Report Published under Section 48(2) of the Personal Data (Privacy) Ordinance (Cap. 486)

根據《個人資料（私隱）條例》（第 486 章）第 48（2）條發表的報告

Report Number: R07-3619

報告編號：R07-3619

Date issued: 14 March 2007

發表日期：2007 年 3 月 14 日

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

The Disclosure of Email Subscriber's Personal Data by Email Service Provider to PRC Law Enforcement Agency

Case number: 200603619

This report in respect of an investigation carried out by me pursuant to section 38 of the Personal Data (Privacy) Ordinance, Cap 486 (the "Ordinance") against Yahoo! Hong Kong Limited is published in the exercise of the power conferred on me by Part VII of the Ordinance. Section 48(2) of the Ordinance provides that *"the Commissioner may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, publish a report –*

(a) setting out -

(i) the result of the investigation;

(ii) any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and

(iii) such other comments arising from the investigation as he thinks fit to make; and

(b) in such manner as he thinks fit."

Roderick B. WOO
Privacy Commissioner for Personal Data

Table of Contents

CHAPTER ONE

Introduction

Preamble

1.1 This Report pertains to an investigation carried out by the Privacy Commissioner for Personal Data (the "**Commissioner**") pursuant to section 38 of the Personal Data (Privacy) Ordinance, Chapter 486 (the "**Ordinance**") in respect of an allegation that Yahoo! Hong Kong Limited (formerly known as Yahoo! Holdings (Hong Kong) Limited) ("**YHHK**") had disclosed an email user's personal data to the PRC authorities, thereby infringing the provisions of the Ordinance.

The Incident

1.2 In October 2005, it was widely reported by local newspapers that a journalist (hereinafter referred to as "**Mr. X**") residing in the PRC, was convicted by the Changsha Intermediate People's Court ("**People's Court**") of the crime of illegally providing state secrets to foreign entities outside PRC in violation of Article 111 of the Criminal Law of the PRC[1] and was sentenced to 10 years' imprisonment.

1.3 According to the news reports, YHHK had disclosed the personal data of Mr. X, who was an email user of "*yahoo.com.cn*", to the PRC authorities and as a result Mr. X was arrested.

1.4 In the verdict (the "**Verdict**") delivered by the People's Court on 27 April 2005[2], it stated that Mr. X had on 20 April 2004 at approximately 11:32 p.m. leaked information "*to an overseas hostile element, taking advantage of the fact that he was working overtime alone in his office to connect to the internet through his phone line and used his personal email*

---

[1] Article 111 of the Criminal Law provides that: "*Whoever steals, buys or unlawfully supplies State secrets or intelligence for an organ, organization or individual outside the territory of China shall be sentenced to fixed-term imprisonment of not less than five years but not more than 10 years; if the circumstances are especially serious, he shall be sentenced to fixed-term imprisonment of not less than 10 years or life imprisonment; if the circumstances are minor, he shall be sentenced to fixed-term imprisonment of not more than five years, criminal detention, public surveillance or deprivation of political rights*".

[2] See Annex A of this Report

account (huoyan-1989@yahoo.com.cn) to send his notes [on the summary of the main contents of a top-secret document issued by the General Office of the Central Committee of the Communist Party of China (CPC) and the General Office of the State Council entitled "A Notice Regarding Current Stabilizing Work" (CPC General Office Document No.11 [2004])]. He also used the alias "198964" as the name of the provider…"

1.5 The Verdict reported the evidence gathered to prove the commission of the offence which included the following:

> "*Account holder information furnished by Yahoo! Holdings (Hong Kong) Ltd., which confirms that for IP address 218.76.8.201 at 11:32:17 p.m. on April 20, 2004, the corresponding user information was as follows: user telephone number: 0731-4376362 located at the Contemporary Business News office in Hunan; address: 2F, Building 88, Jianxiang New Village, Kaifu District, Changsha.*"

1.6 The email account from which the materials classified as state secrets were sent to foreign entities was "*huoyan-1989@yahoo.com.cn*" (the "**Email Account**").

1.7 From the Verdict, it was therefore clear that YHHK had disclosed certain email user information to the PRC authorities but as to the extent of the data disclosed to the PRC authorities by YHHK in the course of the investigation, the Verdict was not conclusive. According to the Verdict, the People's Court had also considered other pieces of evidence including such evidence as written statements given by Mr. X confessing that "he intentionally and illegally provided state secrets to foreign entities".

1.8 The above incident (the "**Incident**") attracted public attention and aroused personal data privacy concern, in particular in relation to the purported disclosure of the email users' information by the email service provider to an law enforcement agency outside Hong Kong, as to whether such act violated the provisions of the Ordinance. The concern was accentuated by the fact that in the course of their provision of services, email service providers would have collected and held massive personal data and any improper handling of the email users' personal data would

have dire consequences on the personal data privacy of the data subjects.

Press Release Issued by YHHK

1.9 On 18 October 2005, in response to the public concern, YHHK issued a press release which expressly refuted its involvement in the disclosure of the relevant user information. It stated that: "*Yahoo! Hong Kong adheres to all applicable local laws and regulations in Hong Kong and our privacy policy. The Chinese authorities have never contacted Yahoo! Hong Kong to request any of its user information. Yahoo! Hong Kong and Yahoo! China are managed and operated separately and independently of one another. As such, Yahoo! Hong Kong and Yahoo! China have never exchanged or revealed respective user information to one another*."

Issues of Personal Data Privacy Concern

1.10 The Incident raises the following issues under the Ordinance: -

1.10.1 Whether "personal data" within the meaning of the Ordinance were disclosed by YHHK to the PRC authorities;

1.10.2 Whether such act of disclosure by YHHK is caught by the jurisdiction of the Ordinance, having particular regard to the circumstances under which the personal data of Mr. X, if any, were collected and disclosed by YHHK; and

1.10.3 If the act or practice is caught by the Ordinance, as to whether there was a contravention of Data Protection Principle ("**DPP**") 3 in respect of the disclosure of the data by YHHK to the PRC authorities; and if so, would there be any exemption provision of the Ordinance available to YHHK?

CHAPTER TWO

Preliminary Enquiries

Preliminary Enquiries Raised with YHHK

2.1 On 21 October 2005, the Commissioner took the initiative to approach YHHK to gather further information for the purpose of ascertaining whether there was any evidence of contravention of the Ordinance.

2.2 On 29 October 2005, YHHK provided a written response to the Commissioner and averred that: -

2.2.1 YHHK was not involved in any disclosure of information relating to Mr. X to the PRC authorities or any agents thereof;

2.2.2 The disclosure was related to a PRC user in the PRC holding a *".cn"* email account registered at the website of Yahoo! China ("**Yahoo! China**");

2.2.3 The disclosure was made by Yahoo! China;

2.2.4 The websites of Yahoo! Hong Kong ("**Yahoo! Hong Kong**") and Yahoo! China were managed and operated independently from one another;

2.2.5 Yahoo! Hong Kong and Yahoo! China did not exchange user account information; and

2.2.6 YHHK would only respond to the Hong Kong law enforcement authorities upon a valid and formal written request pursuant to Hong Kong law and in case of an order for email content disclosure, YHHK would not release any information to law enforcement agencies except on receipt of a search warrant issued by a court

of law in Hong Kong.

Concerns Raised by Members of the Legislative Council

2.3 On 1 November 2005, a special meeting was held in the Legislative Council by the Panel on Information Technology and Broadcasting (the "**Panel**") to discuss about the Incident. The Commissioner was invited to attend this panel meeting. During the meeting, the Commissioner addressed issues relating to the definition of "personal data", jurisdiction of the Ordinance as well as protection of personal information of email users.

2.4 Concerns were raised by members of the Panel as to the definition of "personal data" and in particular whether it covers Internet Protocol address ("**IP address**") as well as the lawfulness of the disclosure of user information by an Internet Service Provider ("**ISP**"). The Legal Service Division of the Legislative Council Secretariat was asked to research and prepare paper[3] on the scope of coverage of "personal data" particularly in view of the widespread use of electronic media for communication.

Further Information from YHHK

2.5 On 19 November 2005 and 9 December 2005 and in response to the Commissioner's enquiries, YHHK provided further information relevant to the Incident as follows: -

2.5.1 The data which the Incident was concerned were collected by Yahoo! China in PRC, which was owned by YHHK at the material time;

2.5.2 The data in question appeared to be in respect of a user of Yahoo! China located in PRC;

2.5.3 The name under which the user registered with Yahoo! China was not Mr. X; Yahoo! China did not know that the user was in fact Mr. X;

[3] See LC Paper No. LS21/05-06 at Annex B of this Report

2.5.4 The data in question was disclosed by Yahoo! China in PRC to the PRC authorities in accordance with PRC laws;

2.5.5 None of the actions germane to the Incident (data collection, storage and disclosure) happened in Hong Kong and that none of the relevant parties (i.e. Yahoo! China, Mr. X and the PRC authorities) were Hong Kong parties;

2.5.6 Even if the Ordinance governed conduct that occurred wholly outside Hong Kong but within PRC, YHHK considered that the exemption under section 58(2) of the Ordinance would be applicable for the release of the relevant data;

2.5.7 Yahoo! China was wholly owned by YHHK prior to the change of ownership to Alibaba.com Corporation ("**Alibaba**") on 24 October 2005;

2.5.8 Yahoo! China was operated by a PRC entity called Peking University Founder Group ("**PUFG**") through Beijing Yahoo! Consulting and Service Company Limited ("**Beijing Yahoo!**") which was wholly owned by YHHK;

2.5.9 The Internet Contents Provider **("ICP")** licence for the Yahoo! China website was issued by the PRC government and held by PUFG;

2.5.10 Records relating to the Incident were kept by Yahoo! China which had subsequently been sold to Alibaba;

2.5.11 According to the Verdict, the user name of the Email Account was "huoyan_1989" and not Mr. X; and

2.5.12 YHHK had no control over the collection and/or disclosure of Yahoo! China's users data.

CHAPTER THREE

The Complaint

3.1 On 30 March 2006, a complaint was received by the Commissioner from Mr. X's authorized representative in Hong Kong. It was alleged that YHHK had disclosed to the PRC authorities Mr. X's personal data relating to the Email Account without his consent, thereby breaching the requirements of the Ordinance.

