Submission in response to
Public Consultation on 2014 Digital 21 Strategy

Chapter 1: A Sound Foundation

By definition, realisation of the potential of ICT depends on the collection, management and use of data, including personal data. As some put it, personal data will be the new "oil" – a valuable resource of the 21st century. It will emerge as a new asset class touching upon all aspects of society and business.

2. Hence, whilst the Privacy Commissioner for Personal Data ("PCPD") supports that Hong Kong has to embrace the next wave of ICT advancements and apply them in powering our economic and social development, we consider that in the process, the Government and all other stakeholders must also embrace privacy and data protection.

3. Privacy is a fundamental human right protected under the Basic Law. At the minimum, the requirements under the Personal Data (Privacy) Ordinance (the "PDPO"), a technology-neutral legislation, must be complied with in the use of ICT by all "data users" (i.e. persons who control the collection, holding, processing or use of personal data). In particular, the six Data Protection Principles ("DPPs")[1] must be adhered to. They govern the fair and lawful collection of personal data (DPP1); accuracy and retention of data (DPP2); use of data (DPP3); data security (DPP4); openness of personal data policies (DPP5); and right of persons who are the subjects of the personal data ("data subjects") as regards data access and correction (DPP6).

Chapter 2: Smarter Hong Kong, Smarter Living

4. Whilst the intelligent use of ICT holds great promise for enriching the quality of life and enhances productivity, consumer privacy and data security must remain a priority.

[1] Provisions of the six DPPs are found in Schedule 1 of the PDPO

5. High-profile data breaches and missteps involving personal data seem to be reported almost daily by the media. This trend must be reversed in order to restore consumer trust in the personal data ecosystem and to reap the maximum benefits of the advances in ICT. It calls for enhanced accountability and responsibility on the part of data users in collecting personal data, and protecting and securing it against intentional and unintentional security breach and misuse.

6. To this end, data users should have in place a privacy management programme[2] that:-

(a) has top management commitment and is integrated into the organisation's governance structure;
(b) establishes policies and procedures giving effect to the DPPs;
(c) provides for appropriate safeguards based on privacy risk assessment;
(d) includes plans for responding to breach and incident; and
(e) incorporates internal oversight and review mechanisms.

7. The process of privacy risk assessment involves identifying, analysing and evaluating the risks to individuals' privacy. This is sometimes accomplished by conducting a "privacy impact assessment"[3] before a new programme or technology is introduced or when the context of the data use has changed significantly.

8. The PCPD advocates that privacy should be embedded into the design specifications of various technologies so that safeguards are built into system architectures, rather than added on later as an afterthought. This "Privacy by Design" approach requires privacy concerns to be addressed when developing information technologies and systems, throughout the entire information life cycle.

[2] The PCPD will issue in early 2014 a Best Practice Guide for implementing privacy management programmes modelled on the document "Getting Accountability Right with a Privacy Management Program" (April 2012) compiled by the Office of the Privacy Commissioner of Canada, and the Offices of the Information & Privacy Commissioners of Alberta and British Columbia, Canada available at www.oipc.bc.ca/guidance-documents/1435

[3] For a detailed explanation on privacy impact assessment, please refer to "Information Leaflet on Privacy Impact Assessments" issued by the PCPD, available at www.pcpd.org.hk/english/publications/files/PIAleaflet_e.pdf

9. The four enabling technologies mentioned in the new edition of the Digital 21 strategy have specific privacy and security concerns of their own.

10. **Cloud computing** technology involves outsourcing of personal data processing and operation which may span across multiple jurisdictions. Some persons other than the data user become the caretaker of the underlying data that have been fed into a given application, thus posing the risk of loss of control by the data user over the data[4]. Section 33 of PDPO requires data users to take all reasonable precautions and exercise all due diligence to ensure that cloud providers operating outside Hong Kong shall offer protection to the personal data to a level which is commensurate with that required under PDPO in Hong Kong. Although this provision has yet to come into effect, DPP2 requires data users to adopt contractual or other means to prevent any personal data transferred to the data processor (local or overseas) from being kept longer than is necessary for processing of the data. Further, DPP4 requires data users to adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor (local or overseas) for processing[5] .

