PCPD's Submission in response to the
Consultation on Strengthening the Regulation of
Person-to-Person Telemarketing Calls

This submission is made by the Privacy Commissioner for Personal Data ("**PCPD**") in response to the Public Consultation carried out by the Commerce and Economic Development Bureau ("**CEDB**") on Strengthening the Regulation of Person-to-Person Telemarketing Calls in Hong Kong ("**Consultation Paper**") in May 2017.

General Comments

2. One of the main issues highlighted in the Consultation Paper is that the wide and proliferated use of person-to-person ("**P2P**") telemarketing calls and the consequential nuisance have caused public concerns.

3. As the regulator to protect individuals' privacy in relation to personal data under the Personal Data (Privacy) Ordinance (Cap 486) ("**PDPO**"), the PCPD would offer views from the perspective of personal data privacy protection only. The PDPO is principle-based aiming at, *inter alia*, regulating activities involving the collection, holding, processing and use of the personal data by individuals (data subjects) and organisations (data users) in the course of activities including economic and commercial activities. Whether a commercial activity is or should be a normal or lawful activity *per se* is a policy or legal issue which is beyond the remit of the statutory powers of the PCPD. The PDPO

does not prohibit marketing activities but regulate them. It is therefore not the PCPD's position to seek to prohibit marketing activities by P2P telemarketing calls generally. The PCPD is mindful that the proposed regulatory framework should not be inconsistent with the principles and requirements under the PDPO and any other interests of the stakeholders should not be unduly compromised, including those in relation to the free flow of information, information and communication technology and economic development. Given the increased public concerns about the nuisance caused as a result of the proliferation of P2P telemarketing calls, the PCPD supports the Administration in taking steps to strengthen the regulation as detailed in the Consultation Paper.

4. The Consultation Paper sets out 3 possible options to strengthen controls over the conduct of P2P telemarketing calls, i.e. (i) trade specific self-regulatory regime, (ii) call-filtering applications in smartphones, and (iii) statutory regime through setting up a Do-not-call register. As explained in the Consultation Paper, there are pros and cons for each of these three options, and the PCPD acknowledges that it is also important to consider the cost effectiveness in analysing these options in light of overseas experience as well.

5. The PCPD agrees that there is no one or quick fix for the problem. Hence, a multi-pronged problem solving approach should be considered. In gist, the PCPD supports the setting up of a statutory Do-not-call register in the long run, and recommends the implementation of the other two options proposed, as well as other appropriate measures in the interim. Detailed observations and comments on these three options and interim measures are discussed in the ensuing paragraphs.

Specific questions raised in the Consultation Paper

(a) Do you prefer a statutory or non-statutory regime for enhancing the regulation of P2P telemarketing calls?

6. The PCPD submits that a statutory regime for P2P telemarketing calls is ultimately the effective regulatory means, taking into account all factors including deterrence.

Background

7. It is important to note from the outset that P2P telemarketing calls which remain unregulated are mainly those made by telemarketers employing phone numbers randomly generated without using other data of the recipients (which are commonly referred to as "cold calls"). Strictly speaking, most of these cold calls are B2P calls. It is not clear whether B2B calls are also included in this consultation exercise. That said, where personal data is involved, whether in P2P, B2P or B2B calls, the PCPD's observations and comments would apply as appropriate.

8. Currently, electronic commercial messages (e.g. fax, SMS, pre-recorded voice or video telephone calls) sent to phone numbers, fax numbers, and email addresses are already governed by the Unsolicited Electronic Messages Ordinance (Cap 593) ("**UEMO**"). Any individual may register and unsubscribe from unwanted electronic messages. P2P telemarketing calls are nevertheless

not included in the remit of the UEMO which was enacted in 2007. Particularly, Schedule 1 to the UEMO has explicitly excluded P2P telemarketing calls to reflect the then Administration's intent to leave room for legitimate marketing activities in the form of P2P telephone calls, which were then considered as creating limited nuisance as compared with pre-recorded messages[1].

