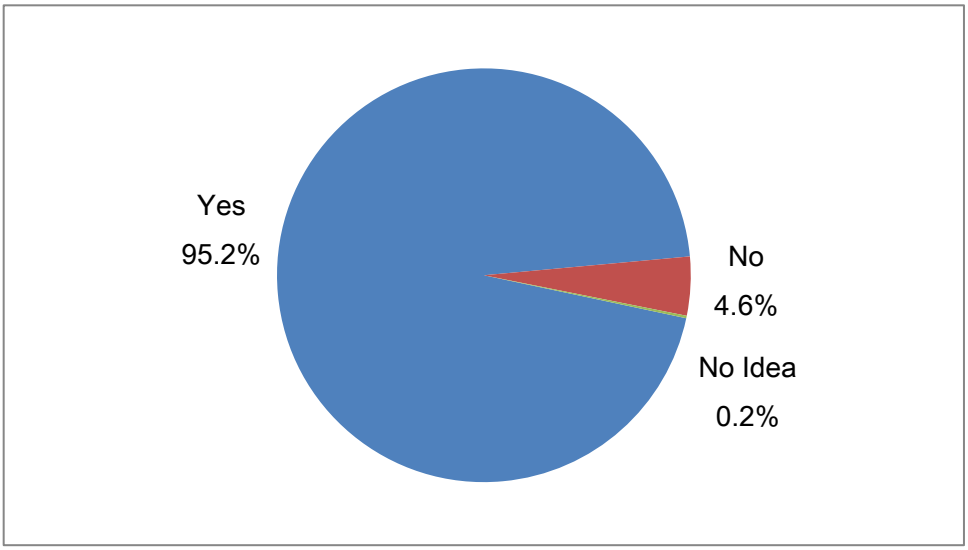
Figure 3.2.8.6 shows that an overwhelming majority (87%) of respondents use a smartphone of whom 95% have WeChat or a similar app installed, of whom 81% installed it themselves, suggesting that a substantial proportion of respondents have had help installing these apps. Respondents aged 60+ and with primary or less education were much less likely to use a smartphone and to have WeChat or a similar app installed, or to have installed WeChat themselves.

Figure 3.2.8.6 Use a smartphone at all



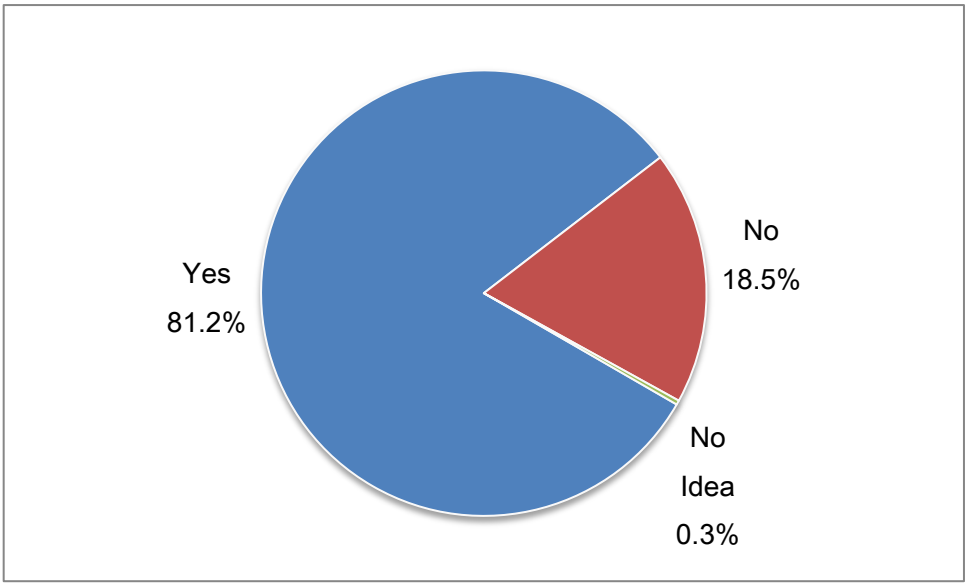
(Base: All respondents = 1,222)

Figure 3.2.8.7 Installed WeChat/ Line/ Viber/ Whatsapp on a smartphone



(Base: All respondents who use a smartphone = 1,064)

Figure 3.2.8.8 Install WeChat/ Line/ Viber/ Whatsapp themselves

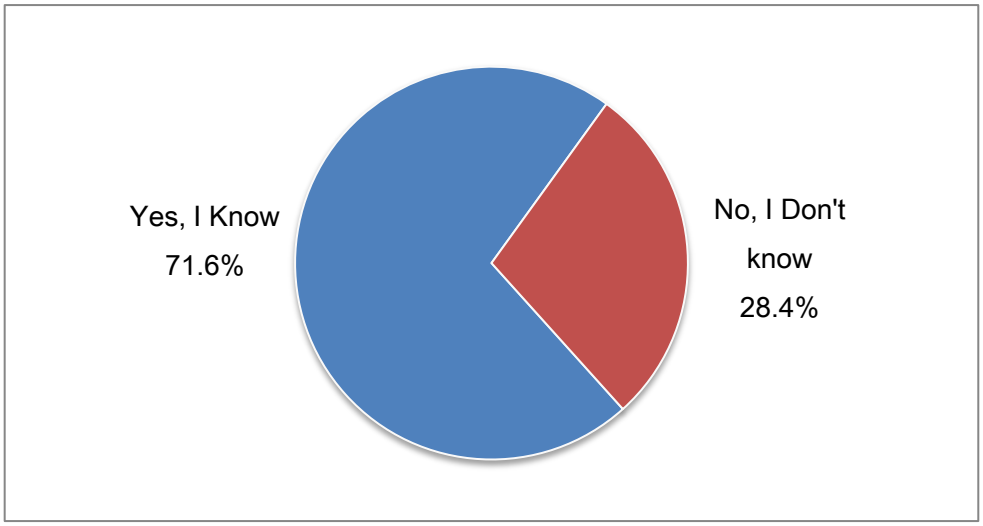


(Base: All respondents who Installed WeChat/ Line/ Viber/ Whatsapp on a smartphone = 1013)

Figure 3.2.8.9. shows that only 72% of respondents with WeChat or a similar app installed were aware that it accesses all of the contacts on their smartphone, while Figure 3.2.8.10 shows that a significant proportion (33%) thought the law should prohibit this (rated this as 10 in terms of privacy problem)

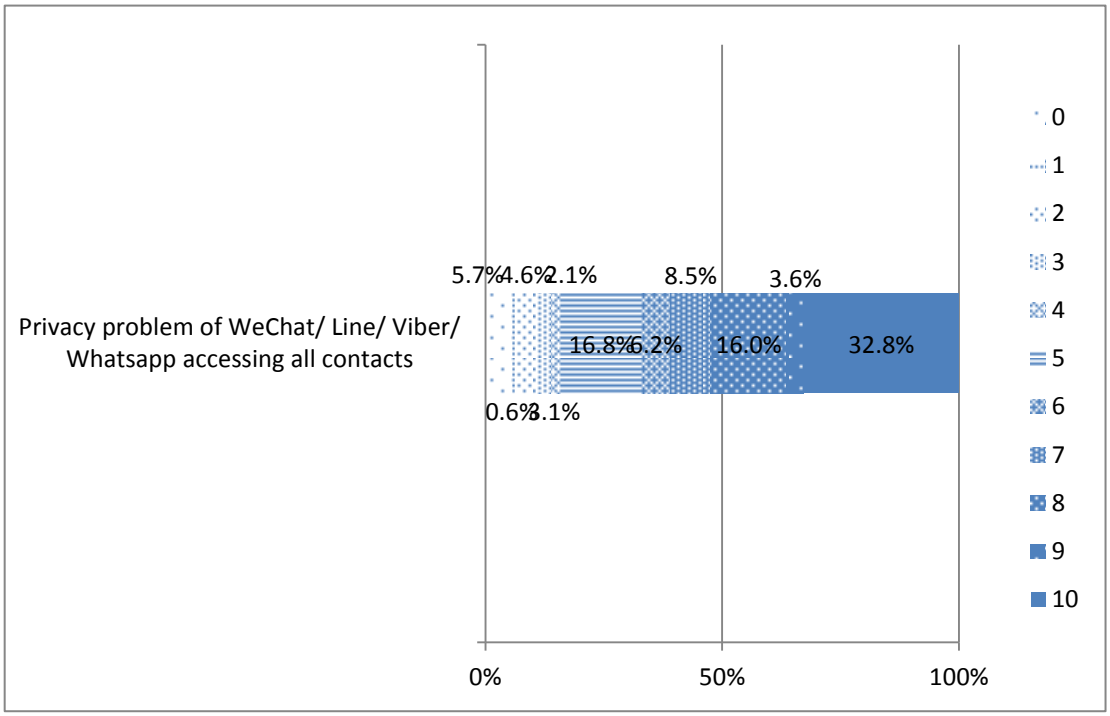
Females, older people and those with lower education were less likely to be aware that these apps access all their contacts, while younger respondents were much less likely to believe this should be prohibited.

Figure 3.2.8.9 Awareness of WeChat/ Line/ Viber/ Whatsapp access all of contacts on the phone



(Base: All respondents who Installed WeChat/ Line/ Viber/ Whatsapp on a smartphone = 1,013)

Figure 3.2.8.10 Privacy problem of all contacts being accessed



(Base: All respondents who Installed WeChat/ Line/ Viber/ Whatsapp on a smartphone excluding "No idea/ Don't know" and "Refuse to answer" = 1,002)

Chapter 4 Focus Group Interviews

A total of 4 focus group interviews were conducted with the 36 participants with a composition designed to reflect different opinions of the general public:

1. People aged between 18 and 40 (males and females);
2. People aged 41 and above (males and females);
3. People with lower education level i.e. secondary education or below (males and females); and
4. People with higher education level i.e. post-secondary education or below (males and females).