11. **Big data analytics** can be highly privacy-intrusive to individuals as conclusions are drawn about their preferences, activities, associations or even health status, which may in turn lead to decisions being made about them, without their knowledge or agreement. One of the more well-known "creepy" examples concerns the US retail giant Target who analyses the purchasing habits of its customers and is able to predict reliably whether a female customer is pregnant and by how many months. It caused great embarrassment when the father of a teenage girl found out that she was pregnant following suspicions about the increase of pregnancy-related advertisements from Target arriving in the mail. That Target has "data-mined" its way into the customer's womb is clearly an

[4] For an exposition of the privacy and security concerns, see the PCPD's "Information Leaflet on Cloud Computing" available at www.pcpd.org.hk/english/publications/files/cloud_computing_e.pdf

[5] For an explanation of the requirements, see "Information Leaflet on Outsourcing the Processing of Personal Data to Data Processors" issued by the PCPD and available at www.pcpd.org.hk/english/publications/files/dataprocessors_e.pdf

act beyond the reasonable privacy expectation of its customers[6]. If not handled properly, big data could end up in a backlash, as exemplified by the debate around the recently proposed European legislation that includes a "right to be forgotten" that is aimed at helping individuals better manage data protection risks online by requiring data users to delete their data if there are no legitimate grounds for retaining it.

12. **Internet of Things** also have privacy implications depending on the use of the data collected and the security of the wireless transmission of the data, including the risk of unauthorized third-party interception. For example, individuals may not always be aware of Radio Frequency Identification ("RFID") tags that are embedded in products they buy. These tags, when linked to personally identifiable information, present the prospect of privacy-intrusive practices relating to the tracking and surveillance of individuals' activities.

13. **Wireless and multi-platform** technologies centre on the pervasive use of mobile devices in conjunction with the Internet. They present new privacy and security challenges. As a mobile device is likely to be 'always on' and rarely parted from its owner, it generates geo-location data which provides for the potential for comprehensive surveillance of the user. When combined with data on what the user does and thinks, detailed insights into the user's private life can be gained. One set of privacy issues in this regard concerns the collection, use and storage of location data by mobile phone companies, mobile apps developers and other players in the mobile ecosystem who are authorised to know the location of the device in order to provide mobile service[7]. Presenting effective privacy notice to the users and obtaining their consent to the use

[6] For guidance on collection of personal data through the Internet and tracking the data subject's online behaviours, data users may refer to "Information Leaflet on Online Behavioural Tracking" and "Guidance for Data User on the Collection and Use of Personal Data through the Internet" issued by the PCPD available at www.pcpd.org.hk/english/publications/files/online_tracking_e.pdf and www.pcpd.org.hk/english/publications/files/guidance_internet_e.pdf respectively.

[7] For guidance in this area, see the document "Personal Data Privacy Protection: What Mobile Apps Developers and Their Clients Should Know" issued by the PCPD, available at www.pcpd.org.hk/english/publications/files/apps_developers_e.pdf

of their data pose unique challenges on smartphone screens, which are typically much smaller than the screens for desktops or laptops[8].

Chapter 3: Empowering Everyone

14. The PCPD agrees that to harness the potentials presented by ICT, the Hong Kong community needs to have the basic skills and confidence to use technology, and have easy access to it. At the same time, there is a need to create a culture of privacy among organisations and individuals through implementation of privacy literacy initiatives.

