

Response to the Result of the Government's Review of the Personal Data (Privacy) Ordinance

1. **Internet Society Hong Kong (ISOC-HK)** would like to take this opportunity to respond to the legislative proposals on the review of the Personal Data (Privacy) Ordinance (PDPO). We believe that any proposal to amend the legislation must take note of the changing technological environment and the need for balance between safeguarding personal data privacy and facilitating continued development of information and communications technology.

Sensitive Personal Data

Proposal No. 1: Sensitive Personal Data

2. We do not support to differentiate “sensitive” personal data at this stage, because we do not believe any such “more stringent regulation of sensitive personal data” would result in a higher level of protection, and we find the Government's proposed classification of, or indeed the singling out of, biometric data is problematic and unreasonable.
3. Although, as the consultation paper previously indicates, biometric data are “unchangeable,” and “the harm caused to an individual is substantial in any biometric system security failure,” we believe that these factors should not be the sole or primary considerations in determining what may constitute “sensitive data.” Instead, as other jurisdictions normally include “racial or ethnic origin, political opinion, religious or philosophical beliefs, membership of trade unions, health condition, and sexual life.... (and) criminal records” as sensitive personal data, we believe the “effect” of such data being made known without consent of the data subject is vastly more important than whether these data are unchangeable or not.
4. It is also noted by the information technology industry that such singling out of biometric data – which is hardly an international norm by any measure – has already sent a chilling effect over the use of such technology, which runs against one of the guiding principles of the consultation, that of seeking a balance of privacy protection with the development of ICT.
5. We believe at the current stage our legislative priorities should be to strengthen enforcement for *all* personal data protection, instead of singling out one type of data for “more stringent regulation,” especially given the very dubious reasoning for such classification. Further consultation is necessary to consider the future implementation of a more stringent regime for sensitive personal data.

Data Security

Proposal No. 2: Regulation of Data Processors and Sub-contracting Activities

6. The definition of data processing and the classification of data processors can be cover a

wide range of activities and players such as software developers and testers, Internet service providers (ISPs), online service providers (OSPs), web hosting service providers, software-as-a-service providers, or even social media. Direct regulation on such a wide range of data processor companies, some of them possibly being overseas, may prove to be difficult to define and execute.

7. We are concerned about the effects of direct regulation on Internet-related businesses, as “such data processors typically have no knowledge of whether the data they are holding are personal data.” As the consultation paper previously properly points out, “compliance...may frustrate free flow of information on the Internet.”
8. We believe that the option of indirect regulation would be sufficient, “as a first step,” to provide the means for redress for the data subject against the data user when necessary, but striking a balance with the nature of Internet-related business and the free flow of information.

Proposal No. 3: Personal Data Security Breach Notification

9. Over the past few years, it is evident that “privacy breach notification” has become part of the expectation held by the public, at least on some of our major institutions, such as those holding our “sensitive” (generally speaking) personal data, such as our financial or health data. Indeed, some would consider the right to be informed of personal data breach to be a “human right,” and notification is also essential for the data subject victim to mitigate the damage.
10. Under a mandatory notification requirement, we are concerned that a purely voluntary system may not provide significant incentives for businesses or institutions to give notifications voluntarily. We are uncertain about the effectiveness of the proposed notification mechanism, and are not confident that data users can make their own call impartially on whether a data breach “may result in a high risk of significant harm to individuals or organizations.” There is currently insufficient guidelines or criteria to help data users to decide whether a data breach should be reported or not.
11. We believe that there are significant overseas experience to make references of for establishing a mandatory privacy breach notification regime for certain kinds of breaches and certain types of institutions, first, such as Government and public institutions, critical infrastructure or regulated utilities, financial and educational institutions. This way, we can accumulate regulatory experience within regulated industry, before rolling out the full mandatory notification to all data users.
12. We also propose that a database of privacy data breaches to be maintained by the PCPD for a period of at least seven (7) years, for the public to search and be informed about the privacy performance of various organizations.

Enforcement Powers of the PCPD

Proposal No. 4: Granting Criminal Investigation and Prosecution Power to the PCPD

13. We believe more consultation is needed before granting criminal investigation and prosecution power to the PCPD, as there is justified concern about the same body holding the dual roles and powers of being the regulator, investigator and prosecutor all at the same time.