There were at least 8 participants in each focus group. Table 1.1 shows the details of the 4 focus group interviews.

Table 4.1 Schedules for the Focus Groups

Category	**Date**	**Time**	**No. of participant**
Group with people aged 41 and above (males and females)	6th November 2014	7:15 p.m.	9
Group with people aged between 18 and 40 (males and females)	10th November 2014	7:10 p.m.	9
Group with people with lower education level i.e. secondary education or below (males and females)	11th November 2014	7:10 p.m.	10
Group with people with higher education level i.e. post-secondary education or below (males and females)	13th November 2014	7:10 p.m.	8

4.1 Findings from the Focus Group Interviews

4.1.1 Demographic Information of Participants

In the discussion group with people aged between 18 and 40, there were 9 participants including 5 females and 4 males. 6 of them aged under 30 and the rest aged between 30 and 39. Half of them were degree holders.

In the discussion group with people aged 41 and above, there were 9 participants including 5 females and 4 males. 2 of them aged between 41 and 49, and the rest aged between 50 and 60. They had different educational level, including degree, tertiary, secondary and primary education.

In the discussion group with people with lower education level, there were 10 participants including 5 females and 5 males. 5 of them aged between 21 and 28, and the rest aged between 49 and 57. Two of them had primary education and the rest had secondary education.

In the discussion group with people with higher education level, there were 8 participants including 3 females and 5 males. One participant aged under 29 and the rest aged between 40 and 54. All of them were degree holders.

4.1.2 Enforcement powers of PCPD

At the beginning of each focus group discussion, a brief introduction of PCPD and the PD(P)O were given to all participants.

4.1.2.1 Awareness of PCPD's media briefing

When asked about awareness of PCPD media releases, some of them could recall a TV advertisement about the use of personal data for the direct selling was regulated or protected by the PD(P)O, the incident where California Fitness asked members to provide their ID copies, the incidents of ParkNShop requesting customers to provide full ID number for applying ParkNShop MoneyBack and Octopus selling personal data of its customers to a third party without customers' authority.

There were more participants with higher education level (all participants) who could

recall the PCPD media release when unprompted than those participants with lower education level (three participants).

4.1.2.2 PCPD's publishing reports that name the organisation at fault

Overall, most of the participants in the discussion groups agreed that publishing reports that name the organisation at fault was effective because it highlighted those organisations that violated the PD(P)O and raised concerns about the importance of protecting personal data information such as the public should be fully aware that their personal data was used for what purpose, their personal data was used by whom and whether they are being asked to provide excessive personal data. Those participants who held the opposite opinion, did so because there was no clear guidelines on what level of personal data to collect for commercial purpose. Therefore, it was difficult to judge whether the companies had violated the PD(P)O or the companies would not flagrantly violate the law to ask for their personal data, but the companies would use other indirect ways to obtain their personal data other than ID number.

4.1.2.3 Awareness and expectations of the role of the PCPD

After a brief introduction of the incident of California Fitness as an example, participants were asked about their awareness and expectations of the role of the PCPD. In general, a lot of the participants did not understand that PCPD is an independent statutory body set up to oversee the enforcement of the PD(P)O.

Participants in the discussion groups suggested the following roles for PCPD:

- PCPD should work with the government agencies responsible for issuing licences, such as adding rules or guidelines on obtaining their customer's personal information when an organisation applies for a licence
- PCPD should cooperate with the police or other relevant departments in the enforcement of the PD(P)O.
- PCPD should establish a code on handling personal data for companies to follow
- PCPD should establish a code on rights to protect personal data for the public
- PCPD should establish a department to prosecute the company in violation of the PD(P)O, rather than passing those cases to the police or the judiciary, so that PCPD could perform its data protection role better.
- PCPD should educate the public and the companies about collecting necessary,

not excessive personal data collection.
- PCPD should state the duration of storing the personal data by different types of companies.
- PCPD should establish a penalty system for those companies that violated the PD(P)O.
- PCPD should take follow-up action when the media was aware of the illegal use of personal privacy incidents
- PCPD should remind those companies that violated the PD(P)O to destroy permanently the ID card copies immediately

Some participants said that it was acceptable for organisations using their photos on their membership cards for identification, as long as they could allow members to opt-out the use of their personal data for any other commercial purposes.

4.1.2.4 Awareness of the consequences of non-compliance with the PD(P)O and what they expect the PCPD to do

When asked about the awareness of the consequences of non-compliance with the PD(P)O, only two participants said that the consequence of violating the PD(P)O would be prosecution or it would be a civil legal suit. The rest did not know the consequences of violating the PD(P)O.

Participants suggested the following follow-up actions:
- the companies that violated the PD(P)O should close for a period of time as punishment.
- the companies that violated the PD(P)O should be a criminal case and the prosecution of these behavior would lead to a fine or imprisonment
- PCPD should establish a penalty mechanism stating different stages of penalty
- PCPD should establish a dedicated reporting mechanism for the users of those companies that have violated the PD(P)O
- PCPD should establish a routine notification mechanism notifying the public if organisations were in violation of the PD(P)O
- PCPD should make sure that those companies that violated the PD(P)O would destroy the respective data.
- PCPD should establish an online blacklist of those companies which have violated the PD(P)O to help strengthening public awareness.
- A comprehensive punishment mechanism should be established and increasing punishment might be a greater deterrent.

- PCPD could offer courses and certificates related to the PD(P)O and staffs of those companies who handle personal data had to obtain the certificates.
- If the companies were found in violation of the PD(P)O, the staff would bear legal responsibility.

4.1.2.5 Whether the current regulatory framework is sufficient to protect the public

When asked about the sufficiency of the current regulatory framework to protect the public, many participants could not comment because they were not familiar with the work of PCPD and the regulatory framework. A few participants thought that the current regulatory framework was sufficient to protect the public but the current regulatory framework contained a lot of legal jargon and it was hard for the general public to understand. Among those participants who thought the current regulatory framework was sufficient to protect the public, they mentioned the following comments:

- sometimes the company would add terms to his contract and he had no choice except to agree to all the terms for using the service.
- the mobile apps sent his personal data to a third party since there were always some clause requiring his consent to use his personal data before he downloaded those mobile applications
- the current regulatory framework did not cover the multinationals, hence insufficient.

Some participants were concerned about the current situation that people were forced to provide personal data, a lot of the personal data could be found openly, and the limited monitoring and enforcement powers of the PCPD.

4.1.3 Direct marketing and the PD(P)O amendment

4.1.3.1 Awareness that organisations are required to provide data subjects with notification

There were more participants aged 41 and above (all participants) who were aware that direct marketing companies had to notify potential customers and get their consent, before approaching them than those participants aged between 18 and 40 (only three participants).

There were more participants with higher education level (over half of the participants) who were aware that direct marketing companies had to notify potential customers and get their consent, before approaching them than those participants with lower education level (only one participant).

4.1.3.2 How people respond to direct marketers' notifications

Among those participants who had received notifications from direct marketing companies in the discussion groups, (i) three out of five participants in the discussion group with people with lower education level would request opt-out (ii) two out of three participants in the discussion group with people aged between 18 and 40 would choose to opt-out from the use of their personal data if the process was easy and convenient or gave an option to be excluded and (iii) all eight participants in the discussion group with people with higher education level would only consent if there was a checked box on the paper notification form or letter. Another participant in the discussion group with people aged between 18 and 40 expressed that making use of personal data for direct marketing was fine as long as options were offered and he was notified. Further, two participants in the discussion group with people with higher education level said that they received notifications about the usage of their personal data for business purpose but the notifications did not mention the phrase "for direct marketing use".

4.1.3.3 Whether people know that organisations can only promote products / services that he/ she previously consented to

Only a few participants in the discussion groups knew that direct marketing calls could only cover the type of products that they agreed to when they approved using their personal data for direct marketing, not all types of products and service.

4.1.3.4 Whether people know that organisations cannot transfer their personal data to a third party (no matter for gain or not) for use in direct marketing unless written consent has been obtained

Overall, a lot of the participants in the discussion groups (four participants in the discussion group with people aged 41 and above and eight participants in the discussion group with people with higher education level), especially all participants

in the discussion group with higher education level, knew that organisations should not transfer their personal data to a third party for the use of direct marketing unless written consent had been obtained.

4.1.3.5 Awareness of their opt-out right

The majority of participants in the discussion groups except only two participants in the discussion group with people aged 41 and above knew that they had the right to opt-out even if they had opted in before. One of them shared her experience with a service provider that she had previously consented to receive its direct marketing calls, and then she repeatedly requested to opt-out of the calls. Unfortunately, the service provider kept on making direct marketing calls to her and different staff handled the calls. The staff pointed out that there was no record of her verbal request to opt-out the calls.

4.1.3.6 How people respond to direct marketers if they do not wish to receive promotional messages

During the discussion, the participants were asked how they respond to direct marketers if they did not wish to receive promotional messages.

The participants in the discussion groups said that they would write a letter or an email to the organisations as a black-and-white record of their request to opt-out of the calls, send verbal opt-out requests to the organisations, use mobile applications to block the direct marketing calls, hang up the phone or angrily tell the caller not to call again. However, some participants said that the companies kept constantly calling them and they knew their actions taken were useless.

4.1.3.7 Whether the PD (P)O amendment enforced in 2013 is sufficient to protect the public

Overall, only a few participants in the discussion groups had heard of the revision of the PD(P)O, but they did not know the details of the PD(P)O.