9. The regime introduced under Part 6A of the PDPO in 2013 has tightened up regulation on telemarketing calls made to specified individuals by using their personal data (e.g. phone numbers and names). Telemarketers and organisations hiring them are required to comply with the legal requirements which include taking specified actions[2] (i.e. providing individuals with prescribed information about the intended marketing activities) and obtaining consent before using the personal data for direct marketing purposes[3]. Furthermore, they are required to honour customers' opt-out requests[4]. Failure to comply with the above requirements under the PDPO may attract criminal liabilities[5].

10. Since the implementation of Part 6A of the PDPO in April 2013, the PCPD has received and handled complaints relating to direct marketing approach by telephone calls as follows:-

---

[1] See paragraph 12 of LegCo Paper (LC Paper No. CB(1)1559/06-07) (http://www.legco.gov.hk/yr06-07/english/hc/papers/hc0511cb1-1559-e.pdf)

[2] Section 35C and 35J of the PDPO.

[3] Section 35E and 35K of the PDPO.

[4] Section 35G and 35L of the PDPO.

[5] It is an offence for a data user to use or provide personal data to another person for use in direct marketing without taking the specified actions or obtaining the data subject's consent (section 35C(1) and 35E(1)). An offender is liable on conviction to a maximum fine of HK$500,000 and to imprisonment for 3 years (section 35C(5) and 35E(4)). If the non-compliance relates to the provision of personal data to another person for use in direct marketing for gain, the penalty level is raised to a maximum fine of HK$1,000,000 and to imprisonment for 5 years (section 35J(5) and 35K(4)).

Year	Number of complaints concerning direct marketing by telephone calls	Number of referrals to the Police	Number of convictions*
2013/14	302	12	0
2014/15	186	11	0
2015/16	215	25	3
2016/17	285	101	3
2017/18 (April - May)	20	2	0

*(*6 out of 9 total convictions concerning offences under Part 6A of the PDPO relate to direct marketing calls.)*

11. The majority of the complaints received concerns (i) the banking and insurance sector, (ii) the beauty sector, and (iii) the telecommunications sector.

12. The low conviction figure of the direct marketing offences under Part 6A of the PDPO is attributable to a number of factors. Although the PCPD's referrals to the Police were triggered by the establishment of a *prima facie* case, prosecution of some of these referred cases were not preferred after criminal investigations by the Police. From the PCPD's regulatory experience, many of the complainants cannot ascertain whether their personal data is involved resulting in the evidential difficulties in establishing either a *prima facie* case or conviction. Thus, this type of P2P telemarketing calls (even made by identifiable callers) is beyond the ambit of the PDPO, and there seems to exist a lacuna in the current regulatory regime.

13. The Consultation Paper states that according to the consultancy study commissioned by the CEDB in 2015[6], there were about 7,000 employees in Hong Kong who were directly or indirectly engaged in making P2P telemarketing calls, and that according to the Public Survey (as part of the consultancy study), 10% of those who responded to P2P telemarketing calls had made commercial transactions as a result.

14. It is unclear from the Consultation Paper if the above percentage reflects cold calls only (i.e. P2P telemarketing calls without using personal data of the recipients other than the phone numbers). The PCPD makes no submission on the weight that should be attached to the economic value and benefit of P2P telemarketing calls. Suffice it to say that the study revealed that the percentage of successful deals conducted through P2P telemarketing call had dropped from 21% (in 2008)[7] to 10% (in 2015). Arguably, it reflects a downturn of the economic benefit achieved by such marketing model. Needless to say, the economic benefit (if any) must be properly balanced against the protection of other interests, including the individual's fundamental right of protecting his own personal data privacy.

Option 1 – Strengthening trade specific self-regulatory regime

15. This option relates to the strengthening of tailor-made codes of practice to cope with P2P telemarketing calls by specific trades themselves. As pointed

[6] The study covered both surveys with the general public (Public Survey) and the business sector and industry (Industry Survey) (see pages 5-8 of the Consultation Paper).
[7] See paragraph 20 in LC Paper No.CB(1) 240/09-10(04) for a similar consultancy study conducted in 2008 (http://www.legco.gov.hk/yr09-10/english/panels/itb/papers/itb1109cb1-240-4-e.pdf)

out in the Consultation Paper, the effectiveness of this self-regulatory regime hinges upon the coverage, willingness and commitment of the members of specific trades.