3.2 No supporting evidence was attached to Mr. X's complaint. Despite repeated requests, no further information or evidence was produced by Mr. X or his authorized representative to the Commissioner for consideration.

3.3 The only piece of evidence that Mr. X's authorized representative relied upon was the contents of the Verdict which confirmed that YHHK had supplied certain email user information to the PRC authorities which led to the eventual arrest and conviction of Mr. X.

3.4 Based on the facts and evidence obtained by him in the course of his preliminary inquiries made about the Incident, the Commissioner decided to carry out an investigation pursuant to section 38 of the Ordinance on 9 May 2006.

CHAPTER FOUR

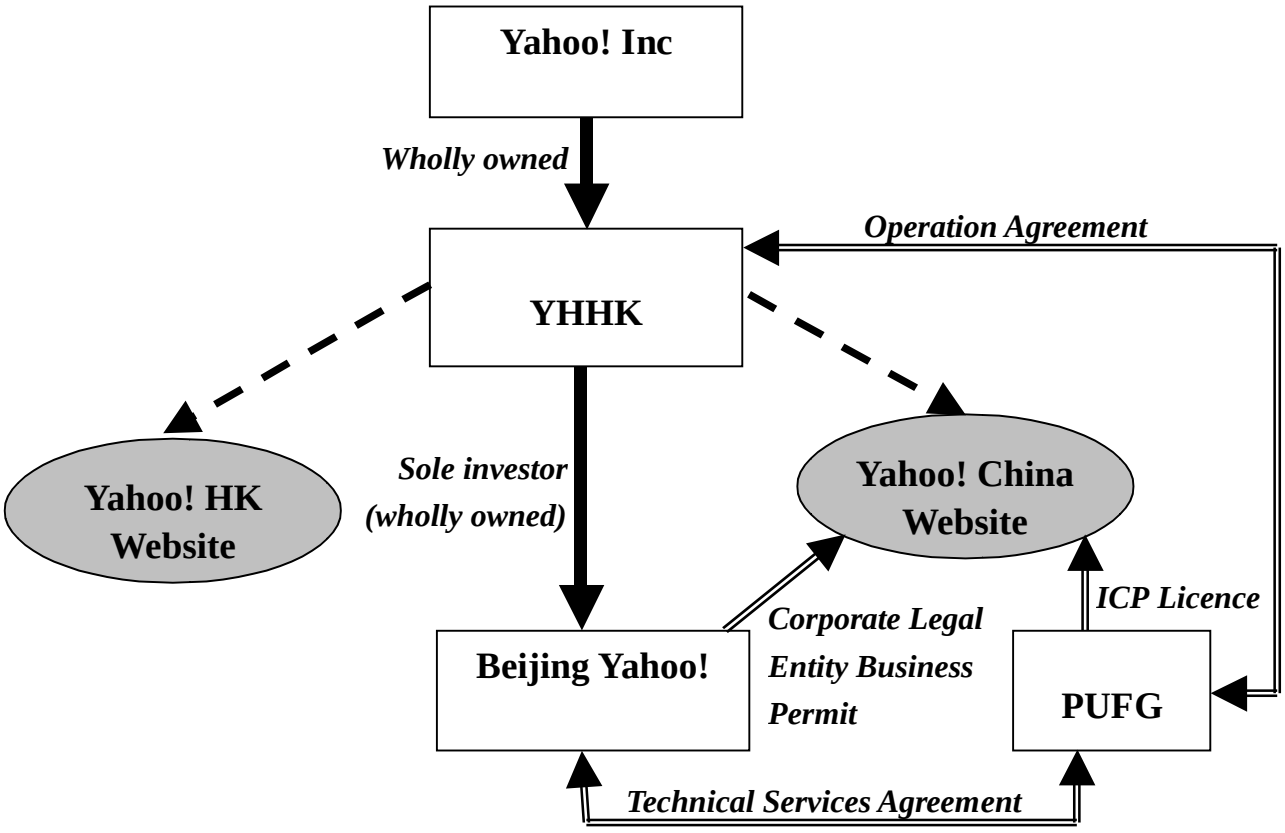
Operation of Yahoo! China and Corporate Structure of YHHK

4.1 The Commissioner finds it important to first examine the operations of Yahoo! Hong Kong and Yahoo! China as well as the corporate structure of YHHK in order to assess the role played by and the legal obligations of YHHK in the Incident.

Operation of Yahoo! China

4.2 YHHK confirmed that the relevant disclosure was made by Yahoo! China on 22 April 2004. The operation of Yahoo! China at the material time is illustrated by the following chart:

Yahoo! China's Operational Structure (April 2004)



4.3 It can be seen from the above chart that Yahoo! Hong Kong and Yahoo! China though both owned by YHHK, the mode of operation was different. YHHK had through its wholly owned PRC corporate entity, namely, Beijing Yahoo! operated Yahoo! China in accordance with the Wholly Foreign-Owned Enterprise Law in PRC. Under the *Certificate of Approval for Establishment of Enterprises with Investment of Taiwan, Hong Kong, Macao and Overseas Chinese in the People's Republic of China* issued by the Beijing Municipal Government on 29 April 2002, YHHK was stated to be the investor of Beijing Yahoo! with registered capital solely contributed by YHHK. Beijing Yahoo! was holder of a Corporate Legal Entity Business Permit describing its enterprise type as "Wholly Foreign-Owned Enterprise (Hong Kong)". Under the articles of association of Beijing Yahoo!, YHHK had the right to appoint and replace each member of the board of directors of Beijing Yahoo!, including the chairman.

4.4 For the purpose of having an ICP licence for the operation of Yahoo! China in PRC, YHHK entered into an Operation Agreement **("Operation Agreement")** with PUFG on 19 February 2003 to utilize its ICP licence. Beijing Yahoo! provided PUFG with technical services to facilitate the operation of the Yahoo! China website under a Technical Services Agreement dated 19 February 2003 **("Technical Services Agreement")**.

4.5 The Commissioner obtained from YHHK the business permits, corporate documents, the Operation Agreement and Technical Services Agreement relating to the operation of Yahoo! China. There is no contrary evidence before the Commissioner to doubt the authenticity of these documents.

4.6 In substance and prior to 24 October 2005, Yahoo! China was wholly owned by YHHK and operated through PUFG and Beijing Yahoo!.

4.7 Since 24 October 2005, Alibaba became the owner and operator of Yahoo! China.

Corporate Structure of YHHK

4.8 YHHK is a Hong Kong company incorporated under the laws of Hong Kong and is the owner and operator of Yahoo! Hong Kong.

4.9 The ultimate parent of YHHK is **Yahoo! Inc.** which is a United States ("**US**") company based in California. Yahoo! Inc. beneficially and ultimately owns the entire issued share capital in YHHK.

4.10 YHHK and Yahoo! Inc. are shareholders which together currently hold about 40% of the issued shares of Alibaba.

4.11 YHHK changed its name to Yahoo! Hong Kong Limited on 22 June 2006.

CHAPTER FIVE

Legal Requirements

5.1 The following provisions of the Ordinance are relevant to this investigation:

5.1.1 **Section 2(1)** of the Ordinance provides that:

"'Personal data' means any data –

(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;"

"'Data user', in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data;"

"'Practicable' means reasonably practicable;"

5.1.2 **DPP 3** in Schedule 1 to the Ordinance provides that:

"Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than—

(a) the purpose for which the data were to be used at the time of the collection of the data; or

(b) a purpose directly related to the purpose referred to in paragraph (a)."

5.1.3 The term **"use"** in relation to personal data is defined under section 2(1) of the Ordinance to include

"disclosure" or *"transfer"* of the data.

5.1.4 According to section 2(3) of the Ordinance, **"prescribed consent"** means *"express consent of the person given voluntarily"* which has not been withdrawn by notice in writing.

5.1.5 **Section 39(1)(d)** of the Ordinance provides that:

"(1) Notwithstanding the generality of the powers conferred on the Commissioner by this Ordinance, the Commissioner may refuse to carry out or continue an investigation initiated by a complaint if –

…

(d) none of the following conditions is fulfilled in respect of the act or practice specified in the complaint –

(i) either –

(A) the complainant (or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person) was resident in Hong Kong; or

(B) the relevant data user was able to control, in or from Hong Kong, the collection, holding, processing or use of the personal data concerned,

at any time the act or practice was done or engaged in, as the case may be;

(ii) the complainant (or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person) was in Hong Kong at any time the act or practice was done or engaged in, as

the case may be;

(iii) in the opinion of the Commissioner, the act or practice done or engaged in, as the case may be, may prejudice the enforcement of any right, or the exercise of any privilege, acquired or accrued in Hong Kong by the complainant (or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person);"

5.1.6 **Section 58(1)** and **(2)** of the Ordinance provides that:

"(1) Personal data held for the purposes of -

(a) the prevention or detection of crime;

(b) the apprehension, prosecution or detention of offenders;

….