After a brief introduction of the PD(P)O amendment about the use of personal data in direct marketing which had been in force since 2013, many participants (all

participants in the discussion groups with people with higher education level and aged between 18 and 40, three participants in the discussion group with people aged 41 and above and six participants in the discussion group with people with lower education level) agreed that this amendment was insufficient to protect the public. Their concern was that a company's violation of the PD(P)O was very difficult to prove since most opt-outs were verbal requests over the phone. It was not convenient for the public to record which companies they had placed opt-out requests with unless all direct marketing calls are recorded. The companies that violated the PD(P)O relied on the public not reporting breaches, therefore there should be detailed instructions for handling these requests so that companies could not claim that they have no record of prior opt-out requests just because they did not keep a full record. The companies might not fully follow the amended law and fail to seek approval for direct marketing of all their products. The PD(P)O only regulates the consent for transferring personal data; the public did not know who sold their personal data to the third parties for direct marketing calls. Further, participants raised that the PD(P)O did not mention the details of lodging complaints and it did not include the Facebook-like form of consent. In addition, some participants claimed that the font size of Terms and Condition in the notification and application forms was too small and suggested requiring a check-box for asking consent. One participant said that she felt safer because she was protected by the opt-out right and written consent before transferring her personal data to a third party.

On the other hand, four participants in the discussion group with people aged 41 and above agreed that this amendment was sufficient to protect the public.

4.1.4 Notification of data leakage to data subjects and PCPD

The repeated incidents of the Police loss of notebooks containing sensitive personal data and loss of fixed penalty ticket and leaked Police internal documents containing personal data via Foxy, such as witness statements, were briefly introduced in each focus group discussion.

Overall, all participants agreed that the data subjects and PCPD should be notified immediately as well as the media. The people involved should be informed immediately because their personal data might be illegally used, so that they needed to be cautious. Sometimes it might be difficult to inform the people involved because their contact information was not known, so then PCPD and the media could

publicise the incident to the public and arouse public caution. PCPD could also conduct the investigation and clarify where the responsibility lay. On the other hand, some participants in the discussion group with people with lower education level were concerned that PCPD did not have any enforcement power and they believed the purpose of informing the PCPD was to keep the incident on record or make a media announcement. So it was not urgent to inform PCPD.

4.1.5 Dealing with organisations which "respect for privacy"

An example of Octopus sharing personal data with five business partners without providing adequate notice to consumers and obtaining customers' consent was briefly introduced in each focus group discussion.

4.1.5.1 To what extent would "respect for privacy" be a factor in choosing a service or a product offered by an organisation

Some participants in the discussion groups (nine participants in the discussion group with people with lower education level, three participants in the discussion group with people aged 41 and above and two participants in the discussion group with people aged between 18 and 40) said that a company's respect towards privacy would affect their patronage because they were afraid their personal data might be used illegally to apply for a loan or sold to a third party for use in direct marketing.

Only one participant in the discussion group with people with lower education level said that a company's respect towards privacy did not affect his patronage because a lot of the personal data had already gone into the public domain nowadays.

Many participants in the discussion groups reported that they did not know whether the organisations had respect for privacy protection, although the organisations would not admit that they disrespect privacy. For example, the CEO of the Octopus claimed that they had informed their customers about their use of personal data, but it was later found that, according to the PD(P)O their practice was not appropriate.

4.1.5.2 PCPD issues investigation reports about organisations contravening the PD(P)O

Participants were asked whether PCPD investigation reports about organisations contravening the PD(P)O affected their willingness to deal with those organisations.

In the focus group discussions, most participants reported that their confidence or trust towards these companies had been decreased by these incidents. They would consider if there was another company that provided similar service with better privacy protection. When applying for membership, they paid more attention to providing their personal data. Some of them were concerned that these companies would continue to leak customer's personal data if they had a history so they would be cautious with these companies. However, some participants noted that consumers might have no choice, if only one vendor could provide such services or products i.e. Octopus.

4.1.5.3 Actions people would take when their personal data has been misused

When the participants' personal data had been misused, the participants would take the following actions:

- should take action to report to the Police as it could strengthen the awareness of the people by reporting
- report to the PCPD
- consult PCPD for the solution and how to prevent their personal data being used again
- hang up the phone
- make up some excuses to make them stop to call
- contact the organisation and ask to stop using their personal data information
- complain to the organisation making the direct marketing calls
- change telephone number
- do nothing

In the discussion group with people aged between 18 and 40 some of the participants claimed that if the consequences were serious, then they would report that their personal data had been misused to the Police.

In the discussion group with people with lower education level, the majority of the participants reported that they would do nothing because it was hard to find out who sold the personal data, followed by reporting to the Police and PCPD.

In the focus group discussion with people with higher education level, all of the participants said that they would hang up the phone when receiving direct marketing calls, but that would solve nothing when receiving direct marketing mails

4.1.5.4 Consider using the anonymous Octopus card instead of a personalised card or one registered for Octopus rewards

Regarding the incident of Octopus selling users' personal data to another company, all participants were asked whether they would consider using the anonymous Octopus card instead of a personalised card or one registered for Octopus rewards.

In the discussion group discussions, all participants would not consider using the anonymous Octopus card instead of a personalised card or one registered for Octopus rewards because some of them were using student Octopus Cards and the rest were using the rewards service for the price discount, convenience or connection with other services.

4.1.5.5 Whether excessive collection of ID card copies reported by PCPD affect people's decisions about which fitness company to enrol with

Regarding the incident of California Fitness collecting their members' ID card copies, all participants were asked whether it would affect their decisions about which fitness company to enrol with.

All participants in the discussion group with people aged 41 and above and the three participants in the other discussion groups (only one participant in the discussion group with people aged between 18 and 40 and two participants in the discussion group with people with higher education level) said that the PCPD reporting would affect their decision about which fitness company to enrol with. The rest of participants claimed it would not affect their decision because their decisions depended on the price and service but they would pay more attention to the personal data requested and some of them believed that the reporting of the incident of California Fitness could raise public awareness and the fitness centre would not violate the PD(P)O again.

4.1.6 Public registry

4.1.6.1 Search information about another person via search engine online

In the focus group discussions, most participants had tried to search for personal data of others for personal purpose via an online search engine because of their curiosity, for example search for old friends and celebrities. Some of them also claimed that they searched for personal data of others for work purpose such as searching for candidates. All of them reported that they did not search personal data of others often.

4.1.6.2 People's expectation of their personal data to be found by the others using search engine online

In the focus group discussions, most participants reported that they expected their personal data to be found by others using search engines online. Some participants claimed that they avoided to be found by others by hiding their personal data in privacy settings or not using their real names and photos on their Facebook.

4.1.6.3 People's expectation of their personal data available in the public domain to be used indiscriminately

In the focus group discussions, all participants agreed that abuse of personal data was likely since the information uploaded on the Internet was assumed to be used by others and the information was easy to access and open to everyone.

4.1.6.4 Balance of transparency, public interest, and privacy protection

During the discussion, participants were asked about the balance of transparency, public interest and privacy protection.

Overall, the participants generally ranked the public interest and privacy as more important than transparency. Public interest was important because of the wide range of people involved and people usually searched for information of their friends

or public figures, but it should be under legal constraint. Some of them said that privacy protection was less important than public interest because it affected the minority of the public. Transparency was related to public right to know.

4.1.6.5 Ask peers before posting

In the focus group discussion with people aged between 18 and 40, only one participant reported that he sometimes asked for his friends' permission before uploading the photo on social media and the rest did not ask their friends' consent because they were close friends and they knew their friends would not be concerned about the posting. One of them said that uploading photos on the social media was a common practice of their generation.

About half of the participants in the discussion group with people with higher education level and those with lower education level reported that they asked peers before posting something about them on the Internet. In addition, one participant said that she wanted her friends to ask her before posting.

The participants in the focus group discussion with people aged 41 and above said that they did not post the information or photos of their friends on the social media because they were aware of the privacy issues and the information uploaded on the Internet was searchable.

4.1.7 Privacy tradeoffs

4.1.7.1 The levels of confidence of people have to protect themselves against online shops and physical shops

The vast majority of the participants in the discussion groups had experience of purchasing products with both online and physical shops. They generally had higher confidence when providing their personal data to a physical shop because they could actually visit and follow up their purchase while it was difficult to find out whether the online shop was real. However, some of them said that their confidence depended on the scale or reputation of the merchant rather than whether it was a physical or online shop. They had never found any problems that the online shops misused their personal data so far and they felt confident using the online store

transactions.

4.1.7.2 Willing to compromise personal data protection in exchange for efficiency and convenience online

All participants in the focus group discussion with people aged 41 and above claimed that they were not willing to provide their or others personal data for higher efficiency and convenience online. Conversely, the participants with people with higher education level would generally provide their and other personal data information (i.e. email address) in exchange for efficiency and convenience online.

Half of the participants in the discussion group with people aged between 18 and 40 agreed that it was fine to provide their personal data for higher efficiency and convenience online, but they would ask for the consent of their friends if personal data of their friends was involved. The rest of them reported that they would provide fake email addresses or they had created a lot of email accounts to address such requests.

The participants in the discussion group with people with lower education level had various opinions to provide their personal data online for higher efficiency and convenience online. One of them said that she would not exchange at all. Another one would give her friends' email address but not telephone number. Two of them would ask for the consent of their friends if personal data of their friends was involved. The last one would not give her friends' information but disclosure of her information would depend on the situation.

4.1.7.3 Willing to compromise personal data protection in exchange for benefit and benefit-in-kind

Among those participants who would provide their personal data in exchange for benefit and benefit-in-kind, many of them would never provide ID number for the benefits.

For the other's personal data, all of them generally won't do so unless they got others' consent.

More participants aged 41 and above (all participants) would provide their personal

data except ID number in exchange for benefit and benefit-in-kind than those participants aged between 18 and 40 (two participants). Also, more participants with higher education level (all participants) would provide their personal data in exchange for benefit and benefit-in-kind than those participants with lower education level (only one participant).

