

Our Ref.: PCPD(O) 115/156 pt. 17

1 March 2012

By Email (co_consultation@cedb.gov.hk) and Post

Assistant Secretary for Commerce and Economic Development
(Commerce and Industry) 3A
Commerce, Industry and Tourism Branch
Commerce and Economic Development Bureau
23/F, West Wing, Central Government Offices,
2 Tim Mei Avenue, Tamar,
Hong Kong

Attn: Mr. Paul Wong

Dear Paul,

**Public Consultation on the Second Draft of
the Code of Practice for Online Service Providers**

Thank you for your email dated 31 January 2012 inviting our submissions on the Second Draft of the Code of Practice (“**Second Draft**”) for Online Service Providers (“**OSPs**”).

2. First of all, please note that this Office is an independent statutory body established to oversee and enforce compliance with the Personal Data (Privacy) Ordinance (“**Ordinance**”). Therefore, our submissions are made solely from the perspective of protecting personal data privacy.

3. We understand that the Copyright (Amendment) Bill 2011 has

introduced a statutory “safe harbour” for OSPs so that their potential liability for copyright infringement occurring on their service platforms would be limited, provided that the OSPs meet certain prescribed conditions. To tie in with the introduction of the “safe harbour”, a non-statutory Code of Practice will be formulated to set out practical guidance and procedures for OSPs to follow when they are notified of infringing activities on their service platforms. The Code will also sets out the procedures for copyright owners to serve notices of alleged infringement and for subscribers to serve counter notices. We have previously provided our comments on the proposals under the Copyright (Amendment) Bill and the first draft of the Code of Practice.

4. We now set out our submissions on the Second Draft.

Collection of personal data

5. Under section 88C of the Copyright (Amendment) Bill, a complainant/copyright owner can send a notice of alleged infringement (“**Notice**”) to an OSP in case an infringement has occurred on the OSP’s service platform, where according to Form A in the Annex to the Second Draft, the person furnishing the Notice must provide particulars such as the name, address, telephone number etc.. On receiving the Notice, the OSP should send a copy of the Notice to the subscriber whose account has been used for the alleged infringement. The subscriber will thus obtain personal information of the complainant/copyright owner by way of receiving the Notice. The subscriber may send a notice to the OSP to dispute the alleged infringement (“**Counter Notice**”). According to Form B in the Annex to the Second Draft, the subscriber has to furnish his name, address, telephone number, etc. in the Counter Notice.

6. Where the complainant/copyright owner or the subscriber is an individual, the name, address, telephone number, etc, of him constitute his “personal data” within the definition of the Personal Data (Privacy) Ordinance¹. Hence, the requirements under the Ordinance and in particular the six data protection principles will apply.

¹ The term “personal data” is defined under section 2(1) of the Personal Data (Privacy) Ordinance as meaning “any data relating (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable”

7. In relation to collection of personal data, Data Protection Principle (“DPP”) 1(1) in Schedule 1 to the Ordinance provides that personal data shall not be collected unless the data are collected for a lawful purpose directly related to a function or activity of a data user who is to use the data; the collection of the data is necessary for or directly related to that purpose; and that the data are adequate but not excessive in relation to that purpose. DPP1(3) requires that the person from whom personal data are to be collected shall be explicitly informed of the purpose for which the data are to be used and the classes of persons to whom the personal data may be transferred.

8. It is noted that paragraphs 1.5(a) to (e) of the Second Draft remind the OSPs to take reasonable steps to notify any prospective complainant or subscriber (who is living individual) of the requirements under DPP1(3). To assist the OSPs in complying with the relevant requirements, it will be desirable that a personal information collection statement (PICS) is explicitly provided under Forms A and B respectively.

9. With regard to the types of personal data to be collected, it is noted that apart from providing the name, address for service in Hong Kong and contact telephone number, a complainant/copyright owner is also required to provide “Additional information (if any)” under paragraph 1 of Form A. There is no explanation of what is “additional information”. We consider it desirable to specify the type of information required under this item so as to ascertain whether the additional information is necessary and not excessive for the intended purpose of use.