(2) Personal data are exempt from the provisions of data protection principle 3 in any case in which -

(a) the use of the data is for any of the purposes referred to in subsection (1) (and whether or not the data are held for any of those purposes); and

(b) the application of those provisions in relation to such use would be likely to prejudice any of the matters referred to in that subsection,

and in any proceedings against any person for a contravention of any of those provisions it shall be a defence to show that he had reasonable grounds for believing that failure to so use the data would have been likely to prejudice any of those matters."

5.1.7 **Section 65(1)** and **(2)** of the Ordinance provides that:

"(1) Any act done or practice engaged in by a person in the course of his employment shall be treated

for the purposes of this Ordinance as done or engaged in by his employer as well as by him, whether or not it was done or engaged in with the employer's knowledge or approval.

(2) 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."

CHAPTER SIX

Investigation and Evidence Gathering

6.1 Unless otherwise stated, all information contained in this chapter were submitted by YHHK or Yahoo! Inc. to the Commissioner during the investigation of this case. The focus of investigation was to find out what personal data, if any, was disclosed by YHHK and the circumstances for such disclosure.

The Business Structure

6.2 YHHK elaborated further on the mode of operation of Yahoo! China. According to YHHK, the business of Yahoo! Hong Kong was run by a management team in Hong Kong and that of Yahoo! China was run by a separate management team in Beijing. All operational, management, strategic and business decisions for Yahoo! China were made by Yahoo! China, with direction from Yahoo! Inc. or its appointed international operations management team.

6.3 YHHK's board of directors discharged all its statutory functions, for example, on the approval of the use of common seal and approval of audited accounts in relation to YHHK only. None of the activities carried out or resolutions passed by the board of directors of YHHK was related to the day-to-day management operations of Yahoo! China.

6.4 Insofar as matters relating to disclosure of personal data of Yahoo! email users are concerned, they were handled primarily by the legal teams of the respective websites. The legal team of Yahoo! China ("**Yahoo! China Legal Team**") reported directly to the legal team of Yahoo! Inc.

6.5 With this line of authority and accountability, although Yahoo! China was legally owned by YHHK, from an operational perspective, it was managed and controlled vertically and ultimately by the management of Yahoo! Inc.

6.6 As such, YHHK did not exercise control over the affairs of Yahoo! China. Such control was in fact exercised wholly by Yahoo! Inc.

Disclosure of User Information to the PRC Authorities

6.7 YHHK was asked by the Commissioner to give details on the circumstances under which the disclosure of the user information relating to the Email Account was made and as to the legal advice, if any, sought relating to the disclosure.

6.8 Yahoo! Inc., responding on behalf of YHHK, gave sequence of events leading to the disclosure of user information relating to the Email Account as follows:

6.8.1 Before 22 April 2004, Yahoo! China received an email from the State Security Bureau **("SSB")** of the PRC demanding for the user information relating to the Email Account. In response, Yahoo! China requested for a formal data disclosure order from SSB.

6.8.2 On 22 April 2004, SSB hand-delivered a data disclosure order (the **"Order"**) issued by the SSB pursuant to Article 45 of the PRC Criminal Procedure Law **("Article 45")**. The Order bore an official chop from the Beijing Branch of SSB and was in respect of criminal investigation into *"illegal disclosure of state secrets overseas"*.

6.8.3 The Yahoo! China Legal Team examined the validity and legality of the Order and confirmed that Yahoo! China was legally obliged to comply with the Order.

6.8.4 The customer care team of Yahoo! China **("Yahoo! China Customer Care Team")** retrieved the required information from the users' database of Yahoo! China, which was located on servers in the PRC.

6.8.5 The Yahoo! China Legal Team confirmed that the

information retrieved corresponded to the information requested by the Order and approved the disclosure.

6.8.6 The YHHK's company chop (the "**YHHK Chop**") was applied by the Yahoo! China Legal Team in their Beijing office on the documents which contained the information requested by and disclosed to SSB.

6.8.7 On or about 22 April 2004, Yahoo! China disclosed the relevant information relating to the Email Account to SSB.

6.8.8 After 22 April 2004, there were subsequent communications between SSB and Yahoo! China regarding further information relating to the Email Account.

6.8.9 Yahoo! China Customer Care Team provided SSB with further information in accordance with the Order.

6.9 Yahoo! Inc. confirmed that Yahoo! China had provided to SSB "*(i) user registration information, (ii) IP log-in information and (iii) certain email contents*" (the "**Information**"). Yahoo! Inc. further stated that users of email service are generally asked to provide information such as name, gender, birthday, etc. for registration. However, there is no guarantee that the information so provided is genuine as many users do not register with real information.

6.10 Article 45 provides that: "*The People's Court, the People's Procuratorates and the public security organs shall have the authority to collect or obtain evidence from the units and individuals concerned. The units and individuals concerned shall provide truthful evidence. Evidence involving State secrets shall be kept confidential. Anyone that falsifies, conceals or destroys evidence, regardless of which side of a case he belongs to, must be investigated under law*".

6.11 Yahoo! China was not made aware of the exact nature or details of the investigation by SSB, but the Order from SSB stated that it was in

respect of a criminal investigation into *"illegal disclosure of state secrets overseas"*.

6.12 Yahoo! China was not made aware as to whether SSB knew the identity of the user of the Email Account at the time of making the request for user information.

6.13 When asked by the Commissioner as to whether any legal advice was obtained prior to the disclosure of the Information to the SSB, Yahoo! Inc. claimed that legal advice on Article 45 was received from their PRC in-house counsel as follows:

6.13.1 Public security organs had the authority to collect or obtain evidence from the units or individuals concerned;

6.13.2 Evidence involving state secrets had to be kept confidential;

6.13.3 Any party that falsified, concealed or destroyed evidence, regardless of which side of a case such party belong to, had to be investigated under law;

6.13.4 Refusal to provide legally required evidence might be deemed obstruction of a government function and might subject the person to no more than 3 years' imprisonment, detention, public surveillance or a fine under Article 277 of the PRC Criminal Law ("**Article 277**"); and

6.13.5 SSB's request for the Information was required under PRC laws, hence the disclosure of the Information was not a voluntary act.

Testimony and Declaration of the Senior Vice President and General Counsel of Yahoo! Inc. ("Mr. Y")

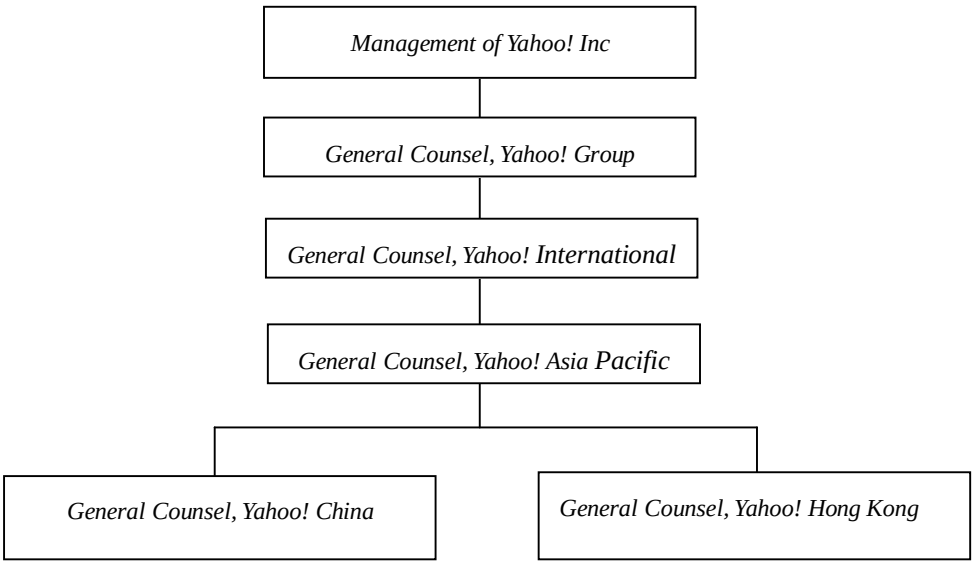
6.14 In support of YHHK's claim that disclosure of the Information

was in compliance with the PRC laws, a testimony given by Mr. Y on behalf of Yahoo! Inc. to the US Congress on 15 February 2006[4] in relation to the facts surrounding Mr. X's case was provided to the Commissioner for consideration.