16. It is noted that there seems to be a lack of trade association or strong cohesion in many industries involved in P2P telemarketing calls. The diversified and versatile market features may render this option inherently or structurally inadequate in terms of the coverage. Paragraph 4.6 of the Consultation Paper suggests that trade associations administering the codes of practice should set up and enforce their own sanctions against non-compliant members (e.g. suspension or disqualification of membership, public condemnation, etc.). However, the benchmark Code of Practice on Person-to-Person Marketing Calls (annexed to the Consultation Paper) does not appear to address the consequences and sanctions of non-compliance, and this lack of effective deterrent effect could probably undermine the effectiveness of self-regulation. Self-discipline of members of the trade appears to be a key element for the self-regulatory regime. According to the Consultation Paper, the self-regulatory regime has been implemented since about June 2011, and yet the CEDB's 2015 study also reveals that 96% of the respondents regard P2P telemarketing calls as nuisance and the public aspiration for regulation is still high. In view of these observations and findings, this self-regulatory option alone does not appear to be capable of taking the case of addressing the nuisance further.

17. In addition, this option is premised on customers' initiative to make opt-out requests to telemarketers. Customers have to opt-out one by one,

company by company. This fragmented opt-out requirement is understandably inconvenient and far from satisfactory from a customer's perspective, and the lack of deterrent effect for non-compliance further reduces the customer's readiness and initiative to so opt-out. In view of the similar unsatisfactory outcome of adopting the codes of practice or fragmented registers maintained by specific trades, some overseas jurisdictions have ultimately switched to the establishment of a statutory Do-not-call register.

Option 2 – Improving call-filtering applications in smartphone

18. This option calls for the Administration's collaboration with software companies to improve and promote the wider use of call-filtering applications. The Consultation Paper suggests that funding or other mode of support should be provided to encourage wider usage of such applications which aim to enhance the blockage function by the increased voluntary reporting of telemarketing phone numbers.

19. One of the drawbacks of this proposal is that it is not in a position to deal with P2P telemarketing calls made to fixed line, and many senior citizens still do not use mobile or smartphones. Secondly, as revealed by previous incidents handled by the PCPD, the underlying privacy risks for these call-filtering or tracing applications cannot be underestimated. In general, the privacy concern associated with this sort of applications is the collection and consolidation of the information from the users' phonebooks to form a large database for commercial purpose (e.g. a "reverse look-up" directory) without giving notice to the relevant individuals or obtaining their consent. The

transparency of the personal data handling procedures and privacy policies of these applications are other concerns.

20. In November 2016, three mobile applications (i.e. "Sync.Me", "Truecaller" and "CM Security") with call-blocking function were reported to have collected the contact information from the phonebooks in users' smartphones. The contact information was then consolidated and held on the databases of the developers of the applications for public search. More recently, in mid May 2017, it was widely reported that subscribers may search the phone numbers of identified individuals by the "DU Caller" applications developed in the mainland.

21. Given the commercial value associated with the database compiled by the developers of the applications, the general public's concerns about the mishandling of such databases are valid and real. To gain public trust and confidence in using the call-filtering applications, the extent of the Administration's involvement in the development and operation of the applications may need to be further deliberated. The PCPD considers that encouragement for wider use of call-filtering or tracing functions without adequate, sufficient and effective oversight would not cure the defect or mischief.

Option 3 – Establishing a Do-not-call register

22. The PCPD is of the view that statutory regulation of P2P telemarketing calls by way of establishing a Do-not-call register is the most effective and consumer-friendly option amongst all three options though longer time is

required for legislating and its subsequent setting up. The strengths of this option include (i) offering individuals (data subjects, including customers) with an "one-stop shop" for registering opt-outs for all P2P telemarketing calls orienting from data users (including commercial entities), (ii) sanctioning non-compliance by an appropriate authority, and (iii) increasing the cost-effectiveness of telemarketing by screening out those customers who would not enter into any transactions at the end of day.