4.1.8 Location requests on iOS (e.g. iPhone) and Android (e.g. Samsung)

In the focus group discussions, all participants preferred iOS because of factors like personalised privacy level, flexibility, a higher privacy protection and more detailed privacy settings available, while for Android, they had to accept all in one go. One participant pointed out that Android would warn users about the possibility of data leakage prior to the download, but iOS enabled users to set own privacy options after the download. In addition, Android users could not download applications if they do not accept Android's privacy policies.

Chapter 5 Conclusion and Recommendation

This survey collected views from 1,222 respondents to the household telephone survey and 36 participants in the focus group interviews about the degree of sensitivity or importance people ascribe to different types of personal data, how people exercise their right under the Ordinance when they find their personal data being misused, public perception of PCPD's performance and public awareness of the privacy issues with social media.

Privacy attitudes about the use of ID cards

From the results of the household telephone survey, around 30% of respondents did not mind legitimate, justified use of ID card information at all, while nearly 40% did mind clearly unjustified use of ID card information. The participants indicated their privacy attitudes about the use of their ID cards in the following different situations:

a) Their ID card details are noted down by a police officer when he stops them in the street (They did not mind at all: 31.1% vs they would mind enough to make a complaint: 8.6%)
b) Their name and ID card number are noted down by a security guard in order to let them into a residential building as a visitor (11.8% vs 17.5%)
c) Providing their ID card number to postman when collecting parcels (29.9% vs 5.3%)
d) Providing their ID card number on a job application form (29.3% vs 4.6%)
e) Providing their ID card copy when attending a job interview, after shortlisting, but before receiving a job offer (15.4% vs 16.9%)
f) Providing their ID card number when enrolling for fitness club membership (8.4% vs 25.3%)
g) Providing a copy of their ID card when enrolling for fitness club membership (5.9% vs 36.4%)

Privacy attitudes to providing different types of personal data

From the results of the household telephone survey, few respondents were very concerned about providing mobile phone number (even though it allows receiving advertising calls), occupation or full date of birth (even though it is often used for validation), but many expressed valid concern about providing personal income and ID card number. Respondents indicated their privacy attitudes about providing personal data in order to obtain a discount in the following different situations:

a) Full residential address (They did not mind at all: 7.4% vs they would mind enough to make a complaint: 26.9%)
b) Mobile phone number (16.8% vs 15.5%)
c) ID card number (6.2% vs 38.6%)
d) Personal income (5.8% vs 38.2%)
e) Occupation (17.3% vs 14.1%)
f) Date, month and year of birth (14.5% vs 22.9%)

Privacy for public registries, CCTV & loyalty cards

From the results of the household telephone survey, 6-16% of respondents had no concern and 18-35% of respondents had serious concern about the current practices of the marriage and lands registry, the companies registry providing the ID card number and residential address of a company director and CCTV covering their doorway. 67% of respondents had serious concern and only 1-2% of respondents had no concern as regards provision of their or their friends/relatives names and addresses when applying for a loyalty card. Respondents indicated their privacy attitudes to collection and/or use of personal data in the following different situations:

a) Marriage registry shows occupation of marrying parties for 3 months publicly (They did not mind at all: 15.0% vs they would mind enough to make a complaint: 18.4%)
b) Lands registry shows registered owners to anyone (13.3% vs 18.6%)
c) Companies registry shows ID card number of directors to anyone (10.0% vs 27.5%)
d) Companies registry shows residential address of directors to anyone (6.4% vs 35.0%)
e) CCTV showing your doorway (16.5% vs 23.2%)
f) Friends provide your name/address for loyalty card without prior agreement (0.9% vs 66.6%)
g) Providing their friends name/address for loyalty card without prior agreement

(1.0% vs 67.4%)

Misuse of personal data

From the results of the household telephone survey, nearly half (46%) of respondents had experienced misuse of their personal data in the last 12 months and the most common source of the problem was banks (57%), followed by telecom companies (32%), fitness/beauty centres (26%) and money lenders (17%). Almost 11% of those who experienced misuse had made a complaint. while of those who had not complained, the major reasons were that friends had provided the information (35%), or they were unwilling to involve the staff of the company responsible for the misuse (25%).

For the notification of data leakage to data subjects and PCPD, all participants in the focus group interviews generally agreed that the data subjects and PCPD as well as the media should be notified immediately.

Awareness of the work of the PCPD

From the results of the household telephone survey, the majority of respondents (63%) were aware of the PCPD through mass media, with smaller proportions through the website/multimedia (19%), PCPD publications (15%) and the PCPD publicity programmes (7%). An overwhelming majority (86%) of respondents agreed or strongly agreed that PCPD has increased community awareness of personal data privacy issues after the Octopus Incident in 2010, with only 14% disagreeing/strongly disagreeing.

Most of the participants in the focus group interviews agreed that naming the organisation at fault in PCPD's investigation reports was effective because it raised public awareness of personal data protection. Meanwhile, most of them reported that their trust had decreased towards those companies against which the PCPD had reported contraventions of the PD(P)O.

Whether the current regulatory framework provides sufficient protection

From the results of the focus group interviews, only several participants aged 41 and above or with lower education level thought the current regulatory framework was sufficient to protect the public and many of them did not have any ideas about the

regulatory framework. No participants with higher education level thought the current regulatory framework was sufficient to protect the public because they were concerned that the current situation was that people were forced to provide personal data and a lot of personal data could be found openly.

Awareness of the consequences of non-compliance with the Ordinance and what they expect the PCPD to do

From the results of the focus group interviews, most of the participants did not know the consequences of violating the Ordinance.

Direct marketing and the PD(P)O amendment

From the results of the focus group interviews, only a few participants aged between 18 and 40 or with lower education level were aware that companies had to notify potential customers and get their consent first before using their personal data for direct marketing. However, most of the participants aged 41 or above or with higher education level were aware of this notification and consent requirement.

The minority of the participants in the focus group interviews knew that direct marketing calls could cover only the type of products that they agreed to, when giving approval to use their personal data for direct marketing.

Many participants in the focus group interviews knew that organisations could not transfer their personal data to a third party for use in direct marketing unless written consent has been obtained.

The majority of participants aged between 18 and 40 knew that they had the right to opt out from an organisations's direct marketing even if they had opted in before. However, the majority of participants aged 41 and above did not know that they had the right to opt out.

The minority of participants in the focus group interviews had heard of the revision of the PD(P)O, including enhanced coverage of direct marketing. After a brief introduction of the PD(P)O amendment in force since 2013 about the direct marketing, the majority of participants believed that the PD(P)O amendment since 2013 was not sufficient to protect the public as the enforcement powers were insufficient.

Trustworthiness in handling complaints

From the results of the household telephone survey, the Independent Complaints Against Corruption (ICAC) is clearly the most trusted agency with 33% rating it as 9 or 10, while PCPD (25% rated as 9 or 10)) edged out the Consumer Council (CC)(24% rated as 9 or 10)). The respondents gave their perceived trustworthiness rating to the following six statutory agencies in handling complaints:

(a) Consumer Council (rating as 9 or 10: 24.3% vs rating 5 or less: 30.0%)
(b) Hong Kong Police Force (19.9% vs 42.5%)
(c) The Ombudsman Hong Kong (19.7% vs 34.9%)
(d) Equal Opportunities Commission (16.4% vs 38.1%)
(e) Independent Commission Against Corruption (32.7% vs 23.4%)
(f) Office of the Privacy Commissioner for Personal Data (25.0% vs 29.9%)

Privacy attitudes towards online activities

(a) Advertising and privacy

From the results of the household telephone survey, the majority of respondents (56%) would certainly not be prepared to pay $20 per month for email services like Gmail with the promise of no advertising at all, while only 6% would be certainly willing, suggesting most people are reluctant to pay for additional privacy protection in this situation.

(b) Facebook and privacy

From the results of the household telephone survey, the majority of respondents (56%) who have ever had a Facebook account use Facebook at least daily with only 18% rarely or never using their account. A strong majority (77%) of Facebook account users are aware of the privacy setting, of whom a strong majority (73%) have ever checked the settings, of whom nearly all (90%) have changed the settings. This suggests that people are now generally aware of the need of privacy protection in social networks and can act to protect themselves. (A privacy awareness survey on Facebook users conducted by the PCPD in 2013 found that over 80% of the respondents knew how to set access right to protect their personal data, but less than 40% did so.)

(c) Smartphones and privacy

From the results of the household telephone survey, an overwhelming majority (87%) of respondents use a smartphone of whom 95% have WeChat or a similar app installed, of whom 81% installed it themselves. Only 72% of respondents with WeChat or a similar app installed were aware that it accesses all of the contacts on their smartphone, while a significant proportion (33%) thought the law should prohibit this.

Privacy tradeoffs

Most participants aged between 18 and 40 or with lower education level in the focus group interviews were not willing to provide their own or others personal data for money or other benefits. Conversely, participants aged 41 or above or with higher education level were willing to provide their own personal data except ID number in exchange for benefit and benefit-in-kind, but not willing to provide others personal data.

Recommendations

The telephone survey results indicate that awareness of PCPD, of privacy rights of individuals and trust in the PCPD are generally quite high and there is good awareness of the need to balance privacy rights differently in different situations. However concern about some current practices of public registries allowing public access to personal data suggests public support for further action by PCPD.

The focus group interviews suggest a number of areas where further action may be needed:

The general public seems unaware of how limited the enforcement powers of the PCPD are, suggesting a need for further education about this, which may increase support for additional powers, especially as better educated participants did not believe that the current regulatory framework was sufficient to protect the public.

