Our Ref. : PCPD/CR(O)26/25/155

26th April 2007

By Post

Secretary for Commerce, Industry and Technology
Division 3
Commerce and Industry Branch
Commerce, Industry and Technology Bureau
Level 29, One Pacific Place
88 Queensway
Hong Kong

Dear Sir,

Consultation Paper : Copyright Protection in the Digital Environment ("the Paper")

I refer to the captioned Paper which was issued with the objective of reviewing the copyright law to meet the challenges in a digital environment.

2. The Paper canvasses specific issues of concern which impact upon the personal data privacy of individuals, namely:-

(i) whether specific mechanism should be provided for under the Copyright Ordinance for copyright owners to request Internet Access Service Providers ("IASPs") to disclose the identity of their clients allegedly engaged in online copyright infringing activities and if so, what features the mechanism should have;

(ii) whether IASPs should be statutorily required to keep records of clients' online communication and if so, how long the records should be kept; and

(iii) if the status quo is to be maintained, whether any industry guidelines

and measures should be formulated to enhance communication between copyright owners and IASPs so as to facilitate the obtaining of information pertaining to alleged online infringers by the copyright owners from the IASPs.

3. As the core protector of personal data privacy of individuals as well as the regulator of data users in Hong Kong, I am concerned about the three issues and would like to give below my submissions and the reasons supporting them.

Issue One: Whether there is a need to introduce specific mechanism for disclosure of infringers' personal data to copyright owners

(a) Legal requirement on disclosure of personal data

4. Under the Personal Data (Privacy) Ordinance ("the Ordinance"), where an IASP discloses its client's identity to a copyright owner, it has to observe the requirements of Data Protection Principle ("DPP") 3 in Schedule 1. This principle provides that unless with the prescribed consent of the data subject, personal data shall not be used for any purpose other than the purpose for which the data were to be used at the time of collection or a purpose directly related to that purpose. The term "use" is defined under section 2(1) of the Ordinance to include the disclosure or transfer of the personal data.

5. IASPs collect personal data of their clients originally for the purpose of providing Internet access service. The subsequent disclosure of their client's personal data to a copyright owner for the purpose of instituting civil proceedings against the client is not for the same purpose or a purpose directly related to it.

6. However, where there is a mandatory requirement of the law for a data user to disclose personal data, I take the view that such disclosure is consistent with the original purpose of collection of the data. It follows that where there is a court order requiring an IASP to disclose personal data, the compliance with the court order by the IASP does not contravene the requirements of DPP3.

7. Apart from mandatory legal requirements to disclose personal data, Part VIII of the Ordinance provides for exemption provisions by virtue of which a data user may disclose personal data contrary to the requirement of DPP3. Of direct relevance is the exemption available under section 58(2) of the Ordinance where the use of the data is for any of the purposes under section 58(1) and that

application of Data Protection Principle 3 would be likely to prejudice any of the matters referred to in that subsection. The purposes under 58(1)(d) are *"prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons"*. Hence, where the situation giving rise to disclosure of personal data by an IASP falls within the criteria laid down in section 58(2), disclosure of the data does not constitute an infringement of the Ordinance.

(b) Norwich Pharmacal Relief

8. In addition, under the existing law, Norwich Pharmacal relief is available to a copyright owner to apply for a court order requiring disclosure of the personal data of an alleged online copyright infringer. The Hong Kong Court in a recent decision[1] has ruled that *"seriously improper conduct"* under section 58(1)(d) covers tortious conduct, including copyright infringement. Thus, where the disclosure of a client's personal data is for an exempted purpose under Part VIII of the Ordinance and that it would be likely to prejudice the exempted purpose if the personal data were not so used, then an IASP may consider invoking the exemption in appropriate cases. It can thus be seen that the Ordinance as it currently stands has provided, in appropriate circumstances, exemptions from the restrictive use of personal data.

(c) US's Digital Millennium Copyright Act

9. The Paper expresses concerns that court procedure is costly and reference was drawn to a relatively "quick and inexpensive" subpoena procedure available under the US's Digital Millennium Copyright Act ("DMCA").

10. Whilst I appreciate that copyright owners have genuine concerns in identifying and pursuing legal action against infringers, a fair balance needs to be struck between the legitimate interest of copyright holders and individuals concerned. The mere fact that a "quick and inexpensive" alternative mechanism can achieve efficient enforcement by a copyright owner is insufficient justification for invasion of the personal data privacy of an individual.

11. There is no provision in the Ordinance which compels data users to disclose personal data. It is clear that the legislative intent is to protect data

---

[1] *Cinepoly Records Company Limited and Others v Hong Kong Broadband Network Limited and Others* [2006]HKLRD 255

subjects from the perspective of personal data protection. It is therefore my submission that any proposed amendments to the Copyright Ordinance should not go against this legislative spirit unless cogent and strong reasons exist. Overseas jurisdictions are generally inclined towards a clear legislative framework and judicial authorization as effective oversight to safeguard personal data privacy[2]. The DMCA was criticized for its privacy intrusiveness and the lack of judicial scrutiny. There are also limitations in the application of DMCA and the US court[3] had ruled that the subpoena procedure does not apply to peer-to-peer file sharing where the IASPs do not perform any storage or linking function.