23. According to PCPD's regulatory experience, a substantial percentage of the direct marketing cases (15%) relates to failure to honour opt-out requests made to the callers. Moreover, a majority of these "opt-out" cases cannot be pursued further due to the lack of evidence in proving the prior opt-out requests.

24. A regulatory regime substantiated by a centralised Do-not-call register would, in PCPD's view, facilitate the ease of proof and effective enforcement for the relevant regulatory authority administering the proposed Do-not-call register on P2P telemarketing calls.

25. The PCPD acknowledges that a statutorily regulated Do-not-call register is not a panacea, and a basket of solutions may be required to address the problem. As pointed out in paragraph 2.3 of the Consultation Paper, most of the jurisdictions examined[8] by the Administration have established a Do-not-call register to cope with P2P telemarketing calls instead of self-regulation within the specific trade.

[8] These jurisdictions are India, Israel, Japan, Korea, Singapore, Australia, New Zealand, South Africa, the Netherlands, the United Kingdom, Canada, the United States, Argentina, Mainland China, Macau and Taiwan.

Personal or business telephone number

26. In the United States, the National Do-not-call Registry is governed by the Federal Communications Commission and Federal Trade Commission pursuant to the *Telephone Consumer Protection Act of 1991* and the *Telemarketing Consumer Fraud and Abuse Prevention Act of 1994* respectively. Previously, companies were required to maintain their own opt-out lists which were found to be ineffective. The special feature of this centralised U.S. National Do-not-call Registry is that only personal telephone numbers registered under an individual's name can be placed on the National Do-not-call registry[9], which enables solicitation of normal business transactions through telemarketing calls made to numbers registered under the name of a company without causing nuisance to any individuals.

27. This feature is also observed in India's system. The Telecom Regulatory Authority of India has put in place the Telecom Unsolicited Commercial Communications Regulation, 2007 for tracking down the unwanted telemarketing calls. The Regulation was launched after the consultation had been conducted by the Telecom Regulatory Authority on unsolicited commercial communications (in 2006). Prior to that, some banks and service providers in India had instituted their own Do-not-call registers where subscribers could volunteer to sign up. However, this registration system was criticised as fragmented and inconvenient since subscribers had to register with different

[9] §64.1200 of Telecommunication Act (https://www.ecfr.gov/cgi-bin/text-idx?rgn=div6&node=47:3.0.1.1.11.12)

institutions, and not comprehensive as there were telemarketers not connected with such institutions[10].

28. In Singapore, both personal and business phone numbers may be registered, so that business organisations can also opt-out receiving telemarketing calls. Not only may a commercial establishment opt to register its numbers with the Do-not-call register but also give explicit consent to those organisations it prefers for marketing purposes. Like its counterpart in India, the centralised Do-not-call register in Singapore started its operation in 2014 after a public consultation in view of the ineffectiveness of voluntary trade specific guidelines[11].

Entire or Partial blockage

29. Another question is whether P2P telemarketing calls made to all sectors should be blocked once registered with the proposed Do-not-call register, or that flexibility should be allowed for individuals to select the specific industries for the "unsubscribe" provisions to apply (or not to apply). In India, the National Do-not-call Register (known as National Customer Preference Register) is operated by the Telecom Regulatory Authority pursuant to the Indian Telecom Commercial Communications Preference Regulations 2010. Customers are given the choice to block entirely all calls, or to opt for partial blockage specifying the category of industry such as banking/ insurance/ financial

[10] See the Consultation Paper on Unsolicited Commercial Communication dated 20 November 2006 (http://www.trai.gov.in/consultation-paper-unsolicited-commercial-communication).

[11] See paragraph 3.10 of the Public Consultation Issued by Ministry of Information, Communications and the Arts on Framework Details for the Establishment of a National Do-not-call Registry (https://www.mci.gov.sg/public-consultations/public-consultation-items/public-consultation-on-the-proposed-do-not-call-dnc-registry?page=2).

products/ credit cards, real estate, education, health, consumer goods and automobiles, communication/ broadcasting/ entertainment/ IT, tourism and leisure, etc[12]. This feature allows customers to receive information about specific categories of products or services that they are genuinely interested in. It may also increase the chance of successful telemarketing attempts to target customers.