6.15 In the testimony, Mr. Y testified that: "*When Yahoo! China in Beijing was required to provide information about the user, who we later learned was [Mr. X], we had no information about the nature of the investigation. Indeed, we were unaware of the particular facts surrounding the case until the news story emerged. … In many cases, Yahoo! does not know the real identity of individuals for whom governments request information, as very often our users subscribe to our services without using their real names. … When we receive a demand from law enforcement authorized under the law of the country in which we operate, we must comply. … Failure to comply in China could have subjected Yahoo! China and its employees to criminal charges, including imprisonment. … In this case, the Chinese government ordered Yahoo! China to provide user information, and Yahoo! China complied with Chinese law.*"

6.16 At the request of the Commissioner, Mr. Y also made a written declaration on 23 August 2006 at Santa Clara, California, US, in support of the submissions made by Yahoo! Inc. to the Commissioner. He declared that: "*… Based on my understanding of what constitutes 'personal data' under the Hong Kong Personal Data (Privacy) Ordinance, no personal data was provided by [Mr. X] in the course of his registration with Yahoo! China. As a standard corporate procedure, law enforcement requests are dealt with at the local subsidiary level and Yahoo! Inc. is not informed of the specific details of law enforcement actions. … In order to provide proper checks and balances and to ensure integrity in the discharge of legal functions, the Legal Department is independent of the business operations. Lawyers in each country are not accountable to and did not report to the local business team. Instead, the reporting line at the time was as follows:*

[4] See Annex C of this Report



Only the Legal Department of Yahoo! China could review the law enforcement order in relation to the [Mr. X] case, implement the required procedure and authorize the disclosure of Yahoo! China's user data to the Beijing Branch of the State Security Bureau and the use of the [YHHK's] chop in the disclosure documents, and, based on corporate policy and practice, as explained above, the Legal Department of Yahoo! China was not controlled by [YHHK]."

No Access to Yahoo! China's User Accounts by YHHK

6.17 The Commissioner asked for direct confirmation from YHHK on the responses given by Yahoo! Inc. YHHK submitted that it did not have control over the collection, holding, processing or use of personal data of Yahoo! China's users and therefore YHHK did not have and had never had access to the records of the Email Account.

6.18 To illustrate that YHHK was unable to access to user's information of Yahoo! China's accounts, YHHK showed the Commissioner the operation of its internal account management system for which attempt to access Yahoo! China's users' account information would be denied with a pop up message that *"you do not have permission to open user:…"*.

No Further Submissions from Mr. X's Authorized Representative

6.19 Despite our repeated requests for information on Mr. X's user's registration information in respect of the Email Account and the Information disclosed to SSB, Mr. X's authorized representative did not supply to the Commissioner any further information.

Verification from Public Records

6.20 According to company search conducted in Hong Kong on YHHK, of the 1,000 issued share capital of YHHK, Yahoo! Inc. is holding 10 issued shares and Yahoo! International Subsidiary Holdings Inc. is holding 990 shares.

6.21 Yahoo! Inc. confirmed that all the issued shares of Yahoo! International Subsidiary Holdings Inc. were at the material time, and are still, owned by Yahoo! Inc. Hence, Yahoo! Inc. ultimately wholly owns YHHK and thus is in a position to respond on behalf of YHHK in relation to this complaint. A copy of the share certificate issued by Yahoo! International Subsidiary Holdings Inc. to Yahoo! Inc. was produced to the Commissioner as supporting evidence.

CHAPTER SEVEN

PRC Laws Application

Issues Relating to PRC Laws

7.1 In the course of investigation, there are two issues relating to the application of PRC laws that the Commissioner has to resolve. The first issue concerns whether Yahoo! China was legally obliged to release the Information to SSB pursuant to Article 45. The second issue relates to the refusal of YHHK to disclose certain information to the Commissioner during the course of investigation.

7.2 On both issues and for the purpose of assessing the weight and relevancy of the submissions from YHHK, the Commissioner sought independent legal advice from two PRC law experts (the **"PRC law experts"**).

First Issue: Article 45 and the Obligation to Comply

7.3 The first issue that concerns the Commissioner is whether Yahoo! China was legally obliged to disclose the Information to SSB. Issues such as the lawfulness of the Order given by SSB, the duty to comply and consequences of non-compliance are relevant for consideration.

7.4 The PRC law experts were consulted on the scope of application of Article 45 to the present case. According to the PRC law experts, since YHHK operated businesses in the PRC, it should comply with the PRC laws, including the PRC's Criminal Procedure Law in respect of the businesses operated in the PRC. The official issuance of the Order duly signed or chopped by SSB is treated as having complied with the legal procedures for its issuance. Any person or unit has legal duty to provide truthful evidence.

7.5 As it is clear from the Verdict that corresponding user information was provided by YHHK and submitted by the prosecution for consideration by the People's Court, the Commissioner has no reason or

contrary information to doubt the existence or authenticity of the Order issued by SSB upon YHHK for the purpose of the investigation carried out by SSB.

7.6 The PRC law experts also referred the Commissioner to the provision of Article 18 of the State Security Law ("**Article 18**")[5] which obliges citizens and organizations to furnish to the state security organ relevant information relating to investigation carried out by it.

7.7 As for the consequences for non-compliance with the disclosure order, Article 277 provides that "… *whoever intentionally obstructs officers of a State security organ or a public security organ from maintaining State security in accordance with law and causes serious consequences, though without resort to violence or threat, shall be punished …"* and will be *"… sentenced to fixed-term imprisonment of not more than three years, criminal detention, or public surveillance or be fined ".*

7.8 Although different views[6] on statutory interpretation were expressed by the PRC law experts as to whether refusal to provide the requested information to SSB amounted to "obstruction" under Article 277, the Commissioner finds that, having taken legal advice, Yahoo! China and YHHK did in the circumstances of the case have genuine penal apprehension on possible violation of Article 45 or Article 277 if it refused to comply with the Order.

Other Consequences on Failure to Supply Information to SSB

7.9 Apart from the criminal sanction that would attach on failure to supply to SSB the Information, the PRC law experts were further of the opinion that by virtue of the business nature undertaken by YHHK in the PRC, it was also obliged to comply with other relevant laws, rules and

---

[5] Article 18 provides that, "*when a State security organ investigates and finds out any circumstances endangering State security and gathers related evidence, citizens and organizations concerned shall faithfully furnish it with relevant information and may not refuse to do so".*

[6] One school of thought opines that Article 277 applies to penalty imposed on offence of interference with public order and does not cover the act of refusal to provide evidence upon request. Another school of thought however views that refusal to provide evidence upon request fulfills the requirements of paragraph 4 of Article 277 as being an act of "non violent" obstruction.

regulations, one of which being the Regulation on Telecommunications of the PRC (the "**Regulation on Telecom**").

7.10 The Regulation on Telecom prohibits organization or individual from producing, publishing or transmitting information which has contents detrimental to state security, state secrecy, etc.[7] The breach of which may in serious cases lead to the revocation of the telecommunications business licence by the Ministry of Information Industry[8]. The Regulation on Telecom also imposes a duty on the business operator to terminate the transmission of such information immediately and report to relevant authorities[9].

7.11 Further, YHHK's business activities in the PRC also require it to comply with the *Regulation on the Internet Information Service* of the PRC which contains provision requiring Internet email service provider to actively cooperate with the relevant state organs in making investigation[10]. The failure to comply with the requirement may render the entity to be subject to administrative sanctions, including admonition and fine[11].

7.12 Having considered the submissions made by YHHK and also advice obtained from the PRC law experts on the application of the PRC laws and regulations and the duty to comply, the Commissioner is satisfied that the Information disclosed by YHHK to SSB pursuant to the Order was a legal obligation imposed upon YHHK, the refusal to comply might result in both criminal and administrative sanctions.

Second Issue: Non-disclosure of the Requested Data to the Commissioner

7.13 During the course of his investigation, the Commissioner asked YHHK to produce (i) the account user's information in respect of the

---

7 Article 57 of the Regulation on Telecommunications.

8 Article 78 of the Regulation on Telecommunications.

9 Article 62 of the Regulation on Telecommunications.

10 Article 18 of the Measures for the Administration of Internet Email Services provides, "*an internet email service provider, or a telecommunication service provider that provides access services to Internet email services shall actively cooperate with the relevant state organ and the Internet Email Revealment Acceptance Center in making investigations*".

11 Article 25 of the Measures for the Administration of Internet Email Services provides the sanctions which include admonition by the Ministry of Information Industry and fine of up to 10,000 Yuan, in addition.

Email Account, (ii) the correspondence with SSB, (iii) the Order, and (iv) the Information (collectively the "**Requested Data**").

7.14 In response to the Commissioner's request, YHHK claimed that it did not have actual knowledge of or access to most of the information or document requested by the Commissioner. It was unable to provide the Commissioner with copies of documents related to the disclosure as it had been advised by their PRC in-house counsel that those documents might be considered as state secrets under Article 2 of the PRC State Secrets Law ("**Article 2**") since they related directly to a criminal investigation in the PRC.

7.15 Article 2 provides that "*state secrets shall be matters that have a vital bearing on state security and national interests and, as specified by legal procedure, are entrusted to a limited number of people for a given period of time*". A relatively wide definition has been given to what constitutes "state secrets" and it includes the "*secrets concerning activities for safeguarding the state security and the investigation of criminal offence*". The question as to whether any information can be classified as "state secrets" is a matter to be determined by the state secret-guarding department[12].

7.16 Upon demand for further details by the Commissioner, YHHK confirmed that the legal advice obtained from their PRC in-house counsel was that:

7.16.1 Information required by relevant government agencies for the investigation of criminal offences was considered to be a state secret; and

7.16.2 In the event of any ambiguity on whether or not a specific item was a state secret, the disclosing entity is required to treat the item as a state secret.

7.17 In considering whether to invoke his powers under the Ordinance to compel production of the Requested Data, the Commissioner sought advice from the PRC law experts on the application of the relevant

[12] Article 11 of the PRC State Secrets Law

provisions of the State Secrets Law as ground of refusal relied upon by YHHK. The PRC law experts shared the view that where the evidence or information for the trial of leakage of state secrets had been so confirmed by the court, the conclusion of the trial did not affect the nature of these evidence or information to remain state secrets and these evidence or information shall continue to be protected under the State Secrets Law.