Most less educated participants were unaware of the requirement for direct marketers to notify potential customers and obtain consent in advance, suggesting a need for further education. Although better educated participants were aware of the notification and consent requirement, they agreed that it was difficult to opt-out in practice,

suggesting a need for regulatory review, especially as the majority of respondents, after explanation of the amendment, agreed that is was insufficient to address the problem, given the limited enforcement powers of PCPD.

The widespread support for naming organisations at fault in investigation reports suggest that PCPD should make further use of this approach.

The support for data leakage to be always reported to the PCPD suggests public support for further powers to require this.

Limitations

1. The data were not weighted for the number of eligible respondents in a household and the number of phones in a household, or to account for non-response.

2. The use of the 'Last Birthday' rule to select respondent when there were more than one eligible respondents resided in a household by the time of the telephone contact could not cover people who were always not at home in the evening and weekends.

3. Household telephone survey excludes households without fixed line telephones which might result in selection bias due to under-representation of certain segments of the population, such as newly formed households who may only have mobile telephones.

Appendix A: Telephone Survey Questionnaire

Part I: Introduction

第一部份: 介紹

Good afternoon/evening! My name is (surname). I am an interviewer at the Social Sciences Research Centre, University of Hong Kong, conducting a survey for the Office of the Privacy Commissioner for Personal Data. I would like to ask for your opinion on personal data protection in HK.

午安/晚安。我姓 x，我係香港大學社會科學研究中心嘅訪問員。我哋現正為個人資料私隱專員公署進行一項電話調查，希望收集有關你對香港保護個人資料嘅意見。

[v1 Telephone #] [v1 電話號碼 #]
[v2 Interviewer #] [v2 訪問員 #]

<respondent selection using modified next birthday rule>
<使用下一個最快生日規則選出被訪者>
Among all those who are at home, may I speak to the one aged at least 18 who will next have a birthday?

麻煩請而家喺你屋企而又年滿18歲，同埋最接近下次生日既嗰位成員黎接聽電話

(Interviewer: explain the respondent selection method by using “Next Birthday” rule if respondent questions) If the respondent is aged at least 18; please ask him/her to answer the phone. (Interviewer: Repeat the introduction)

(訪問員: 如被訪者查詢，解釋"下一個最快生日"規則)如被訪者已年滿18歲，邀請他/她聽電話。(訪問員: 再次讀出介紹)

Good morning/afternoon/evening! My name is (surname). I am an interviewer at the Social Sciences Research Centre, University of Hong Kong, conducting a survey for the Office of the Privacy Commissioner for Personal Data. I would like to ask for your opinion on personal data protection in HK, which would only take about 15 minutes. Our conversation may be audio-recorded for further data checking. I would like to stress that all information collected will remain strictly confidential. Individual details will not be disclosed or identifiable from this survey. If you have any questions or concerns about the research, please contact HKUSSRC at 3917-1600. If you have questions about your rights as a research participant, please contact the Human Research Ethics Committee for Non-Clinical Faculties, HKU (2241-5267).

早晨/午安/晚安。我姓 x，我係香港大學社會科學研究中心嘅訪問員。我哋現正為個人資料私隱專員公署進行一項電話調查，希望收集有關你對香港保護個人資料嘅意見。整個訪問需時大約 15 分鐘。為方便日後核對資料，訪問會被錄音。所有收集到嘅資料會絕對保密，任何喺呢次調查所收集到嘅個人資料都唔會被公開或被識辨得到。如果你對呢項調查有任何查詢或意見，請致電 3917-1600 向香港大學社會科學研究中心。如果你想知道更多有關研究參與者嘅權益，請致電 2241-5267 向香港大學非臨床研究操守委員會查詢。

We would like to invite you to take part in the survey. Do you agree to the audio recording? Do you agree to participate in this survey?

我地想邀請你參與呢項調查。請問你同意被錄音嘛? 你同唔同意參與呢項調查?

If agree, interview starts, else interview ends, thank respondent.

如同意, 訪問員開始, 否則訪問結束, 多謝被訪者

I am now going to ask some questions about your ID card, where I would like you to tell me how much you mind on a scale from 0-10 where 0 means you do not mind at all and 10 means you would mind enough to make a complaint:
而家我會問一啲同你身份證有關嘅問題，請你用 0 至 10 分表示你嘅介意程度，0 分表示你會完全唔介意，10 分表示你會非常介意並足以令你去作出一個投訴。

Q1. How much do you mind if your ID card details are noted down by a police officer when he stops you in the street?
當你喺街上被警員截停嘅時候，你有幾介意你嘅身份證資料被警員記錄?
a) 0-10

c) no idea 唔知道
d) refuse to answer 拒絕回答

Q2. How much do you mind if your name and ID card number are noted down by a security guard in order to let you into a residential building as a visitor?
當你以訪客身份進入一座住宅大廈嘅時候，你有幾介意保安人員記錄你嘅姓名和身份證號碼?

a) 0－10
c) no idea 唔知道
d) refuse to answer 拒絕回答

Q3. How much do you mind providing your ID card number to postman when collecting parcels?
當你領取包裹嘅時候，你有幾介意向郵差提供你嘅身份證號碼?

a) 0－10
c) no idea 唔知道
d) refuse to answer 拒絕回答

Q4. How much do you mind providing your ID card number on a job application form?
你有幾介意喺職位申請表中提供你嘅身份證號碼?

a) 0－10
c) no idea 唔知道
d) refuse to answer 拒絕回答

Q5 How much do you mind providing your ID card copy when attending a job interview, after shortlisting, but before receiving a job offer
你有幾介意喺見工嘅時候，即未接獲聘任之前，提供你嘅身份證副本?

a) 0－10
c) no idea 唔知道
d) refuse to answer 拒絕回答

Q6. How much do you mind providing your ID card number when enrolling for fitness club membership?
當你登記健身中心會籍嘅時候，你有幾介意提供你嘅身份證號碼?

a) 0－10
c) no idea 唔知道
d) refuse to answer 拒絕回答

Q7. How much do you mind providing a copy of your ID card when enrolling for fitness club membership?
當你登記健身中心會籍嘅時候，你有幾介意提供你嘅身份證副本?

a) 0－10
c) no idea 唔知道
d) refuse to answer 拒絕回答

Now I'll ask you similar questions about how much you mind providing different types of personal **data in return for a discount card from a retail shop where you frequently buy things, on the 0-10** scale where 0 means you do not mind at all and 10 means you would certainly refuse.

而家我會問一啲相似嘅問題，係關於你有幾介意為咗換取你經常光顧嘅零售商店嘅優惠卡而提供唔同種類嘅個人資料，請你用 0 至 10 分表示你嘅介意程度，0 分表示你完全唔介意，10 分表示你肯定會拒絕。

Q8. Your **full residential address**?
你嘅**詳細居住地址**？

a) 0－10
c) no idea / don't know 唔知道
d) refuse to answer 拒絕回答

Q9. Your **mobile phone number**?
你嘅**手提電話號碼**？

a) 0－10
c) no idea / don't know 唔知道
d) refuse to answer 拒絕回答

Q10. Your **ID card number**?
你嘅**身份證號碼**？

a) 0－10
c) no idea / don't know 唔知道
d) refuse to answer 拒絕回答

Q11. Your **personal income**?
你嘅**個人收入**？

a) 0－10
c) no idea / don't know 唔知道
d) refuse to answer 拒絕回答

Q12. Your **occupation**?
你嘅**職業**？

a) 0－10
c) no idea / don't know 唔知道
d) refuse to answer 拒絕回答

Q13. Your **date, month and year of birth**?
你嘅**出生年、月、日**？

a) 0－10
c) no idea / don't know 唔知道
d) refuse to answer 拒絕回答

I am going to list some situations, which may be an invasion of personal data privacy. Please use a number between 0 and 10 where 0 means it is not an invasion of personal data privacy and 10 is a very severe invasion of personal data privacy.

我將會講出一啲可能係侵犯個人資料私隱嘅情況。請你用 0 至 10 分來表示，0 分代表完全冇侵犯個人資料私隱，而 10 分代表非常侵犯個人資料私隱。

Q14. Marriage Registry exhibits the "Notice of Intended Marriage" containing the occupation of the intended marrying parties in places open to public for 3 months.

婚姻登記處喺公眾地方展示包括準備結婚人士職業嘅「擬結婚通知書」3個月。

a) 0 – 10	0-10
b) difficult to say / no idea / don't know	好難講/ 唔知道
c) refuse to answer	拒絕回答

Q15. Name of the registered owners and the value of the property transaction can be checked out by anyone in the Lands Registry.
任何人士都可以喺土地註冊處查核註冊業主嘅姓名同物業成交價。

a) 0 – 10	0-10
b) difficult to say / no idea / don't know	好難講/ 唔知道
c) refuse to answer	拒絕回答

Q16. Full HKID card number of a company director can be checked out by anyone in the Companies Registry.
任何人士都可以喺公司註冊處查核公司董事嘅完整身份證號碼。

a) 0 – 10	0-10
b) difficult to say / no idea / don't know	好難講/ 唔知道
c) refuse to answer	拒絕回答

Q17. Residential address of a company director can be checked out by anyone in the Companies Registry.
任何人士都可以喺公司註冊處查核公司董事嘅住址。

a) 0 – 10	0-10
b) difficult to say / no idea / don't know	好難講/ 唔知道
c) refuse to answer	拒絕回答

Q18. CCTV covering the doorway of your flat.
閉路電視嘅錄影範圍覆蓋你居住單位嘅出入口。

a) 0 to 10	0-10
c) no idea / don't know	唔知道
d) refuse to answer	拒絕回答

Q19. Your friends / relatives refer you to a retail shop and provide your name and address to the retail shop when he/she applies for a loyalty card without getting your agreement first

當你嘅親戚或朋友申請一間零售商店嘅積分優惠卡時，喺未得到你嘅同意前，將你嘅姓名同住址轉介俾嗰間零售商店。

a) 0 to 10 0-10
c) no idea / don't know 唔知道
d) refuse to answer 拒絕回答

Q20. You refer your friends / relatives to a retail shop and provide their names and addresses in the application form for a loyalty card without getting their agreement first

當你申請一間零售商店嘅積分優惠卡時，喺未得到你嘅親戚/朋友同意前，將佢哋嘅姓名同住址轉介俾嗰間零售商店。

a) 0 to 10 0-10
c) no idea / don't know 唔知道
d) refuse to answer 拒絕回答

Misuse of personal data
個人資料被濫用

Q.21 Have you personally experienced what you consider to be a misuse of your personal data within the last 12 months? (if yes, ask Q22, otherwise, skip to Q25)
喺過去 12 個月內，你有冇親身經歷過，你認為你嘅個人資料被濫用嘅情況? (如有, 問 Q22, 否則, 跳至 Q25)

a) yes 有
b) no (skip to Q25) 冇 (跳至 Q25)
c) difficult to say / no opinion / can't remember / don't know (skip to Q25)
好難講/冇意見/唔記得/唔知道 (跳至 Q25)
d) refuse to answer (skip to Q25) 拒絕回答 (跳至 Q25)

Q22. Who or what type of organisation was responsible for the last misuse of your personal data?
就最近嗰次你嘅個人資料被濫用，請問邊個或邊啲機構應該負責呢?