Use of personal data

10. The Second Draft contains directions involving the transfer of the complainant’s Notice or the subscriber’s Counter Notice respectively to each other *via* the OSPs. First and foremost, the contact particulars of the subscribers or the complainants/copyright owners will be used by the OSPs *in the respective service of the Notice or Counter Notice*. Furthermore, the personal data *contained in the Notice or Counter Notice* may then be disclosed by the OSPs to the subscriber or the complainant/copyright owner as a result, unless in the latter case the subscriber opts for the non-disclosure of his personal data in the Counter Notice sent to the complainant by the OSP.

11. In this connection, DPP3 provides that personal data shall not, without the prescribed consent of the data subject, be used (including disclosed or transferred) for any purpose other than the original purpose that the data were to be used at the time of collection of the data or a purpose directly related to the original purpose. The term “prescribed consent” is defined under Section 2(3) of the Ordinance as meaning an express and voluntary consent which has not been withdrawn in writing.

12. Regarding the personal data contained in the Notice or Counter Notice, they are transferred or disclosed by the OSPs to the subscriber or the complainant/copyright owner for the purpose of handling any alleged infringement of copyright ownership in the service platform. Such transfer or disclosure appears to be directly related to the original purpose of collection.

13. However, potential issue may arise when the OSP uses the subscriber’s personal data collected during the account opening process for serving the Notice (paragraphs 3.13 and 4.11 of the Second Draft refer). It is necessary to examine the terms and conditions in the relevant subscription form and other documents (including any PICS) when opening the account with the OSP to ascertain the original purpose of collection of the latter’s personal data. Where no such purpose of use was specified in the relevant form or documents, the subsequent change of the purpose of use of the personal data (i.e. for use in serving the Notice) may constitute a breach of DPP3 unless an express and voluntary consent of the subscriber is obtained. As the proposed operation will affect pre-existing subscribers (i.e. those who exist prior to the proposed amendment of the Copyright Ordinance), it is necessary to address this issue to safeguard the existing subscribers’ personal data privacy rights.

Security of personal data

14. It is expected that the OSPs will receive numerous Notices and Counter Notices hence involving storage and transfer of a substantial amount of personal data. It is apparent that the OSPs will have access to the personal data of the copyright owners and the subscribers who serve the Notices and the Counter Notices. Besides, the OSPs will be responsible for the operation, administration and maintenance of the personal data storage system. In this connection, DPP4 provides that all practicable steps should be taken to ensure that personal data held by a data user are protected against unauthorized or

accidental access, processing, erasure or other use having regard to (i) any security measures incorporated (whether by automated means or otherwise) in any equipment in which the data are stored, and (ii) any measures taken for ensuring the secure transmission of the data. In order to comply with DPP4, the OSPs have to take all practical measures to safeguard the security of personal data held or transmitted by them during the process.

Retention period of 18 months

15. Regarding the retention of the Notices and Counter Notices for a period of 18 months by OSPs, DPP2(2) requires that personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are or are to be used. Given the relatively short period of time within which the Counter Notice is required to be issued (paragraph 4.15 of the Second Draft refers), there should be strong justification to support a retention period of 18 months. The longer the retention of personal data, the higher the risk of data security.

Liability as principal

16. Under the Second Draft, the OSPs may designate an agent to receive Notice and/or Counter Notice by electronic or other means and perform other tasks. In this connection, Section 65 of the Ordinance provides for civil liability of a principal for the acts done by its agent. It is stated in section 65(2) of the Ordinance that, *“any act done or practice engaged in by a person as agent for another person with the authority (whether express or implied, and whether precedent or subsequent) of that other person shall be treated for the purposes of this Ordinance as done or engaged in by that other person as well as by him”*. Hence, it is incumbent on the OSP to ensure that its agent is well versed in the Ordinance regarding personal data privacy protection, especially the use of personal data (DPP3) and security of personal data (DPP4). Otherwise, the OSP may run the risk of being liable as the principal.

Consequence on breach of the Code

17. It is unclear as to the consequence of the breach of the Code. The lack of adverse consequence on the breach of the Code may greatly undermine its effectiveness in protecting personal data privacy.

18. We hope you will take into account of our comments in fine-tuning the Second Draft. Should you require further information, please feel free to contact the undersigned at 2877 7139.

Yours sincerely,

(Jeffrey LAU)
Legal Counsel
for Privacy Commissioner for Personal Data