(d) Compensation not enough to cover the costs of proceedings

12. It is stated in the Paper that the compensation received by the copyright owners from the infringer could not cover the costs incurred in such proceedings. The Paper explains that "*one of the reasons is that rather than aiming to compensate the copyright owners for their loss, the civil actions were mainly intended to send out a warning message to the community: individual infringers were generally only asked to pay an amount sufficient to achieve the desired purpose*."

13. I note from the explanation that it is the voluntary decision of the copyright owners to seek a lesser sum of compensation. Therefore, the possibility of obtaining a higher compensation from copyright infringers to cover the costs, not being tested, is yet to be seen. The justification for a less costly procedure therefore is not substantiated.

(e) Why a "quick" procedure is necessary?

14. The Paper does not explain in detail the reason why a "quick" procedure is justified in seeking discovery of the identity of alleged copyright infringers.

---

[2] For instance, under EU Directive 2004/48/EC of 29 April 2004 on the "The Enforcement of Intellectual Property Rights", available at (http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_195/l_19520040602en00160025.pdf), it is the "…. *competent judicial authorities"* which is to order disclosure of information on the alleged infringement of intellectual property right. The Australian Government in reviewing its Copyright Act in 2004 did consider the DMCA subpoena procedure but remarked that *"the high level of privacy invasiveness of the activity would demand a commensurate level of authority to govern decisions on access"* which should be *"vested in the courts to rule on discovery applications and on appropriate judicial authorities to issue warrants to law enforcement agencies"* and therefore did not support the DMCA subpoena procedure, see for reference at (http://www.privacy.gov.au/publications/copyrgtsub.pdf)

[3] *RIAA v Verizon Internet Services Inc.*, 2003 US Court of Appeal No. 03-7015.

Should there be good reasons justifying a quick procedure to be adopted, I believe that administrative arrangement may be made by the Judiciary to accommodate the situations. For example, there are Duty Judges available to deal with urgent applications such as injunction. In addition, a simple and quick procedure is provided for the Police to obtain warrants from the Magistrates. Thus, there is no justifiable ground to dispense with judicial scrutiny.

(f) Opening up the floodgate

15. At present, the IASPs will not provide personal data of their clients' to a third party. Even if the third party is a law enforcement agency seeking the information for the purpose of detecting crime, the IASPs require a court order or a warrant before releasing the data. Comparing with the Police in protecting the peace and order of the community, the copyright owner is only enforcing his own civil right. Unless there is strong justification, I am against providing special treatment for copyright owners. To do so will open up the floodgate for others requiring the IASPs to disclose personal data without court orders. This is undesirable from the privacy perspective. I think judicial scrutiny should not be taken away easily.

(g) My submission

16. In the light of the above, any decision to introduce a specific mechanism compelling disclosure of personal data by the IASPs should not be lightly made without a careful analysis of the impact that it might have on personal data privacy. Any disproportionate measures that outweigh the legitimate and reasonable expectation of privacy of the data subjects should be avoided, particularly in view of the following: —

(i) The purpose of collection of the personal data of the subscribers by the IASPs, i.e. for provision of internet access services and the duty of confidentiality owed by the IASPs to the subscribers;

(ii) The adverse action or consequences that may likely ensue should the alleged infringer's personal data be disclosed by the IASPs which might exceed the original purpose of collection of personal data or its directly related purpose;

(iii) The likelihood that personal data belonging to unrelated parties are inadvertently or mistakenly disclosed by the IASPs or that

unnecessary personal data are disclosed aggravating the harm, if any, to be inflicted upon the data subjects;

(iv) The risk that personal data so disclosed to the copyright owner be used for other unrelated purposes; and

(v) The practical difficulty, if any, for the IASPs to ascertain whether the requestor is the copyright owner.

Issue Two: Whether statutory requirement be imposed for IASPs to keep records of clients' online communications

(a) Legal requirement on retention of personal data

17. Insofar as these records contain personal data, the IASPs shall comply with the requirements of DPP2(2) of the Ordinance so that personal data shall not be kept longer than is necessary for fulfilment of the purpose for which the data are or are to be used. Section 26 of the Ordinance also imposes a duty upon the data user to erase personal data where the data are no longer required for the purpose (including any directly related purpose) for which the data were to be used unless any such erasure is prohibited under any law or it is in the public interest (including historical interest) for the data not to be erased. The retention of clients' online communication in order to provide evidence for copyright infringement apparently does not fall within the scope of the original purpose of collection of the clients' personal data by the IASPs or any directly related purpose.