(**Multiple response, Unprompted**)
(可選多項, 不要讀出答案)

a)	government departments	政府部門
b)	banks	銀行
c)	money lending companies	財務公司／放債公司
d)	public hospitals	公營醫院
e)	private hospitals	私營醫院
f)	insurance companies	保險公司
g)	real estate agents	地產代理
h)	property management	物業管理
i)	schools	學校
j)	telecommunication companies	電訊公司
k)	social services organisations	社會服務機構
l)	mass media / journalists	大眾媒體/記者
m)	fitness and beauty centres	健身及美容中心
n)	retail outlets	零售商店
o)	your employer	你嘅僱主
p)	family members living in the same household	同住嘅家庭成員
q)	friends / classmates / colleagues	朋友/ 同學/同事
r)	neighbours	鄰居
s)	other individuals	其他人
t)	other organisations	其他組織
u)	difficult to say / no opinion / can't remember / don't know	好難講/冇意見/唔記得/唔知道
v)	refuse to answer	拒絕回答

Q23. Did you make a complaint about this case of your personal data being misused?
就嗰次你嘅個人資料被濫用，你有冇作出過投訴呢?

a) yes (skip to Q25) 有(跳至 Q25)
b) no 冇
c) difficult to say / no opinion / don't know (skip to Q25)

好難講/冇意見/唔記得/唔知道 (跳至 Q25)
d) refuse to answer (skip to Q25) 拒絕回答 (跳至 Q25)

Q24. What is your main reason for not lodging a complaint?
你冇作出投訴嘅主要原因係乜嘢?

a) cannot afford the time 唔得閒/抽唔到時間
b) not worthwhile 唔值得
c) troublesome 怕麻煩
d) don't know where to lodge a complaint 唔知道向邊個機構/部門作出投訴
e) did not know the right conferred by the law 唔知道法例賦予嘅權利
f) other reasons, please specify:_____ 其他原因，請註明：_____
g) difficult to say / no opinion / don't know 好難講/冇意見/唔記得/唔知道
h) refuse to answer 拒絕回答

Channels for learning about the Office of the Privacy Commissioner for Personal Data (PCPD) and the effectiveness and trustworthiness of the PCPD
了解個人資料私隱專員公署嘅途徑、其工作效率及可靠程度

Have you been made aware of the work of the Office of the Privacy Commissioner for Personal Data (PCPD) through the following channels?

你有冇透過以下嘅途徑留意過個人資料私隱專員公署嘅工作?

Q.25 mass media (e.g. news on TV, newspaper and radio or advertisements)
大眾媒體（如電視、報紙及電台嘅新聞或廣告）

a) yes 有
b) no 冇
c) no idea 唔知道
d) refuse to answer 拒絕回答

Q.26 PCPD's publications (e.g. guidance notes, pamphlets, fact sheets and code of practices)
個人資料私隱專員公署嘅刊物（如指引、小冊子，資訊單張和實務守則）

a) yes 有
b) no 冇

c) no idea 唔知道
d) refuse to answer 拒絕回答

Q.27 PCPD web site and multimedia (e.g. web videos)
個人資料私隱專員公署嘅網頁同多媒體資訊（如網上短片）

a) yes 有
b) no 冇
c) no idea 唔知道
d) refuse to answer 拒絕回答

Q.28 PCPD publicity programmes (e.g. seminars, workshops and exhibitions)
個人資料私隱專員公署嘅推廣活動（例如講座、研習班及展覽）

a) yes 有
b) no 冇
c) no idea 唔知道
d) refuse to answer 拒絕回答

Q29 In 2010, Octopus admitted to sharing personal data with five business partners without providing adequate notice to consumers and obtaining customers' consent.

To what extent do you agree that the PCPD has increased community awareness of personal data privacy issues after the Octopus Incident in 2010? Do you strongly agree, agree, disagree or strongly disagree?

喺2010年八達通獎賞公司承認在沒有向客戶提供足夠資訊及取得客戶的同意下，與五個合作商戶共用客戶的個人資料。

請問你同唔同意個人資料私隱公署喺 2010 年八達通事件發生後，提升咗社會對個人資料私隱呢方面嘅意識呢？你非常同意，同意，唔同意定係非常唔同意?

a) strongly agree 非常同意
b) agree 同意
c) disagree 唔同意
d) strongly disagree 非常唔同意

e) difficult to say / no opinion / don't know 好難講/冇意見/唔記得/唔知道
f) refuse to answer 拒絕回答

What is your opinion on the trustworthiness of the following organisations when handling complaints? Please tell me a number indicating the level of trustworthiness, 0 means that you have no trust and 10 means total trust.
請問你對以下嘅機構喺處理投訴嘅可信性有咩睇法? 請以 0 至 10 分來表示可信程度, 0 分代表你完全唔信任，而 10 分代表完全信任

Q30. Consumer Council 消費者委員會

a) 0 – 10 0-10
b) difficult to say 好難講
c) no idea / don't know 唔知道
d) refuse to answer 拒絕回答

Q31. Hong Kong Police Force 香港警務處

a) 0 – 10 0-10
b) difficult to say 好難講
c) no idea / don't know 唔知道
d) refuse to answer 拒絕回答

Q32. The Ombudsman Hong Kong 香港申訴專員公署

a) 0 – 10 0-10
b) difficult to say 好難講
c) no idea / don't know 唔知道
d) refuse to answer 拒絕回答

Q33 Equal Opportunities Commission 平等機會委員會

a) 0 – 10 0-10
b) difficult to say 好難講
c) no idea / don't know 唔知道
d) refuse to answer 拒絕回答

Q34 Independent Commission Against Corruption 廉政公署

a) 0 – 10 0-10
b) difficult to say 好難講
c) no idea / don't know 唔知道
d) refuse to answer 拒絕回答

Q35. Office of the Privacy Commissioner for Personal Data 個人資料私隱專員公署

a) 0 – 10 0-10
b) difficult to say 好難講
c) no idea / don't know 唔知道
d) refuse to answer 拒絕回答

Privacy / security concerns about transactions on the Internet
關於喺互聯網上交易嘅私隱/安全問題

Q36. Google currently offers Internet search and basic email services for free in return for showing you advertising which is targeted based on the information Google collected and analysed from your previous search and email behavior. If Google was to offer comparable services of search and email, but without any advertising at all, how willing would you be to pay HK$20 per month for this, on a scale from 0-10 where 0 means I certainly would not use it and 10 means I certainly would be willing to pay this amount.

現時 Google (即"谷歌")為用戶免費提供互聯網搜尋及基本電郵服務，收集用戶過往嘅搜尋及電郵行為資料作出分析，從而顯示出相關嘅廣告。假如 Google 提供相類似嘅搜尋及電郵服務，你會有幾願意每月支付港幣$20，享用呢啲服務但唔再收到任何廣告訊息呢? 請你用 0-10 分來表示，0 分表示我肯定唔會使用，而 10 分表示這刻我肯定願意支付。

a) 0-10
b) never use Internet or email service 從來唔用互聯網或電郵服務
c) difficult to say / no opinion / don't know 好難講/冇意見/唔記得/唔知道
d) refuse to answer 拒絕回答

Q37. How often do you normally use Facebook?
你一般有幾經常使用 Facebook?

a) ever registered Facebook account but no longer use	曾經有 Facebook 帳戶但不再使用
b) rarely	很少
c) less than weekly	少於一星期一次
d) at least weekly but less than daily	一星期至少一次但少於每天一次
e) at least daily	至少每天一次
f) no Facebook account (skip to Q41)	從來都冇 Facebook 帳戶 (跳至 Q41)

Q38. Are you aware that there are privacy settings in Facebook?
你有冇留意到Facebook係有私隱設定?

a) yes	有
b) no (skip to Q41)	冇
c) refuse to answer	拒絕回答

Q39. Have you ever checked the privacy settings in Facebook?
你有冇曾經檢查過 Facebook 嘅私隱設定?

a) yes	有
b) no (skip to Q41)	冇
c) refuse to answer	拒絕回答

Q40. Have you ever changed the privacy settings in Facebook?
你有冇曾經改變 Facebook 嘅私隱設定?