7.18 The Commissioner noticed that there are differences in opinions given by the PRC law experts on the finer details in respect of whether all evidence and information furnished to SSB for investigation of a crime (whether they be actually used or not) could rightly fall within the definition of "state secrets". The PRC law experts however shared the consensus that any breach of the State Secrets Law is an offence carrying with it serious penal consequences[13].

7.19 In the circumstances, the Commissioner considers the following factors needed to be looked at:

7.19.1 The Information supplied by Yahoo! China to SSB might have been or could have been used for investigation of the crime in question;

7.19.2 The broad scope of definition given to "state secrets" and the powers vested in the relevant PRC authorities to so classify the data;

7.19.3 The trial of Mr. X's case was not conducted in public and no transcript of the trial is available. The Verdict setting out what it describes as undisputed facts is the only evidence that the Commissioner can safely rely;

7.19.4 There was no evidence to suggest that the Requested Data were not classified as state secrets; and

[13] See, for instance, the criminal sanction laid down in Article 111 of the PRC's Criminal Law for supplying state secrets to organization or individual outside the territory of China. Person convicted shall be sentenced to fixed term imprisonment of not less than 5 years but not more than 10 years.

7.19.5 Breach of State Secrets Law is a serious offence in PRC.

7.20 Having considered the above factors, the Commissioner accepts that YHHK's concerns for breach of the State Secrets Law are genuine and reasonable. The Commissioner therefore did not exercise power to compel YHHK for production of the Requested Data.

CHAPTER EIGHT

The Commissioner's Findings

Focus of Investigation

8.1 The relevant legal issues that concern the Commissioner in this investigation are:

8.1.1 **Personal data**: whether the Information disclosed to SSB amounts to "personal data" as defined by the Ordinance.

8.1.2 **Data user**: whether YHHK is a data user for the purposes of the Ordinance.

8.1.3 **Extra-territorial jurisdiction**: whether the Ordinance applies to an act of disclosure of personal data which was done entirely outside Hong Kong.

8.1.4 **DPP3**: whether the alleged disclosure of user information pursuant to the Order from SSB is within the original or directly related purpose of collection.

8.1.5 **Exemption in section 58**: whether the disclosure of personal data to a foreign law enforcement agency for investigation of a foreign crime could be exempted under section 58 of the Ordinance.

Undisputed Facts

8.2 The following facts are not in dispute :

8.2.1 The Email Account (being a ".cn" account) was registered in the PRC via Yahoo! China;

8.2.2 The Email Account was subscribed by a PRC user;

8.2.3 The Information was disclosed in the PRC by Yahoo! China pursuant to the Order issued by SSB;

8.2.4 YHHK was at the material time the legal owner of Yahoo! China in the PRC; and

8.2.5 Yahoo! Inc. owned YHHK.

Whether IP Address is "Personal Data" within the Definition of the Ordinance

8.3 In order to constitute "personal data" under the Ordinance, the data must satisfy the three criteria laid down in the Ordinance, namely, that (a) it relates 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. The word "practicable" is further defined under section 2(1) as "reasonably practicable".

8.4 According to the Verdict, the email user information furnished by YHHK to SSB was: -

> *"Account holder information furnished by Yahoo! Holdings (Hong Kong) Ltd., which confirms that for IP address 218.76.8.201 at 11:32:17 p.m. on April 20, 2004, the corresponding user information was as follows : user telephone number : 0731-4376362 located at the Contemporary Business News office in Hunan; address : 2F, Building 88, Jianxiang New Village, Kaifu District, Changsha."*

8.5 Question arises as to whether the information mentioned in the Verdict, without more, amounted to "personal data" and in particular, whether such information fulfills paragraphs (a) and (b) of the definition. Since no prescribed test on what amounts to "indirect" identification is provided under the Ordinance, the term itself tends to be conceptual.

8.6 In interpreting the law, the Commissioner takes a purposive approach in statutory interpretation in order to *"best ensure the attainment*

of the object of the Ordinance according to its true intent, meaning and spirit"[14] and to guard against any *"absurd"* result from arising[15].

8.7 In the Commissioner's view, under the first limb of the definition, data which relate "directly" to an individual are data which speak of or otherwise yield information about the individual directly. Data which relate "indirectly" to an individual are data from which information concerning the individual has to be inferred or indirectly inferred from the data when read in conjunction with other data.

8.8 As for the second limb of direct or indirect identification, if identification can be ascertained solely from the data in question (including information inferred from the data), the ascertainment is "direct". If identification can be ascertained only if recourse is made to other data readily obtainable by the data user, identification is "indirect". It is a question to be decided by the facts of the case. What is not readily obtainable by the data user is unlikely to fall within the benchmark of reasonable practicability.

8.9 Since the user information in the present case includes an IP address, the Commissioner has to consider whether an IP address *per se* is "personal data" under the Ordinance.

8.10 Basically, an IP address is a specific machine address assigned by the ISP to the user's computer and is therefore unique to a specific computer. Whenever a transaction requesting or sending data occurs on the Internet, this unique address accompanies the data. The information is about an inanimate computer, not an individual. An IP address alone can neither reveal the exact location of the computer concerned nor the identity of the computer user.

8.11 Applying the two limbs of the definition of "personal data", an IP address itself does not contain information that "relates" to an individual nor is the registered user's information readily obtainable, for example, through information available in the public domain. The

---

[14] See section 19 of the Interpretation and General Clauses Ordinance, Cap. 1, Laws of Hong Kong.

[15] The principle of *"presumption against absurdity"* in the golden rule of statutory interpretation, see Benion's *Statutory Interpretation*, third edition, Butterworths.

Commissioner therefore takes the view that an IP address *per se* does not meet the definition of "personal data".

8.12 The Commissioner has verified and sought advice from Senior Counsel who fully agreed that an IP address alone is not "personal data" but that "personal data" can include an IP address when combined with, for example, identifying particulars of an individual. Whether or not it is part of any personal data in a particular case depends on the facts of the case and the two limbs of the definition of "personal data" illustrated above.

8.13 Incidentally, the paper issued by the Legal Service Division of the Legislative Council Secretariat[16], titled *"Scope of 'personal data' under the Personal Data (Privacy) Ordinance (Cap. 486) and related issues"* also expressed a similar view that a restrictive approach is generally adopted by the courts in relation to whether IP addresses constitute "personal data". Applying the above reasoning, the *"IP address 218.76.8.201"* mentioned in the Verdict does not *per se* constitute "personal data".

8.14 As for the corresponding user information mentioned in the Verdict, i.e. "*user telephone number: 0731-4376362, the Contemporary Business News office in Hunan, address: 2F, Building 88, Jianxiang New Village, Kaifu District, Changsha"*, no safe conclusion can be drawn that the corresponding user information *ex facie* belongs to a living individual as opposed to a corporate or unincorporate body or relates to a real as opposed to a fictitious individual. In the circumstances, the Commissioner finds insufficient evidence to support that the two limbs of the definition of "personal data" are met.

Whether Personal Data were Disclosed by YHHK to SSB?

8.15 It was unclear from the Verdict what exactly was "*the account holder information"* furnished by YHHK. Yahoo! Inc. confirmed to the Commissioner that only the Information, i.e. *(i) user registration information, (ii) IP log-in information and (iii) certain email content* were provided to SSB. No contrary evidence or allegations came to sight

[16] See LC Paper No. LS21/05-06 at Annex B of this Report

during the course of investigation for the Commissioner to cast doubt on the admission made by Yahoo! Inc. or to draw any inference that personal data other than the Information were disclosed to SSB.

8.16 Having regard to:-

8.16.1 The views expressed in paragraphs 8.10 to 8.14 above (i.e. that IP address alone does not constitute "personal data" and no *ex facie* evidence from the Verdict that an individual with real identity was the registered account holder of the Email Account);

8.16.2 The fact that the email address of *huoyan-1989@yahoo.com.cn* itself does not disclose the identity of Mr. X;

8.16.3 YHHK had categorically denied that the subscriber to the Email Account was registered under the name of Mr. X and they had no knowledge that the user was in fact Mr. X; and

8.16.4 There is no other concrete evidence to refute the claims made by YHHK in paragraph 8.16.3 above,

the Commissioner finds it unsafe and unsatisfactory to conclude that Mr. X's personal data were contained in the Information which had been disclosed by YHHK to SSB.

8.17 On the basis of the above, the Commissioner can conclude his findings here. However, in view of the public concerns raised about the Incident, as an academic exercise, the Commissioner shall attempt to answer the following hypothetical questions on the assumption (which has not been proved) that "personal data" of Mr. X were disclosed by YHHK:

8.17.1 Whether YHHK is a "data user" in relation to the information disclosed to SSB?

8.17.2 Whether the Ordinance has extra-territorial application

to the act complained of?

8.17.3 If the Ordinance has jurisdiction over the act complained of, had YHHK contravened DPP3?

Whether YHHK is a "Data User" in relation to the Information Disclosed to SSB

8.18 Is YHHK a "data user" who should be held responsible for the disclosure under the Ordinance? A "data user" is defined under the Ordinance to mean one who *"either alone or jointly in common with other persons, **controls** the collection, holding, processing or use of the data"*. What constitutes "control" is not defined under the Ordinance. In the Commissioner's view, control can either mean the physical act of collection, holding, processing or using of the personal data or it can mean the ability of determining the purpose for which and the manner in which the data are to be collected, held, processed or used.