(b) International standard

18. At international level, the EU Directive 2006/24/EC[4] issued on 15 March 2006 gives directions on the obligations of IASPs to retain records of online communications. Article 6 of the Directive provides that:-

"Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than 6 months and not more

[4] Directive 2006/24/EC of the European Parliament and of the Council issued on 15 March 2006 on "*The retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks*", available at (http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/l_105/l_10520060413en00540063.pdf)

than 2 years from the date of the communication."

19. The categories of data specified in Article 5 relates to data necessary to trace and identify the source of a communication concerning internet access, including the name and address of the subscriber or registered user to whom an Internet Protocol address was allocated at the time of communication.

20. Article 4 of the Directive, however, obliges the Members States to adopt measures to ensure that data retained in accordance with the Directive are provided only to competent national authorities in specific cases and in accordance with national law. Article 1 of the Directive specifically refers that the aims of the Directive is to ensure the data retained are available for the purpose of the investigation, detection and prosecution of serious crime as defined by each Member State in its national law.

21. The Directive, however, does not require an IASP to retain such data for the purpose of facilitating any possible enforcement action anticipated by copyright owners. In fact, such requirement does not seem to be approved by EU in view of the following comments made by Article 29 Data Protection Working Party in its Working Document on "Data Protection issues related to Intellectual Property Right" issued on 18 January 2005[5]:-

> *"Any personal data collected at the occasion of the provision of a protected product or service shall therefore be deleted as soon as it is no longer necessary for billing purpose or for any other purpose acknowledged by the user, such as maintaining a commercial relationship. It would not be compliant with this legal principle to keep all users data on a general basis just in the possible eventuality of alleged misuse of copyright information by a specific user."* (p.6 of the Working Document)
>
> *"On the basis of the compatibility principle as well as in compliance with the confidentiality principle included in Directives 2002/58 and 95/46, data retained by ISPs processed for specific purposes including mainly the performance of a telecommunication service cannot be transferred to third parties such as right holders, except, in defined circumstances provided by law, to public law enforcement authorities."* (p.7 of the Working

[5] The Working Party was set up under Article 29 of Directive 95/46/EC. The Working Document on "Data Protection issues related to Intellectual Property Right" issued on 18 January 2005 is available at (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp104_en.pdf).

Document)

"ISPs can neither be obliged, except in specific cases where there is an injunction of enforcement authorities, to provide for a general "a priori" storage of all traffic data related to copyright… Where traffic data are to be retained in specific cases, there must therefore be a demonstrable need, the period of retention must be as short as possible and the practice must be clearly regulated by law, in a way that provides sufficient safeguards against unlawful access and other abuse". (p.7 of the Working Document)

(c) Not to retain unnecessary indiscriminately

22. When considering the duty and period of retention to be prescribed, one must not lose sight of the legitimate concerns for personal data privacy. The continual retention of personal data by the IASPs will invariably expose the data to increased risks of unlawful or unauthorized access and use especially when the database is built and amassed over a period of time. Internet security in this technological era is a subject that warrants special attention. There should be in place sufficient safeguard to protect the personal data against leakage or improper access and use. IASPs should not arbitrarily or indiscriminately store and hoard unnecessary data belonging to their clients, especially since these online communications may contain sensitive personal data both of their clients and third parties.

(d) My submission

23. In view of the foregoing, I urge that a decision should not be lightly made on the imposition of a duty on IASPs to keep and retain clients' data solely for the purpose of facilitating the gathering of evidence by copyright owners.

Issue Three: Whether industry guidelines or measures be implemented to facilitate communication between IASPs and copyright owners

24. As mentioned above, disclosure of personal data in compliance with a court order is not regarded as contravention of DPP3. However, where the IASPs rely upon the exemption provision under Part VIII of the Ordinance to make voluntary disclosure, they should take care to ensure that the criteria laid down in the exemption provisions are properly met because in each case they take the risk of committing a breach of the provisions of the Ordinance. For example, reliance

upon the exemption under section 58(2) requires the data user to justify the basis upon which the exempted purpose would likely to be prejudiced if the personal data are not so disclosed. After all, the exemption provisions of the Ordinance are permissive in nature. A data user may disclose the personal data in reliance of an exemption provision but it is not mandatory for a data user to disclose the data. When a complaint comes before me, I shall take into account all the circumstances of the case to assess and determine whether the requirements of the Ordinance are duly observed by the IASPs in making disclosure of personal data in question.

My submission

25. While the implementation of industry guidelines may facilitate better communications between IASPs and the copyright owners, they do not and cannot have the legal effect of overriding the requirements of the Ordinance. It should not be used as an instrument compelling disclosure of personal data by the IASPs.

I hope the above will assist in your formulating a policy that will strike a proper balance between the protection of copyright owners and the protection of individual's personal data privacy rights which is presently guaranteed by the laws of Hong Kong.

Yours sincerely,

(Roderick B WOO)
Privacy Commissioner for Personal Data