a) yes	有
b) no	冇
c) refuse to answer	拒絕回答

Q41. Do you use a smartphone at all (i.e. phone with Internet access and apps)?
你有冇使用智能手機 (即係可以上網同可以使用應用程式嘅手機)

a) yes	有
b) no	冇
c) no idea	唔知道
d) refuse to answer	拒絕回答

If Yes to Q42, ask Q43
如 Q42 答有, 問 Q43

Q42. Do you have any of WeChat/Line/Viber/Whatsapp installed on a smartphone you use (i.e. apps for direct messaging friends or family)?
你所使用嘅智能手機有冇安裝 微信/ Line/ Viber/ Whatsapp (即係可以同朋友或者家人直接通訊嘅應用程式)

a) yes	有
b) no (skip to Q46)	冇 (跳至 Q46)
c) no idea (skip to Q46)	唔知道 (跳至 Q46)
d) refuse to answer (skip to Q46)	拒絕回答 (跳至 Q46)

Q43. Did you install any of those apps yourself?
呢啲應用程式係唔係你自己安裝?

a) yes	是
b) no	否
c) no idea	唔知道
d) refuse to answer	拒絕回答

Q44. Were you aware that these apps access all of your contacts on your phone?
你知唔知道呢啲應用程式會查閱你電話上所有聯絡人嘅資料?

a) yes, I know	知道
b) no, I don't know	唔知道
c) refuse to answer	拒絕回答

Q45. How much of a privacy problem do you think this practice of accessing all your contacts is? Please use a number between 0 and 10 where 0 means it is no problem at all and 10 means the law should prohibit this.
你認為查閱你所有聯絡人資料嘅做法會有幾大嘅私隱問題? 請用 0 至 10 分來表示, 0 分代表冇侵犯私隱，而 10 分代表法例應該禁止呢個做法。

a) 0 – 10	0-10
c) no idea / don't know	唔知道
d) refuse to answer	拒絕回答

Demographics:

背景

The following questions are about your personal data for analysis purposes only.
以下問題是關於你嘅個人資料並只會用作分析用途

Q46.Record the respondent's gender
記錄被訪者嘅姓別

a) male 男
b) female 女
c) refuse to answer 拒絕回答

Q47.How old are you?
你嘅年齡係?

a) absolute number 確實年齡
b) refuse to answer 拒絕回答

Q48.What is your education level?
你嘅教育程度係?

a) primary or below 小學或以下
b) secondary 中學
c) tertiary or above 專上或以上
d) refuse to answer 拒絕回答

Q.49 What is your normal monthly personal income (read out the income brackets if necessary)?
你每月嘅個人收入大約係? (如有需要可讀出收入範圍)

a) no income 冇收入
b) under 2000 少於 2000
d) 2000 – 3999 2000 - 3999
e) 4000 – 5999 4000 - 5999
f) 6000 – 7999 6000 - 7999
g) 8000 – 9999 8000 - 9999
h) 10000 – 14999 10000 - 14999
i) 15000 – 19999 15000 - 19999

j)	20000 – 29999	20000 - 29999
k)	30000 – 49999	30000 - 49999
l)	50000 and over	50000 或以上
m)	difficult to say / no opinion / don't know	好難講/ 冇意見/ 唔知道
n)	refuse to answer	拒絕回答

Thank you for answering the questions, goodbye
問卷已完成，多謝，拜拜。

End of Questionnaire
問卷完

Appendix B: Focus Group Interviews Guidelines

Information sheet for focus groups

Thank you for agreeing to participate in today's focus group which will last for one and half hours. We are commissioned by Office of the Privacy Commissioner for Personal Data, Hong Kong to collect public views on personal data protection in HK. I would like to stress that all information collected today will be treated in strict confidence. The focus group is being audio recorded, but the recording will only be retained securely for four weeks to allow me to write up an anonymised summary. If you have any concerns now, please speak up now and if you have any concerns later, you can call me, Linda Cho, on 3917-1900. If you have questions about your rights as a research participant, please contact the Human Research Ethics Committee for Non-Clinical Faculties, HKU (2241-5267).

If everyone agrees to the audio-recording, let's start:

感謝您們同意參與今天的焦點小組討論，整個討論大約個半小時。香港大學社會科學研究中心是受香港個人資料私隱專員公署委託進行是次的調查，目的是想瞭解您們對香港保護個人資料的意見。我想強調的是，今天所有收集的意見將會絕對保密。焦點小組現正在錄製音頻檔案，但錄音只會被安全保留四個星期，讓我完成編寫一個不記名的報告。如果您有任何問題，請現在說起來，如果以後有任何問題，請致電 3917-1600 向本人查詢。如你想知道更多有關研究參與者的權益，請致電 2241-5267 向香港大學非臨床研究操守委員會查詢。

如果每個人都同意所述的音頻記錄，讓我們開始：

Introduction to PD(P)O in Hong Kong

The Office of the Privacy Commissioner for Personal Data (PCPD) is an independent statutory body set up to oversee the enforcement of the Personal Data (Privacy) Ordinance (Cap. 486) which came into force on 20th December, 1996.

The objectives of the Ordinance:

Protecting the privacy right of a "data subject" in respect of "personal data", but general privacy issues are not protected.

A data subject refers to the living individual who is the subject of the "personal data" concerned.

Definitions under the Ordinance

"Personal Data" should satisfy three conditions:

(1) relating directly or indirectly to a living individual;
(2) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
(3) in a form in which "access to" or "processing of" the data is practicable.

Data: any representation of information in any document, including expression of opinion or personal identifier (e.g. person's name, telephone number, address, sex, age, occupation, salary, nationality, photo, identity card number, medical record, etc).

Document: in addition to written document, "document" includes visual or non-visual device, e.g. photo, audio tape, video tape, optical disc.

Data Protection Principles under the Ordinance

Data users must comply with the six data protection principles in the collection, holding, accuracy, retention period, security, privacy policy and access to and correction of personal data.

The six data protection principles form the base of the Ordinance.

簡介個人資料私隱專員公署

簡介香港個人資料(私隱)條例

個人資料私隱專員公署是一個獨立法定機構，負責監察香港法例第486章個人資料(私隱)條例的施行。條例在一九九六年十二月二十日生效。

條例的宗旨

- 條例旨在保障「資料當事人」在「個人資料」方面的私隱權利，但並不保障一般私隱事宜
- 「資料當事人」是有關「個人資料」所指的在世人士

條例內的詞彙定義

「個人資料」須符合以下三項條件：
(1)直接或間接與一名在世人士有關 ；
(2)從該等資料直接或間接地確定有關的個人的身分是切實可行的；而
(3)該等資料的存在形式令予以「查閱」及「處理」均是切實可行的。

「資料」： 任何文件中資訊的任何陳述，包括意見的表達或身份代號(如個人姓名、電話號碼、地址、性別、年齡、宗教信仰、國籍、相片、身分證號碼、信貸紀錄等) 。

「文件」： 除書面文件外，任何視覺上或非視覺上的物件， 如相片、錄音帶、錄影帶、光碟均被視為「文件」。

條例設定的保障資料原則

資料使用者在收集、持有、準確性、保留期間、保安、私隱政策、查閱及更改個人資料各方面 ，必須遵從該六項原則的規定 。

條例載列六項保障資料原則，是條例的基本精神。

Part 1 Compliance & enforcement of PCPD

Introduce the PCPD enforcement powers (using California Fitness as an example) **and types of actions PCPD can take:**

- first explain the California Fitness situation – they were collecting copies of ID cards for all customers, which is a serious security risk and was excessive.

"California Fitness , breached data privacy by collecting excessive personal data, including copies of Hong Kong Identity Card, from its customers who applied for or renewed membership"

- To assess the awareness and expectations of the role of the PCPD (e.g. as an independent statutory body, enforcement powers under Ordinance, promotion and educational roles; scope of privacy protection i.e. personal data only)
- To find out if people are aware of the consequences of non-compliance with the Ordinance and what they expect the PCPD to do, especially as it only has HK jurisdiction and discuss possible remedies: Request for apology? Reporting case to PCPD for record? Request for monetary compensation? Request stopping the contravening act?
- To find out whether they think the current regulatory framework is sufficient to protect them
- Publishing reports (does the reports that name the organisation at fault or work? Are you aware of these from the PCPD's media briefing?)

<u>For SSRC information</u>

The action taken by PCPD in this case:

- The Commissioner served an enforcement notice on California Fitness directing it to remedy and prevent any recurrence of the contravention.

Introduce direct marketing and the PD(P)O amendment to see if they believe the amendments are sufficient

- Whether people are aware that organisations are required provide data subjects notification (i.e. intention to use the personal data in direct

marketing) and obtain their consent before using their personal data for direct marketing

- To assess how people respond to direct marketers' notifications (to secure consent for use of personal data)
- Whether people know that organisations can only promote products / services that he/ she previously consented (i.e. permitted class of marketing subject)
- Whether people know that organisations cannot transfer their personal data to third party (no matter for gain or not) for use in direct marketing unless **written** consent has been obtained
- To access whether people aware of their opt-out right
- To understand how people respond to direct marketer if they do not wish to receive promotional messages

Introduce Notification of data leakage to data subjects and PCPD

"The Police Force Repeated Incidents of Loss of Notebooks containing Sensitive Personal Data and loss of fixed penalty ticket"
"Leaked police internal documents containing personal data via Foxy, such as witness statement"

- What is their expectation as to whether PCPD or data subjects should be notified and when (scenarios would be useful to see what they think).

Give example of Octopus sharing personal data with five business partners without providing adequate notice to consumers and obtaining customers 'consent

"The collection and use of customers' personal data under the Octopus Rewards Programme run by Octopus Rewards Limited, OHL admitted to the public that it had transferred customers' personal data to CIGNA and another business partner, Card Protection Plan Limited."