8.19 Although strictly speaking, the actual physical act of collection and disclosure of the personal data in question might not be committed by YHHK but by Yahoo! China in the PRC, YHHK was accountable to the act done under section 65(1) and (2) of the Ordinance no matter whether it was done by its employees (i.e. staff employed for providing service to Yahoo! China) or its agents (i.e. Beijing Yahoo! as its foreign investment vehicle operating Yahoo! China). This is reinforced by the undisputed fact that the YHHK Chop was appended onto the documents disclosing the Information. Insofar as outside parties are concerned, the purported authority of YHHK was therefore deemed given.

8.20 As for the ability to determine the purpose for which and the manner in which the data are to be collected, held, processed or used, the Commissioner finds the following facts of the case to be relevant for consideration:

8.20.1 Yahoo! China was a website, not a legal entity, nor was it something separate from YHHK which owned the website;

8.20.2 Control is evidenced by the Privacy Policy Statement ("**PPS**")[17] and Terms of Service ("**TOS**")[18] of Yahoo! China pursuant to which personal data were supplied or collected by or on behalf of YHHK from users, particularly when users logged-in online to register an email account;

8.20.3 It was with YHHK that the users entered into contractual relationship by subscribing to the PPS and TOS when opening their email accounts with Yahoo! China; and

8.20.4 The documents disclosing the Information with the YHHK Chop appended thereto showed that YHHK had the ability to control the disclosure of personal data.

8.21 YHHK argued that since the handling of email account user information was managed by Yahoo! China under the ultimate control of Yahoo! Inc., YHHK did not have "control" over the collection, holding, processing or use of the user information.

8.22 The Commissioner does not find YHHK's argument convincing. It is because at the material time when the Information was disclosed, YHHK owned 100% of the shareholding of Beijing Yahoo! that operated Yahoo! China. The division of labour and works of the Yahoo! group of companies (including those of the reporting lines of the legal teams within the Yahoo! group) are no more than internal and inter-companies management arrangement. Such arrangement does not affect or overshadow the fact that YHHK remained a legal entity that should be held responsible for all acts (including the act or practice of personal data management) and businesses carried out by YHHK in PRC.

---

[17] *"Yahoo! uses information for the following general purposes: to customize the advertising and content you see, fulfill your requests for products and services, improve our services, contact you, conduct research, and provide anonymous reporting for internal and external clients…"*

[18] *"Information Sharing & Disclosure: Yahoo! does not rent, sell, or share personal information about you with other people or nonaffiliated companies except to provide products or services you've requested, when we have your permission, or under the following circumstances:-… We respond to subpoenas, court orders, or legal process,…*

8.23 Having said that, it is still logical to infer that the test of control should be read subject to a proviso, namely, that the infringing act or practice must itself (namely, the act of disclosure of the Information to SSB) be capable of the subject of control in or from Hong Kong by the data user. In determining whether there was in any particular case any effective control or the ability to exercise control in or from Hong Kong by the data user, reference must be made not just to the position under Hong Kong law, but also to any applicable foreign law.

8.24 YHHK submitted that the disclosure of the Information to SSB was in compliance with Article 45. YHHK was obliged to comply in light of the criminal sanction attached to non-compliance.

8.25 Having assessed the situation by taking into account the advice given by the PRC law experts on the applicability of the PRC law (i.e. Article 45 and other laws and the Regulation on Telecom), the obligation of YHHK to comply with such law (i.e. being the legal person responsible for acts and businesses carried out in PRC) and the circumstances under which the Information was requested (i.e. through the Order), the Commissioner forms the view that the disclosure of Information in the circumstances of the case was not a voluntary act initiated by YHHK but was compelled under the force of PRC law. Such being the case, the control, if any, was vitiated by the operation of PRC law. The subject matter of the complaint (i.e. the disclosure of the Information to SSB) therefore fell outside the control of YHHK.

8.26 As YHHK had no control over the data disclosure, YHHK is not, for the purpose of this investigation "data user" as defined under section 2(1) of the Ordinance. It logically follows that the Ordinance has no application to the act of disclosure of the Information in PRC.

Whether the Ordinance has Extra-territorial Application to the Act Complained Of

8.27 In view of the fact that the subject matter of complaint arose and happened in the PRC, the Commissioner also considers the extra-territorial application, if any, of the Ordinance to the present case.

8.28 The Ordinance does not contain provisions conferring express extra-territorial application. In the absence of such provision, the territorial principle applies and the Ordinance does not extend to bind any act committed by a foreign party on foreign soil. The territorial principle is illustrated by Section 39(1)(d)[19] of the Ordinance in which it singles out a set of conditions to be fulfilled before the Commissioner can exercise his powers of investigation.

8.29 The conditions consist essentially of the territorial link that a complainant is present in Hong Kong, or was at the relevant time a resident of Hong Kong, or some relevant rights had been acquired in Hong Kong which in the Commissioner's opinion will be prejudiced by the act or practice complained of. Another condition is that *"the relevant data user was able to control, in or from Hong Kong, the collection, holding, processing or use of the personal data concerned"*. It suffices to find jurisdiction if any part of the data cycle was at the relevant time controlled by a relevant data user *"in or from"* Hong Kong.

8.30 The mere presence, without more, of a person in Hong Kong who has the ability to control his business abroad is generally not sufficient to attract or to enable the Commissioner to assume jurisdiction under the Ordinance in relation to personal data held and acts done by that person or his companies abroad that do not affect any person in or have any other connection with Hong Kong. That something "more", which may attract or enable the Commissioner to assume jurisdiction under the Ordinance, can consist of an act or acts of control exercised *"in or from Hong Kong"* by a person based in Hong Kong.

8.31 Applying the test of control mentioned above, where the data are outside but the controller is within the jurisdiction, there may be situations where such act of control *"in or from Hong Kong"* is precluded or lost as a result of the operation of applicable foreign law.

8.32 In the present case, the Commissioner accepts that the Information was released to SSB in the PRC pursuant to the Order. The disclosure was made under the name of YHHK with the appending of the YHHK Chop. The question as to the operation of the PRC laws and the

[19] See paragraph 5.1.5

duty to comply with the PRC laws in relation to the disclosure of the Information have been discussed in Chapter Seven above. The Commissioner comes to the view that the control on the disclosure of the personal data by YHHK, if any, had been precluded or lost as a result of the operation of the PRC laws.

8.33 Since none of the conditions mentioned in section 39(1)(d) of the Ordinance was satisfied and none of the act of collection, holding, processing and use of the personal data was proved to have been taken place in Hong Kong, the Commissioner comes to the conclusion that the matter complained of falls outside the jurisdiction of the Ordinance.

If the Ordinance had Jurisdiction over the Act Complained of, had YHHK Contravened DPP3?

8.34 In view of the public interest aroused by the Incident, the Commissioner endeavours to proceed further and poses the question: "If the Ordinance did apply to the act of disclosure, whether such act contravened DPP3?" In this connection, DPP3 provides in essence that unless with the prescribed consent of the data subject, personal data shall only be used for a purpose consistent with the original purpose of collection.

8.35 It is beyond doubt that no prescribed consent had been obtained from Mr. X prior to the disclosure of the Information to SSB. The question that the Commissioner shall look at is whether the disclosure fell within the original purpose of collection or its directly related purpose. In this respect the Commissioner finds it relevant to first look at the TOS and the PPS issued by Yahoo! China when personal data of email users were collected.

8.36 Since YHHK and Yahoo! Inc. could not provide the Commissioner with user registration information for the Email Account on the ground that this might infringe the PRC State Secrets Law, the Commissioner proceeds on the basis of the general standard provisions of the TOS and the PPS used by Yahoo! China and takes it that the same apply to the opening of the Email Account by Mr. X.

8.37 The standard terms of the PPS used by Yahoo! China (which are available on its website) states that personal information is collected and received when a user registers for or uses its services. Provision is made in the standard email user's account registration page for the user to provide, upon registration, name, email address, date of birth, sex, postal code, occupation, profession and personal interest. The PPS also states, *inter alia*, that information collected or received from the user's browser, including the IP addresses, "cookies" information, etc. will automatically be recorded in the server's logs. Besides, Yahoo! Mail includes senders' IP address in the "header" of outgoing emails. The PPS of Yahoo! China also states that the information of the users would be shared in compliance with court subpoena, legal order or in accordance with legal proceedings.

8.38 Users of Yahoo! China's webmail services are required to accept the TOS of YHHK prior to the use of their email accounts. The TOS expressly states that YHHK might share information in response to subpoenas, court orders and legal process. The users agree to such conduct as provided in the TOS for use of Yahoo! China, including non-disclosure of state secrets. The users also agree that Yahoo! China will act in accordance with PRC laws in retention and disclosure of the information.

8.39 The TOS and the PPS have specified the purposes of usage of the data and the classes of permitted transferees of the data to include law enforcement agencies.

8.40 The Commissioner sought advice from the PRC law experts and the advice given to him confirms that disclosure in the circumstances of the case was in compliance with the statutory obligation laid down in PRC laws. The general view taken by the Commissioner in respect of the application of DPP3 is that compliance with statutory requirement on disclosure of personal data is regarded as use for a purpose consistent with the purpose of collection and is thus allowed under DPP3. By adopting the same line of thought and also drawing reference to the advice given by the PRC law experts, the Commissioner is satisfied that the disclosure by YHHK in compliance with statutory requirement is obligatory and also proper in accordance with the TOS and PPS.