30. Partial blockage will likely increase the operation or administration costs, but it gives flexibility to both the consumers and telemarketers. It has also been suggested by some stakeholders in the telemarketing industry that a flexible approach of this nature should be adopted for the regulatory regime.

Consent and Exemptions

31. Another regulatory model commonly adopted overseas (e.g. Singapore) is to allow registered users to give their subsequent consent to specific organisation(s). Application of the "unsubscribe" provisions will cease if the registered users subsequently give consent, despite the prior registration with the Do-not-call register[13]. There are specific exemptions and organisations that operate in the public interest may also be unsubscribed. For example, a message (including voice call) which is necessary to respond to an emergency that threatens the life, health or safety of any individual, and a message (including voice call) sent for the sole purpose to conduct research or survey are

[12] See Schedule I of the Telecom Commercial Communications Customer Preference Regulations, 2010 (http://www.nccptrai.gov.in/nccpregistry/regulation1diccndiv.pdf).

[13] For the current regime under the UEMO, register users may provide consent to the sending of electronic messages (see section 10 of UEMO).

exempted under the 8th Schedule of the Singapore *Personal Data Protection Act 2012*.

Implementation and Enforcement Issues

32. Paragraphs 5.5 to 5.11 of the Consultation Paper list out a number of implementation and enforcement issues regarding this option which include:-

- Difficulty in collecting evidence and ways to circumvent the regulatory regime (e.g. caller-ID spoofing, VoIP calls from overseas jurisdictions, etc.); and
- Calls originating from overseas jurisdictions.

33. The PCPD notes the difficulties in dealing with cases involving a cross-border or cross-boundary element. The notorious one is that the regulatory regime under the UEMO can only deal with electronic messages with a Hong Kong link[14]. As suggested in paragraph 5.10 of the Consultation Paper,

[14] Section 3 of the UEMO
(1) For the purposes of this Ordinance, a commercial electronic message has a Hong Kong link if, and only if—
(a) the message originates in Hong Kong;
(b) the individual or organization who sent the message or authorized the sending of the message is—
(i) an individual who is physically present in Hong Kong when the message is sent;
(ii) an organization (other than a Hong Kong company) that is carrying on business or activities in Hong Kong when the message is sent; or
(iii) a Hong Kong company;
(c) the telecommunications device that is used to access the message is located in Hong Kong;
(d) the registered user of the electronic address to which the message is sent is—
(i) an individual who is physically present in Hong Kong when the message is accessed; or
(ii) an organization that is carrying on business or activities in Hong Kong when the message is accessed; or
(e) the message is sent to an electronic address that is allocated or assigned by the Authority.
(2) For the purposes of subsection (1)(b), (c), (d) and (e), it is immaterial whether the commercial electronic message originates in Hong Kong or elsewhere.
(3) For the purposes of subsection (1)(b)(iii), it is immaterial whether the commercial electronic message is sent, or is authorized to be sent, from Hong Kong or elsewhere.

the level of cross-border (or cross-boundary) collaboration by law enforcement agencies to cope with P2P telemarketing calls is not the same as the other criminal offences (such as fraud or scams), and it depends on the relevant laws of the overseas jurisdictions. In this regard, consideration may be given to strengthen the interoperability in respect of the relevant enforcement or intelligence sharing through international network. It is noted that the Communications Authority is a member of the Unsolicited Communications Enforcement Network[15]. For international cooperation arrangement, a similar regulatory framework amongst jurisdictions may enhance enforcement and reciprocal assistance.

34. It is generally accepted that there is no silver bullet for all problems. Indeed the above enforcement issues of overseas calls and circumvention methods also exist in the other two non-statutory options. Hence, the implementation and enforcement difficulties of a statutory regime should not be overstated.

(b) If you opt for a statutory regime, do you prefer to have some non-statutory measures in place in the interim (e.g. trade specific self-regulatory regime or call -filtering applications in smartphones)?