15. The Hong Kong population's privacy awareness in recent years is known to be high. In May 2012, 84% of Hong Kong people surveyed by a technology firm indicated that they were 'very concerned' or 'extremely concerned' about unauthorised access to, or misuse of, their personal data[9]. However, in a survey [10]conducted by the PCPD in July 2012, it was revealed that smartphone users were pretty lax in managing, controlling or protecting the personal data on their smartphones:-

- Over 90% of users have installed apps but only 27% of them read and consider the apps privacy policy before installing the apps;
- 57% of apps users do not know what personal data on their phones are accessed by the apps installed;
- 51% of social network apps users do not know that their contacts and social relationship data would be uploaded to a central server;
- Only 53% of users take steps to protect their phones and personal data by means such as screen lock and anti-virus software.

[8] The PCPD conducted in May 2013 a survey of 60 smartphone apps developed by Hong Kong entities and found that their transparency in terms of privacy policy was generally inadequate. Only 60% of the apps provided Privacy Policy Statements and most of them did not explain what smartphone data they would access and the purposes for the access. For details, see study at www.pcpd.org.hk/english/publications/files/mobile_app_sweep_e.pdf. For guidance to data users, see "Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement" issued by the PCPD (www.pcpd.org.hk/english/publications/files/GN_picspps_e.pdf)

[9] Unisys survey in 2012; the corresponding figures in 2011, 2010 and 2009 are 85%, 81% and 82% respectively

[10] Full survey report can be downloaded from :
www.pcpd.org.hk/english/publications/files/smartphone_survey_e.pdf;
Executive Summary of the report can be downloaded from :
www.pcpd.org.hk/english/publications/files/smartphone_survey_ex_sum_e.pdf

16. Further analysis revealed that the youngest smartphone users (ages 15-20) were the most active users but they were the least concerned or vigilant when it came to privacy and data protection.

17. Equally disappointing are the results of a compliance check conducted by PCPD in 2012 which unearthed inadvertent online exposure of sensitive personal information of students (including Hong Kong identity card number and birth certificate number) that could be used for fraudulent ends. The personal information of as many as 8,505 students of 11 local educational institutions, including tertiary institutions, could be compromised as a result of the data breach[11]. This is cause for alarm. Bearing in mind that the PCPD had only spent limited time in this exercise of Internet search based on some crude means, the extent of the cyber security problem identified is disproportionate. It reflected a serious lack of vigilance and adequate security measure on the part of the educational institutions in safeguarding personal data.

18. All these findings call for the need to embark on programmes of privacy education and awareness enhancement, particularly in relation to the knowledge and skills necessary for the data subjects to stay safe online and use ICT to their benefit. Such initiatives are being undertaken by the PCPD but should also involve a wide range of stakeholders, including the Government, self-regulatory bodies, civil society organisations, and educators.

Chapter 4: Igniting Business Innovation

19. The PCPD agrees that the tertiary education sector is the major driver of Hong Kong's technology innovation. It is therefore appropriate to incorporate privacy and data protection modules in the academic programmes of universities and other tertiary institutions.

20. Business innovations should of course be promoted but they must not lose sight of privacy and data protection. The concepts of Privacy

[11] For more details, see media release at www.pcpd.org.hk/english/infocentre/press_20130115_4.html

Impact Assessment and Privacy by Design, as explained in paragraphs (7) and (8) above, must be embraced by default.

21. In promoting Public Sector Information for free re-use, the Government should take note that personal data available in the public domain, including those in public registers, are still subject to regulation under the PDPO[12]. In particular, DPP3 provides that personal data should be used only for the purposes for which it was collected or a directly related purpose, unless the express and voluntary consent of the data subject is obtained. Ideally, the purpose and limitations of use of information in the public domain are spelled out to avoid doubt on their re-use. For example, in the case of public registers, the original purpose of collecting and making public the personal data in the registers could be stated as specifically as practicable in the enabling legislation. Where it is necessary to ascertain whether the reuse of such data is for the same purpose or a directly related purpose, we need to consider the specific context in which the data was collected and the reasonable expectations of the data subjects as to the further use made of the data based on that context[13].