Dealing with organisations which "respect for privacy"

- To what extent would "respect for privacy" be a factor in choosing a service or a product offered by an organisation
- PCPD issues investigation reports about organisations contravening the PD(P)O. Does it affect people's willingness to deal with those organisations?
- What actions people would take in case their personal data has been misused? (e.g. Contact the culprit direct, take legal actions, cease any dealings with the organisation, lodge a complaint (including reasons for not lodging a complaint), expose the issue to the public, change the mode of dealings (e.g. from online to offline), enhance own data security (e.g. change passwords)
- In Octopus case, would they consider using the anonymous Octopus card instead of a personalized card or one registered for Octopus rewards (such as the Wellcome rewards). If not, probe to elaborate reasons.
- Refer back to California Fitness - would the PCPD reporting their collection of ID card copies affect their decisions about which fitness company to enrol with (assuming they want some fitness training)?

第一部分　　**PCPD的審查及執法權力**

簡介PCPD的執法權力 (以加州健身中心作為一個例子) **及PCPD可以採取的行動**

- 解釋California Fitness(加州健身中心)的個案情況 –加州健身中心向所有客戶收集身份證副本 ，屬超乎適度，並帶來嚴重的私隱風險。

> 「California Fitness 向申請入會或續會的人士收集超乎適度的個人資料，包括香港身份證副本，侵犯顧客的個人資料私隱。」

- 評估參與者對 PCPD 的角色的認識及期望 (如作為一個獨立的法定機構，根據條例的執法權力，推廣教育的作用; 保障私隱的範圍，即只包括個人資料)
- 了解參與者是否知道不遵守條例的後果，以及他們期望 PCPD 採取什麼行動， 特別是它的司法管轄權只可在香港，並討論有可能的補救措施： 要求道歉？向 PCPD 備案？ 要求金錢賠償？要求停止違反條例規定的行為？
- 了解參與者是否認為目前的監管框架是足以保護他們
- 報告發布 (點名批評是否有效？有注意到公署的新聞發佈會?）

<u>SSRC 的資料</u>

在這種情況下個人資料私隱專員採取的行動

專員向加州健身中心送達執行通知，指令該公司糾正該項違反，及防止該項違反再發生。

簡介直銷及PD(P)O的修訂 以查看他們是否認為修訂已足夠的

- 參與者是否知道直銷商須通知資料當事人將會使用個人資料作直接促銷及取得取同意後, 方可發出促銷信息
- 評估參與者對直銷商的通知 (以獲得同意使用個人資料)的回應情況
- 參與者是否知道直銷商只可促銷資料當事人已同意的/許可的產品及服務類別

- 參與者是否知道直銷商未有取得資料當事人的書面同意下不可提供個人資料予另一人以作直接促銷之用(不論是否得益)
- 評估參與者對拒絕直銷活動權利的認知
- 了解參與者如果不想再收到促銷信息會如何回應直銷商

簡介給資料當事人及個人資料私隱專員公署有關資料外洩事故的通知

「警務處接連遺失載有敏感個人資料的記事冊及「涉嫌犯定額罰款交通罪行的通知書」(俗稱「牛肉乾」)。」
「香港警務處涉嫌經Foxy共享軟件意外洩漏載有市民個人資料的內部文件，例如證人口供。」

- 參與者對於 PCPD 或資料當事人是否需要通知以及應在甚麼時間被通知的期望 (方案是有效地看出他們的想法)

八達通例子－八達通獎賞公司在沒有向客戶提供足夠資訊及取得客戶的同意下，與五個合作商戶共用客戶的個人資料。

「八達通控股有限公司，在營運八達通日日賞計劃時，收集及使用客戶的個人資料，八達通獎賞公司公開承認曾將該計劃的會員個人資料轉移給信諾及另一個參與商戶－Card Protection Plan Limited。」

與『尊重私隱』的機構交易

- 參與者在選擇一個機構提供的服務或產品時，考慮『尊重私隱』的因素有多大的重要性
- 公署會就機構違反私隱條例發表調查報告。參與者會否因此影響與該些機構往來
- 如果個人資料被濫用，參與者會作出乜嘢行動? (e.g.直接聯絡違規者，採取法律行動，停止與該機構交易，作出投訴(包括不作出投訴的原因)，向公眾公開事件，改變交易模式，加強資料保安（例如更改密碼）)
- 在八達通個案中，參與者會否考慮轉用不記名的八達通，以代替個人八達通或已登記八達通日日賞的八達通(例如於惠康購物時賺取優惠) 。如果不會，追問原因。
- 回想 California Fitness(加州健身中心)的個案情況 - 公署公佈他們收集會員的身份證副本會否影響你參加哪一間健身中心／公司的決定（假設參與者想參加健身訓練）?

Part 2 Public registry

Introduce the broader issue of personal data (e.g. name, address, property and car ownership, photos) **that can be found on the Internet** (discuss FB, government registries, Do_No_Evil app) – is it self-published, leaked by friends or available from government registries, to understand

- Do people search information about another person via search engine online (how often? Purpose? For personal interest or work related purpose?)
- Do people expect their personal data to be found by the others using search engine online
- To what extent do people expect their personal data available in the public domain to be used indiscriminately
- How people balance transparency, public interest, and privacy protection
- Do people understand the consequences of being part of a social network – when should we ask peers before posting?

第二部分　　公共註冊

簡介可以在互聯網 (FB的討論區、 政府註冊庫、 『起你底』應用程式)上找到更廣泛的個人資料 (如 姓名、地址、 物業及汽車擁有權、相片) – 這些資料是否自行發佈, 被朋友洩露或可以從政府註冊庫得到，從而了解

- 參與者有否在網上搜尋器尋找其他人的個人資料 (有幾經常? 目的? 個人興趣或工作原因)
- 參與者是否預期他們的個人資料可以在網上被他人在搜尋器找到
- 參與者對於他們的個人資料在公共領域被濫用的期望程度
- 參與者如何平衡透明度，公眾利益和保障私隱
- 參與者是否了解作為一個社交網絡的一部分的後果 – 在發布前，參與者應該在甚麼時候詢問同伴?

Part 3 Privacy tradeoffs

Introduce the question of providing personal data to retailers (online shops, brand names or unknown, local or overseas **and physical shops**, chains and local shops)

- To assess the levels of confidence of people have to protect themselves with online shops and with physical shops (Do people have different attitudes towards them?)
- To what extent people are willing to compromise personal data protection (e.g. email address of their own, family and friends) in exchange for efficiency and convenience online
- Are people willing (to what extent and at what price) to compromise personal data protection (of their own, family and friends) in exchange for benefit and benefit-in-kind (e.g. a chance of gaining a discount, redeeming cash vouchers, convenience of staying in contact)

第三部分 隱私的取捨

簡介在向零售商提供個人資料的問題(網上商店 - 品牌名稱或未知的，本地或海外) 和實體店 - 連鎖 店和本地商店)

- 評估參與者對於網上商店和實體商店保護自己個人資料的信心水平是否有差異
- 參與者為了換取網上的效率和方便而損害保障個人資料 (如自己、家人或朋友的電郵地址)的願意程度
- 參與者是否願意 (到什麼程度及在什麼價格) 損害保障個人資料 (自己、家人及朋友) 以換取好處及任何的利益 (如獲得一個折扣的機會、兌換現金券、方便保持聯絡)

Part 4. Facebook & Mobile Apps

Introduce discussion of privacy settings in FB - do FB users aware, ever check or change privacy settings – if not, why not?)

Introduce mobile apps (e.g. ones for social networking, to find restaurant, ATM nearby) **and what data they collect.**

First discuss Whatsapp/Viber/Line/WeChat (do they have any concern about sharing contacts given that these apps access your whole contact list and how they do they frame the choice in terms of social benefits, sharing contacts of friends and family without other parties consent?)

- **In general, d**o they expect transparency before installation and transparency of what they collect regardless of whether it is personal data (e.g. photos, contacts, location), why the data is being collected or how it would be used.
-
- Do they read and understand the information prior to download (e.g. privacy policies and personal data collection statement)? If not, probe to elaborate reasons (e.g. written in legalese, hard to find those information, too long?)
- Discuss location requests on iOS (e.g. iPhone) and Android (e.g. Samsung) as another example (once and for all, or offer choices and ability to change after installing the app).

Note for SSRC:

	Operations	**Characteristics (for SSRC information only)**
iOS (e.g. iPhone)	Click "download" -> no pop up message -> open the app -> ask for permission to access data -> can choose "allow" or "don't allow"	- Less transparent but more control - Able to change after installing the app
Android (e.g. Samsung)	Pop up message after clicking install -> requesting permissions to different kinds of data (e.g. contact list, album, location) -> click "accept" to download the apps	- More transparent but little control - All-or-nothing

第四部分　**Facebook** 及手機應用程式

簡介Facebook (FB) 的私隱設定及相關的討論 - 了解使用FB的用戶知不知道有私隱設定，有沒有曾經檢示或更改他們的私隱設定，如果他們沒有，為什麼沒有呢？

簡介手機應用程式 (如那些對於那些社交網絡、尋找餐廳、在附近的 ATM) **及他們收集哪些資料**

簡介 Whatsapp/Viber/Line/WeChat

鑑於該些應用程式會讀取電話上所有聯絡人的資料，參與者對於與手機應用程式研發商共享通訊錄有沒有產生任何的憂慮。在沒有得到其他人的同意下分享朋友及家人的聯絡方法，就社交效益，他們會如何作出選擇?

- 一般而言，參與者是否期望安裝前的透明度及他們收集什麼資料無論是否是個人資料的透明度 (如照片、通訊錄、位置)，為何收集資料或如何使用資料
- 參與者有否閱讀及是否明白程式在下載前提供資訊（包括私隱政策及個人資料收集聲明）。如不明白，追問原因（例如使用法律術語、找不到有關資訊、太冗長）
- 討論有關 iOS 和 Android 的位置請求的另一個例子 (一次過, 或提供選擇，同時可以於安裝程式後作改變)

ŧ