35. The PCPD supports the thinking that the three suggested options should not be mutually exclusive. It is indeed worth considering the two non-statutory options (i.e. trade specific self-regulatory regime and call-filtering applications in smartphones) as transitional or interim measures. A multi-pronged problem

[15] For more information on the area of cooperation, please see: https://www.ucenet.org/.

solving approach can only be conducive to protecting personal data privacy in a timely and effective manner.

36. Insofar as the trade specific self-regulatory regime is concerned, the Administration may consider adopting a pragmatic approach in setting the priority of industries for promoting self-regulation. It should also be noted that it has been suggested by legislators during a meeting of the Panel on Information Technology and Broadcasting held on 10 July 2017 that the numbers of complaints concerning P2P telemarketing calls in the beauty and finance sectors are the highest, according to the stakeholders in the fields[16]. The PCPD has issued guidelines/ information leaflets[17] for data protection on these fronts and would stand ready to offer any other assistance that the industries may deem necessary.

Registration of telemarketers, applying specified pre-fix to telemarketers and accredited system

37. Paragraphs 4.31 to 4.36 of the Consultation Paper state that assigning prefixes to telemarketers is considered not feasible for a number of reasons, including (i) new law and registration system for telemarketers will be required for implementation, and (ii) the proposal will generate a higher demand for

[16] The discussion is available at Legislative Council's website: http://www.legco.gov.hk/yr16-17/english/panels/itb/agenda/itb20170710.htm.

[17] See the "*Guidance on the Proper Handling of Customers' Personal Data for the Beauty Industry*" (available at: https://www.pcpd.org.hk//english/resources_centre/publications/files/BeautyIndustry_ENG.pdf); and the "*Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry"* (available at: https://www.pcpd.org.hk//english/resources_centre/publications/files/GN_banking_e.pdf), both issued by the PCPD.

telephone numbers and create adverse impact on the existing 8-digit numbering plan.

38. In the absence of further statistics and related information, the PCPD is not in a position to comment on the high demand for specific telephone numbers and adverse impact on the existing 8-digit numbering plan. It has however been noted that some commentators suggest that the use of the pre-fix "4" in telephone numbers under the existing policy of the office of the Communications Authority is relatively low.

39. Telecommunications service providers in India are imposed with the statutory obligations to assign pre-fixes to telemarketers, and the telemarketers are required to register their names online with the National Telemarketer Register[18]. While a statutory framework takes time, the Administration may consider the feasibility of requesting telecommunications service providers to assign specific pre-fix to telemarketers. The relevant terms and conditions may be included in service contracts to enable the telecommunications service providers to assign pre-fixes to P2P telemarketers who are in demand of high volume call services. This measure offers a wide coverage over telemarketers for different industries and trade, and the Administration is invited to further explore this as an interim measure.

40. To encourage telemarketers to be compliant, an accreditation or certification system may also be set up in the telemarketing industry to

[18] See Chapter III and Schedule III of the Telecom Commercial Communications Customer Preference Regulations, 2010 (http://www.nccptrai.gov.in/nccpregistry/regulation1diccndiv.pdf).

demonstrate their good track record on their compliance with the code of practice and its strategy regarding personal data privacy protection (e.g. in honouring customers' opt out requests).

(c) Other suggestions

(i) The proposed statutory regime to be implemented under the UEMO

41. There is little doubt that a user-friendly statutory framework for a Do-not-call register will be welcomed by the data subjects. At present, the office of the Communications Authority administers and enforces the Do-not-call registers for unsolicited electronic messages under the UEMO, and it would seem to be more straight-forward and less confusing for the P2P telemarketing calls recipients to apply to the same regulatory authority for registration for the nuisance calls. Furthermore, with the current Do-not-call registers under the UEMO, to expand the scope to include P2P telemarketing calls rather than setting up a new regulatory scheme whether under the PDPO or a specific legislation would seem to have relatively less resources implication.