8.41 In the circumstances, the act of disclosure in question does not apparently fall foul of the provisions of DPP3.

8.42 However, where disclosure is only permitted but not required by law and that disclosure of the personal data may lead to adverse action being taken against the data subject by the law enforcement agencies, a data user must act with caution. Even if the Personal Information Collection Statement given by the data user is couched in terms wide enough to cover such act of voluntary disclosure on the part of the data user, the data user should also consider whether the exemption provisions under Part VIII of the Ordinance is applicable, thereby justifying disclosure.

Exemption in Section 58

8.43 In the present case, YHHK had put forward the argument on the application of the exemption provision under section 58(2). YHHK argued that the purpose of use of the personal data in the present case was for detection of crime and that the words *"crime"* and *"offenders"* in section 58(1) covered crime committed in another jurisdiction and offenders in another jurisdiction. Therefore, disclosure of personal data collected and controlled in another jurisdiction because of the need to comply with the law of that jurisdiction must, by virtue of section 58(2), be exempted from DPP3.

8.44 An exemption under section 58 if properly invoked will have the effect of exempting from the application of DPP3 when the following criteria are satisfied, namely,

8.44.1 The use of the data is for any of the purposes specified in section 58(1); and

8.44.2 The application of DPP3 to such use would be likely to prejudice any of those purposes.

8.45 Section 58(1)(a) and (b) of the Ordinance provide the exempted purposes of *"the prevention or detection of crime"* and *"the apprehension, prosecution or detention of offenders"*. The word *"crime"* is not defined in the Ordinance. Nor is there any provision in the Ordinance dealing

with crimes or offences or other unlawful acts under foreign laws. In deciding whether to adopt the broad approach as suggested by YHHK, the Commissioner has studied other relevant statutes in Hong Kong and has also sought Senior Counsel's advice on the proper interpretation to take.

8.46 In Hong Kong, the Mutual Legal Assistance in Criminal Matters Ordinance, Cap. 525 ("**MLA Ordinance**") regulates the provision and obtaining of assistance in criminal matters between Hong Kong and places outside Hong Kong; and for matters incidental thereto or connected therewith. Section 5(1)(g) of the MLA Ordinance provides: "*A request by a place outside Hong Kong for assistance under this Ordinance shall be refused if, in the opinion of the Secretary for Justice, the request relates to an act or omission that, if it had occurred in Hong Kong, would not have constituted a Hong Kong offence*".

8.47 This reflects an important public policy consideration that cannot be simply brushed aside when construing "crime" or "offenders" in section 58. The Commissioner finds it a sensible, prudent and reasonable stance to take in construing the words "*crime*" or "*offenders*" under section 58(1)(a) and (b) of the Ordinance to represent crime or offence under Hong Kong laws though they are also wide enough to include those cases to which MLA Ordinance is applicable.

8.48 Thus, where any part of a data processing cycle took place in Hong Kong and a data user takes the voluntary step to furnish personal data held and controlled by it to a foreign law enforcement agency in respect of a foreign crime or offence, it is doing so at its own peril if it turns out that the act or omission alleged, though a crime under foreign law, does not constitute a Hong Kong offence had the act or omission occurred in Hong Kong.

8.49 Applying the above approach to the present case, since the crime committed by Mr. X in the PRC does not amount to a crime under the current Hong Kong laws, had YHHK been in control over the use of the personal data in or from Hong Kong, YHHK would not have been successful in invoking section 58(2) in exempting the application of DPP3 to justify its act of disclosure in question for "*the prevention or detection of crime*" or "*the apprehension, prosecution or detention of offenders*".

Conclusion

8.50 The crux of the complaint in the present case is :

8.50.1 Whether "personal data" was disclosed by YHHK; and

8.50.2 Whether YHHK as data user had breached the provisions of the Ordinance in disclosing the "personal data" of Mr. X.

8.51 Issues that the Commissioner regards to be of particular importance are the concept of control in respect of a data user and the question of extra-territorial jurisdiction, if any, of the Ordinance, to the action complained of. Mixed questions of facts and laws are involved.

8.52 The investigation works have been rendered difficult owing to the absence of any direct evidence from Mr. X and the unavailability of the Requested Data.

8.53 The difficulties notwithstanding, the Commissioner's Office has gathered as far as practicable all the other relevant information from YHHK and Yahoo! Inc. The Commissioner has compared Hong Kong law with overseas privacy laws through discussion and exchange of correspondence with his overseas counterparts. He has also sought legal advice from a Senior Counsel and two PRC law experts. Based on the available evidence and information before him, the Commissioner concludes that "personal data" of Mr. X had not been proved to have been disclosed by YHHK to SSB.

8.54 In the circumstances, the Commissioner is of the opinion that there has been no contravention of the requirements of the Ordinance by YHHK.

8.55 Under section 47(4) of the Ordinance, the complainant, Mr. X has a right to appeal to the Administrative Appeals Board against the Commissioner's decision made in this report.

CHAPTER NINE

Comments Arising from the Investigation

Scope of Application of the Ordinance

9.1 The Incident gives rise to the following causes of concern on the scope of application of the Ordinance to the following situations:

9.1.1 Where none of the act of collection, holding, processing and use of the personal data takes place in Hong Kong; and

9.1.2 Where disclosure of personal data is made pursuant to a lawful requirement imposed by a foreign authority for the purpose of investigation of a foreign crime.

9.2 The Ordinance as it currently stands does not provide a simple or easy answer to the above questions. The question in paragraph 9.1.1 above is to be answered from the perspectives of the definition of "data user" and the extra-territorial application, if any, of the Ordinance, whereas the question in paragraph 9.1.2 is to be looked at by reference to the definition of "crime" in the Ordinance. These issues which are pertinent to the present complaint have been addressed by the Commissioner in his findings in Chapter Eight.

9.3 In the light of his findings and with a view to enhance the effective and efficient operation of the Ordinance, the Commissioner finds it an opportune time to review the sufficiency of the provisions of the Ordinance in these areas.

Extraterritorial Application of the Ordinance

9.4 The keynote is the word "control" which appears both in the definition of "data user" under section 2(1) of the Ordinance as well as under section 39(1)(d)(i)(B) in respect of restrictions on investigations initiated by complaints. A statutory definition is lacking to give a clear

meaning to the word "control". While being fully cognizant of the borderless nature of the exercise of control particularly in the electronic age, the Commissioner acknowledges that control is not confined to the physical act of collection, holding, processing or use of the personal data in Hong Kong but can extend to cover the ability of the data user in determining *"in or from Hong Kong"* the purpose for which and the manner in which any data is to be collected, held, processed or used.

9.5 The power of control possessed by a data user could, however, be lost or vitiated as a result of the act or practice of the data user done or engaged in outside Hong Kong if such act or practice is required by an applicable foreign law. Similar view has been expressed in some overseas privacy legislations[20].

9.6 Insofar as any part of the data processing cycle is within the power of control of the data user *"in or from Hong Kong"*, it provides the territorial link that makes it fall within the precinct of the Ordinance for which due compliance is required. The legislative spirit is reflected in section 33 of the Ordinance concerning prohibition on transborder flow of personal data. Although section 33 is not yet operative, it is clearly provided in subsection (1) thereof that it applies to personal data the collection, holding, processing or use of which takes place in Hong Kong; or is controlled by a data user whose principal place of business is in Hong Kong. It should, however, be noted that section 33 must be premised on the fact that the personal data are held in Hong Kong before being transferred overseas.

9.7 Thus, a data user is not to be exonerated from the obligation to protect personal data that were transferred outside Hong Kong. The data user shall ensure compliance with the requirements under the Ordinance, in particular, the DPPs and be accountable for any improper handling of the personal data in question.

9.8 The Commissioner has made reference to overseas privacy legislations which show that existence of certain territorial link is required

---

[20] For example, section 13D(1) of the Australian Privacy Act, 1988 provides that *"…an act or practice of an organization done or engaged in outside Australia and an external Territory is not an interference with the privacy of an individual if the act or practice is required by an applicable law of a foreign country"*.

for the legislation to attract jurisdiction. For example, in Australia, under the Privacy Act 1988, there is express provision[21] which extends the application of the Privacy Act to acts done outside Australia by an organization provided that:

9.8.1 there is certain specified link with Australia, such as incorporation, location of central management and control in Australia, citizenship, etc; and

9.8.2 where the personal information relates to an Australian citizen or a person whose continued presence in Australia is not subject to a limitation as to time imposed by law.

9.9 In New Zealand, the extra-territorial provision under the Privacy Act of 1993 applies to information held by an agency which includes information that has been *"transferred out of New Zealand"* by that agency[22].

9.10 In the United Kingdom ("**UK**"), the Data Protection Act 1998 confines its application to a data controller which is *"established"* in the UK[23] and the data are *"processed in the context of that establishment"*. The term *"established"* is in turn defined to mean an individual who is ordinarily resident in the UK or a body incorporated under the law of UK.

9.11 The Commissioner finds territorial link exists where any part of the data processing cycle takes place in Hong Kong and that a data user does not relinquish control if any part of the data processing cycle was controlled by it in or from Hong Kong, for instance, where the data were collected in Hong Kong by the data user but were subsequently transferred by it outside Hong Kong for data processing.

9.12 Conversely, where a Hong Kong resident who has the ability to control his business abroad, say in the PRC but none of the act of collection, holding, processing or use of the personal data in relation to his

[21] Section 5B of the Privacy Act, 1988
[22] Section 10 of the Privacy Act, 1993
[23] Section 5 of the Data Protection Act 1998

business undertaking takes place in Hong Kong, should such personal data so obtained in the course of his overseas business be caught under the purview of the Ordinance? These issues arising from this complaint give food for thoughts for Government to consider legislative amendments in order to quell any uncertainty hinging around the meaning of "control" of personal data and the application of the Ordinance.