Proposal No. 5: Legal Assistance to Data Subjects under Section 66

14. In principle, we agree with the proposal to allow the PCPD to be given the power to provide legal assistance to the aggrieved data subject, as it is common that an average aggrieved citizen would find it difficult to pursue costly legal proceedings. However, we also believe that conditions should be imposed on the granting of such assistance, such as, similar to the case of the Equal Opportunities Commission (EOC), if the case raises a question of principle, and if the case is a representative case with public interest.
15. However, we are also concerned about the possible effects of such actions taken against ISPs and OSPs, which merely provide the conduits (as a common carrier) or the open platform for Internet users' expressions. Any frivolous action may deter the free flow of information and cause detrimental effects on the freedom of expression. Hence, we propose that a clear set of guidelines be established to "regulate" the scope of enforcement of the PCPD, especially over cases that may involve the freedom of expression in an open forum.

Proposal No. 6: Award Compensation to Aggrieved Data Subjects

16. We agree with the Legal Reform Commission's view that the combination of enforcement and punitive functions vested in a single authority is undesirable. We agree that it should be left for a court to determine the amount of compensation to the data subjects.

Offences and Sanctions

Proposal No. 7: Making Contravention of a Data Protection Principle an Offence

17. We believe making such contravention of the broad data protection principles an offence would cause turmoil and confusion, as "DPPs are couched in general terms and can be subject to a wide range of interpretations," and may "have significant impact on civil liberties if an inadvertent act or omission could attract criminal liability." Therefore we do not believe we should make the contravention of a DPP an offence at the present moment.

Proposal No. 8: Unauthorized Obtaining, Disclosure and Sale of Personal Data

18. We agree in principle to make it an offence if a person "knowingly or recklessly obtained the personal data without the consent of the data user and discloses the personal data so obtained for profits or malicious purposes." However, we believe clear guidelines must be issued to the public, as the behaviors of many Internet users are currently accustomed to may come very close to entering an offence.

Proposal No. 9: Repeated Contravention of a Data Protection Principle on Same Facts

19. We agree that it is appropriate to make it an offence for a data user, who having complied with the directions in an enforcement notice to the satisfaction of the PCPD, subsequently intentionally does the same act or engages in the same practice for which the PCPD had previously issued an enforcement notice. Heavier sanctions should also be placed upon a repeat offender.
20. Currently the PCPD can only issue enforcement notice to a party when data breach occurs and if the PCPD considers the party will repeat the abuse. This is a very limited power. We propose the Privacy Commissioner be granted the right to serve an enforcement notice when a breach is occurred.

Proposal No. 10: Imposing Monetary Penalty on Serious Contravention of Data Protection Principles

21. We agree that instead of empowering the PCPD to require data users to pay monetary penalty, it is more appropriate to consider singling out particular acts or practices of contravention of DPPs of a serious nature and making them an offence.

Proposal No. 11: Repeated Non-compliance with Enforcement Notice

22. We support imposing a heavier sanction for data users who repeatedly contravene an enforcement notice.

Proposal No. 12: Raising Penalty for Misuse of Personal Data in Direct Marketing

23. We support raising the penalty level for misusing personal data in direct marketing.

Territorial Scope of the Ordinance

24. The PDPO currently has not enacted Section 33 to order data users to take all reasonable precautions and to exercise all due diligence to ensure that the personal data will not be collected, held, processed or used in a place outside Hong Kong in any manner which, if that place were Hong Kong, would be contravention of a requirement under the Ordinance.
25. We believe that the PDPO should be on par with international standard, such that it should enact Section 33, to comply with, for instance, the European Union requirement and OECD guidelines. This compliance is vital for Hong Kong to remain competitive and allow outsourcing business to be competitive internationally by providing trust with legal protection.

About Us

24. Internet Society Hong Kong (ISOC-HK) is the local chapter of the Internet Society (ISOC), the global organization of Internet users and professionals, providing leadership in issues confronting the future of the Internet, including global coordination, development and

cooperation of the Internet, technology standards, Internet governance and online civil society.

Internet Society Hong Kong
2010.12.31