42. During the legislative stage of the UEMO, the Administration once pointed out that if it was decided in future to bring P2P telemarketing calls into the ambit of the UEMO, such decision could be effected expeditiously under clause 6 of the then Bill (i.e. the current section 7 of the UEMO) by amending Schedule 1 by way of publishing a notice in the gazette, it being a subsidiary

legislation subject to the scrutiny of the Legislative Council[19]. In this regard, the Administration may review the situation and adopt the most appropriate approach in effecting legislative amendment.

(ii) The proposed statutory regime to be included in the PDPO

43. The PDPO was enacted to protect the privacy of individual's personal data. Since the majority of P2P telemarketing calls, such as cold calls without mentioning the name of the recipients, do not involve the recipients' personal data within the definition of the legislation, amendment to the PDPO is required to give effect to the intention of including P2P telemarketing calls in the protection net, given that the calls inevitably involve a contact number of the recipients and link to the recipients. It will naturally take time to complete the legislative process[20].

44. If the policy decision is to have the PCPD charged with the regulatory responsibility for the proposed Do-not-call register, the PCPD would also seek to strengthen the sanctioning power of the PCPD so as to enhance the effectiveness of enforcement. As indicated in the preceding paragraphs, there are few successful convictions for the offences under the direct marketing provisions in Part 6A of the PDPO. Out of the 9 convictions so far, the highest fine imposed was HK$30,000, the penalty level having been raised in April 2013 to a maximum fine of HK$1,000,000 and an imprisonment for 5 years where the

[19] See paragraph 12 of LegCo Paper (LC Paper No. CB(1)1559/06-07) (http://www.legco.gov.hk/yr06-07/english/hc/papers/hc0511cb1-1559-e.pdf)

[20] In this regard, it is noted that the Singapore *Personal Data Protection Act 2012* provides a separate and distinct part on Do-not-call register. The purpose of the Act is described as *"an Act to govern the collection, use and disclosure of personal data by organisations, and to establish Do Not Call Register and to provide for its administration, and for matters connected therewith…."*

non-compliance relates to the provision of personal data to another person for use in direct marketing for gain.

45. To give effect to deterrence in light of the gravity and prevalence of the nuisance calls as highlighted in paragraph 1.14 of the Consultation Paper, the PCPD would revive his previous proposal of empowering him to impose administrative fines on data users for serious contraventions of the PDPO[21]. One main advantage is that even if no affected victims are willing to go through a criminal trial, the PCPD may still take into account the overall practice of an offending party making P2P telemarketing calls and the total number of affected individuals when deciding the proper and appropriate monetary penalty independent of court procedure. Imposing administrative fines by regulatory authorities is not novel in Hong Kong. Some statutory bodies such as the Hong Kong Monetary Authority, the Securities and Futures Commission, the Mandatory Provident Fund Schemes Authority and the Insurance Authority are also empowered to impose monetary penalties administratively[22].

46. Imposing administrative fines by data protection authorities is not uncommon in other jurisdictions either. It is noted that the European Union's General Data Protection Regulation (which will take effect from 25 May 2018) empowers European Union's data protection authorities to impose increased administrative fines on data users or controllers and processors for contravention

[21] The PCPD made this proposal in the last ordinance review exercise in 2010. For details, please see paragraphs 9.1 to 9.10 under Proposal 39 of the PCPD's Submission in response to the "Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance" at: https://www.pcpd.org.hk/english/enforcement/response/files/PCPD_submission_311210.pdf

[22] See section 203A of the Securities and Futures Ordinance (Cap 571); sections 194 and 196 of the Securities and Futures Ordinance (Cap 571); section 34ZW of the Mandatory Provident Fund Schemes Ordinance (Cap 485); and section 41P of the Insurance Ordinance (Cap 41).

of the regulations. A fine with upper level as high as €20 million (roughly HK$160 million) or 4% of the total worldwide annual turnover of preceding financial year million, whichever is higher, is set to be enforced in all member states of the European Union[23]. Currently, some data protection authorities in common law jurisdictions such as the United Kingdom Information Commissioner and the Singapore Personal Data Privacy Commissioner are already vested with the power to impose administrative fines. For example, in March 2017, the United Kingdom Information Commissioner imposed a monetary penalty of £270,000 (roughly HK$2.45 million) on a company that made 22 million nuisance calls[24].