22. It is worth pointing out that anonymisation and de-identification techniques may be adopted as means to enable prolonged retention, repurposing and/or analytics of personal data in the public domain, while at the same time preserving privacy. Over the past decade, however, it has become clear that not all anonymisation and de-identification techniques are equally robust. As a result, the use of these techniques to eliminate privacy risks is increasingly questioned.

23. As regards the proposal to make all Government information released for public consumption machine-readable by default, we have grave reservations if it applies to personal data also. Instead, the Government should restrict massive download of personal data from Government sources, as it would facilitate the aggregation, re-arranging

[12] For quick reference, please refer to the PCPD article entitled "Drawing the line: Differentiating between Access to Public Domain Information and Protection of Personal Data", available at www.pcpd.org.hk/english/infocentre/files/201310_hklawyer_e.pdf.

[13] Please refer to "Guidance on the Use of Personal Data Obtained from the Public Domain" issued by the PCPD available at www.pcpd.org.hk/english/publications/files/GN_public_domain_e.pdf

and matching of such data, resulting in a function creep, that is, use of the data by subsequent data users for a new purpose.

Chapter 5: Supporting a Thriving ICT Industry

24. The PCPD supports the Government's strategy to support a thriving ICT industry. Privacy education should be a key component in the process.

25. For example, the online portal to be set up by OGCIO to support tech startups should contain practical business and legal tips on privacy and data protection so that the startups could address with confidence privacy expectations of data subjects and compliance obligations under PDPO[14]. In developing an ICT professional recognition framework, OGCIO should recognise that privacy is a burgeoning discipline, and include privacy management and data protection as part of the required skills and capabilities for ICT professionals.

26. In promoting best practices in the development of multi-platform apps, the Government should take special note of the unique privacy challenges presented by mobile devices, as explained in paragraph (13) above.

27. In promoting and building Hong Kong as a data centre and a leader in the management of cloud services, the Government should address the privacy issues of cross-border data flows, as outlined in paragraph (10) above[15]. In particular, in strengthening Hong Kong's ICT collaboration with the Mainland, the Government should note that the Mainland does not have legislation that provides for universal data protection and hence, under section 33 of PDPO (yet to be implemented), severe restrictions will apply in the transfer of personal data from Hong Kong to the Mainland.

[14] Apart from the privacy guidelines issued by the PCPD, startups may refer to "A Practical Guide for IT Managers and Professionals on the Personal Data (Privacy) Ordinance" issued by the Hong Kong Computer Society.

[15] Cross-border data privacy issues in the Asia-Pacific region are being addressed by a Data Privacy Subgroup (DPS) of Asia-Pacific Economic Cooperation's Electronic Commerce Steering Group. Hong Kong, China is a member of the DPS.

Chapter 6: Transforming and Integrating Public Services

28. The PCPD welcomes the Government to take the lead in capitalising ICTs to provide convenient and efficient services to the public. To ensure success in this regard, the Government should also take the lead in supporting and implementing privacy management programmes (referred to in paragraph (6) above) in all bureaux and departments[16]

Concluding Remarks

29. From a privacy perspective, ICTs are essentially neutral. What matters are the choices we make when designing and using them. They can be privacy-intrusive or privacy-enhancing. Privacy-enhancing technologies respect privacy, embody DPPs and empower individuals.

30. Adding privacy to information technologies and systems should not require subtracting security, usability, efficiency, organisational control or other desirable functions or attributes. The belief that privacy requires trade-offs is a false dichotomy. Rather, it promotes consumer trust and confidence, and thereby achieves positive-sum, win-win results.

31. Resource-permitting, the PCPD stands ready to assist the Government and other stakeholders to reach this goal through a privacy-respecting adoption of the 2014 Digital 21 Strategy.

Office of the Privacy Commissioner for Personal Data
30 November 2013

[16] The PCPD wrote to the Secretary for Constitutional and Mainland Affairs on 19 December 2012 to seek the Government's pledge to support and implement Privacy Management Programmes, and a definitive response is awaited.