(iii) Building up a culture of protecting and respecting personal data privacy through education, promotion and Privacy Management Programme

47. Education and promotion are no less important than enforcement in addressing the problems arising from the nuisance caused by P2P telemarketing calls. The PCPD believes that education and promotion will help increase awareness and understanding of the existing and proposed regulatory framework with a view to building up a culture to protect and respect personal data privacy.

48. The PCPD also advocates the adoption by data users of a proactive strategy, the Privacy Management Programme ("**PMP**"), which aims to help the data users manage privacy and data protection responsibly and demonstrate their commitment to good corporate governance.

---

[23] See Article 83 of the European Union's General Data Protection Regulation.
[24] See the details from ICO's website: https://ico.org.uk/action-weve-taken/enforcement/media-tactics-ltd-mpn/.

49. PMP serves as a strategic framework to assist an organisation in constructing a robust privacy infrastructure and service designs, supported by on-going reviews and monitoring process to facilitate compliance with the requirements under the PDPO. It involves top management's commitment to ensure that data privacy is built in by design for all policies, initiatives, programmes and services. Details of the draft PMP are set out in the "*Privacy Management Programme: A Best Practice Guide*" issued by the PCPD[25]. It is planned that the finalised PMP, with the relevant guidance and toolkits, will be made available for public adoption upon the conclusion of a consultancy report and pilot test conducted in selective governmental organisations in the near future.

Conclusion

50. The PCPD fully appreciates that complex issues are involved in abating the nuisance caused by unwanted P2P telemarketing calls, which can only be addressed with determination and efforts on the part of all stakeholders.

51. The nuisance has persisted for quite some time not only in Hong Kong but also other jurisdictions. The general consensus seems that the problem should be addressed and any lacuna or loopholes in the relevant laws and regulatory frameworks should be plugged properly without delay. The concerns of P2P telemarketing calls relate to whether those receiving the calls (cold calls

[25] See the "*Privacy Management Programme: A Best Practice Guide*" issued by the PCPD (available at: http://www.pcpd.org.hk/english/resources_centre/publications/files/PMP_guide_e.pdf).

included) are in a position to keep their own personal data (personal contact numbers included) under their own control, and their wish not to receive the calls are respected. Invariably, it is a matter of notification and consent, transparency and trust. Direct marketing activities involving personal data not being banned but regulated, the PCPD remains mindful that P2P telemarketing calls should be regulated without unduly compromising the economic contribution the telemarketing industry may make. It is essentially a balancing exercise between the protection of one's own personal data in terms of contact number and the legitimate use of personal data by others in the interest of economic, information and communications technology development. The proposed establishment of a new Do-not-call register seems to satisfy the proportionality test by giving individuals (data subjects) the option to stop the organisations (data users or controllers) from using their contact numbers in promoting goods and services even though their other personal data (such as names) are not involved. Establishing such a register by legislation clearly ensures certainty, clarity and deterrence, particularly with the inclusion of administrative fines. Restoring the proposed register back to the existing UEMO Do-not-call framework has its own advantages but the PCPD is well poised to take it up as and when the Administration deems proper and appropriate.

52. The advantages of the other two options proposed to address the problem of unwanted nuisance P2P telemarketing calls (i.e. strengthening trade specific self-regulatory regime and imposing call-filtering applications in smartphone) seem to be outweighed by their structural and technical weaknesses, their lack of comprehensiveness and effectiveness, as well as current and potential privacy risks. That said, they should be capable of serving as interim

or transitional measures until the new statutory Do-not-call register is put in place ultimately.

53. In addition to supporting the establishment of a new statutory Do-not-call register for P2P telemarketing calls, the PCPD remains duty bound to continue to educate and promote awareness and understanding of personal data privacy protection laws and framework including those relating to the P2P telemarketing calls amongst all stakeholders (data subjects and data users), and the adoption of PMP as and when it is ready to be launched. Interoperability with overseas data protection authorities in tackling cross-border or cross-boundary data issues (P2P telemarketing calls included) will continue to be strengthened, too.

The Privacy Commissioner for Personal Data, Hong Kong
July 2017