The Definition of "Crime"

9.13 Following the reasoning given in paragraphs 8.43 to 8.49 of this Report, the Commissioner finds it desirable to have a clear definition of the word "crime" in the Ordinance. In the absence of a clear definition, it would be difficult for the data user to assess whether an exemption provision under sections 58(1) and (2) can be properly invoked, especially when it is requested by, say, an overseas law enforcement agency to disclose certain personal data for the purpose of investigation of a foreign crime.

9.14 Reference has been drawn to provisions found in some overseas privacy legislations. For instance, in Australia, disclosure of personal information by a private sector organization is allowed under Privacy Principle 2.1(g) of the *Australian Privacy Act, 1988* when it is "*required or authorized by or under any law*". The Mutual Assistance Criminal Matters Act enables the Commonwealth to provide international assistance in criminal matters upon request of a foreign country and disclosure pursuant thereto is viewed as "authorized by law" covered by the Australian Privacy Act.

9.15 In New Zealand, an exception to disclosure of personal information is provided under Information Privacy Principle 11(e) which allows disclosure "*to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution and punishment of offences*". The term "*public sector agency*" is further defined under section 2 of the Privacy Act 1993 in a way that it could only be New Zealand public body.

9.16 In order to give clearer guidance to data user and for better protection of personal data privacy, the Commissioner proposes that the

word “crime” in the Ordinance be defined to mean Hong Kong crime and also to cases where the MLA Ordinance is applicable. Hence an overseas crime will fall outside the ambit of the Ordinance if such act or omission, had it occurred in Hong Kong, has not constituted a criminal offence in Hong Kong. With a clear definition in place, it will facilitate the data user to assess and determine whether the exemption provision under sections 58(1) and (2) of the Ordinance can be properly invoked in any particular circumstances of the case especially when personal data is requested to be disclosed to an overseas law enforcement agency or regulatory body which might lead to the taking of adverse action against the data subject concerned.

9.17 Similar consideration should also be given to the meaning of the word “*offenders*” in section 58(1)(b) of the Ordinance.

Consideration by Policy Bureau

9.18 The Commissioner shall bring to the attention of the Home Affairs Bureau issues emanating from this Report and it is hoped that the Government will give due consideration to the need to review and amend the Ordinance for effective enforcement and guidance to data users and data subjects alike.

GLOSSARY

Alibaba	*Alibaba.com Corporation*
Article 2	*Article 2 of the PRC State Secrets Law*
Article 18	*Article 18 of the PRC State Security Law*
Article 45	*Article 45 of the PRC Criminal Procedure Law*
Article 277	*Article 277 of the PRC Criminal Law*
Beijing Yahoo!	*Beijing Yahoo! Consulting and Service Company Limited*
Commissioner	*The Privacy Commissioner for Personal Data*
DPP	*Data Protection Principles in Schedule 1 to the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong*
Email Account	*The email account "huoyan-1989@yahoo.com.cn" from which materials classified as state secrets were sent to foreign entities*
ICP	*Internet Contents Provider*
Incident	*The incident leading to the conviction of Mr. X for providing state secrets to foreign entities*
Information	*The "user registration information, IP log-in information and certain email contents" disclosed to the State Security Bureau, PRC*
IP address	*Internet Protocol address*
ISP	*Internet Service Provider*

GLOSSARY

MLA Ordinance	*Mutual Legal Assistance in Criminal Matters Ordinance, Chapter 525, Laws of Hong Kong*
Mr. X	*The complainant of this investigation*
Mr. Y	*Senior Vice President and General Counsel of Yahoo! Inc.*
Operation Agreement	*The Agreement dated 19 February 2003 entered between YHHK and PUFG for provision of ICP licence for Yahoo! China*
Order	*The data disclosure order issued by State Security Bureau pursuant to Article 45 of the PRC Criminal Procedure Law*
Ordinance	*Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong*
Panel	*Panel on Information Technology and Broadcasting of the Legislative Council*
People's Court	*Changsha Intermediate People's Court, PRC*
PPS	*Privacy Policy Statement of Yahoo! China*
PRC	*People's Republic of China*
PRC law experts	*The two experts retained by the Commissioner to provide PRC law advice*
PUFG	*Peking University Founder Group*
Regulation on Telecom	*The PRC Regulation on Telecommunications*

GLOSSARY

Requested Data	*The data that the Commissioner had requested YHHK to provide : (i) the account user's information in respect of the Email Account, (ii) the correspondence with SSB, (iii) the Information, and (iv) the Order*
SSB	*State Security Bureau, PRC*
Technical Services Agreement	*The Agreement dated 19 February 2003 entered into between Beijing Yahoo! and PUFG for provision of technical services to facilitate the operation of Yahoo! China*
TOS	*Terms of Service of Yahoo! China*
UK	*United Kingdom*
US	*United States*
Verdict	*The verdict delivered by the Changsha Intermediate People's Court on 27 April 2005*
Yahoo! China	*The website of Yahoo! China : "http://www.yahoo.com.cn"*
Yahoo! China Customer Care Team	*The customer care team of Yahoo! China website*
Yahoo! China Legal Team	*The legal team of Yahoo! China*
Yahoo! Hong Kong	*The website of Yahoo! Hong Kong : "http://www.yahoo.com.hk"*
Yahoo! Inc.	*The ultimate parent of YHHK, a company based in California, US*

GLOSSARY

Yahoo! Inc. Legal Team	*The legal team of Yahoo! Inc.*
YHHK	*Yahoo! Holdings (Hong Kong) Limited, presently known as Yahoo! Hong Kong Limited*
YHHK Chop	*The company chop of YHHK*

湖南省长沙市中级人民法院

刑事判决书

（2005）长中刑一初字第29号

公诉机关湖南省长沙市人民检察院.

被告人[redacted]，化名"198964"，男，1968年7月25日出生于宁夏回族自治区盐池县，汉族，大学文化，无业，住山西省太原市[redacted]。因涉嫌犯为境外非法提供国家秘密罪，于2004年11月24日被抓获，次日被刑事拘留，同年12月14日被逮捕。现押长沙市看守所。

委托辩护人[redacted]，上海市天易律师事务所律师。

长沙市人民检察院以长检刑诉字（2005）第13号起诉书指控被告人[redacted]犯为境外非法提供国家秘密罪一案，于2005年1月31日向本院提起公诉。本院依法组成合议庭，不公开开庭审理了本案，长沙市人民检察院指派代理检察员[redacted]出庭支持公诉，被告人[redacted]及其辩护人[redacted]等到庭参加诉讼。现已审理终结。

长沙市人民检察院指控，2004年2月11日至同年4月22日期间，被告人[redacted]受聘湖南省当代商报社，任编辑部主任。同年4月20日下午5时许，湖南省当代商报社副总编[redacted]；[redacted]

[redacted]在例行评报会和编前会后，又召集该报社要闻部、热线机动部、编辑部等部门负责人参加了一个专门会议。在该专门会上，[redacted]口头传达了属于绝密级国家秘密的中共中央办公厅、国务院办公厅《关于当前稳定工作的通知》（中办发[2004]11号）的重要内容摘要，并强调该文件属于绝密文件，不能记录、传播，但被告人[redacted]私自将此重要内容摘要作了记录。同日下午19时许至凌晨2时许，被告人[redacted]在其办公室，通过其个人的电子邮箱 huoyan-1989@yahoo.com.cn，向位于美国纽约的“民主亚洲基金会”筹设人之一、境外网站“民主论坛”及电子刊物《民主通讯》主编[redacted]的电子邮箱[redacted]发送了其私自记录的上述中办发[2004]11号文件的重要内容摘要，并将提供者化名为“198964”，同时要求[redacted]尽快想办法发出去，但不要用[redacted]的名字。当日，署名“198964”提供的上述中办发[2004]11号文件的重要内容摘要在《民主论坛》刊登发表，此后又被“博讯”、“中国民主正义党”等境外网站转载发表。

对指控的上述事实，公诉机关提供了证人证言、密级鉴定书、相关物证、书证、抓获经过材料、现场照片及物证照片、被告人的身份证明材料、被告人的供述等证据证实，该院认为，被告人[redacted]的行为已触犯《中华人民共和国刑法》第一百一十一条之规定，构成为境外非法提供国家秘密罪，向本院提起公诉，要求依法判处。

被告人[redacted]及其辩护人对起诉书指控的犯罪事实及本案的

定性不持异议。被告人[redacted]辩解："其为境外非法提供国家秘密的犯罪行为不属于情节特别严重。"其辩护人辩称："鉴于被告人[redacted]的行为并未给国家安全和利益造成极其严重的危害后果和认罪态度好，请求对其从轻处罚。"

经审理查明：被告人[redacted]于2001年4月与境外网站"民主论坛"及电子刊物《民主通讯》的主编[redacted]（中国台湾省人，居住美国纽约，系"民主亚洲基金会"的筹设人之一）相识。2004年4月20日下午5时许，湖南省当代商报社副总编[redacted]、[redacted]在例行评报会和编前会后，又召集该报社要闻部、热线机动部、编辑部等部门负责人开会，时任该报社新闻中心和编辑中心主任的[redacted]参加了会议。[redacted]在会上口头传达了属于绝密级国家秘密的中共中央办公厅、国务院办公厅《关于当前稳定工作的通知》（中办发[2004]11号）的重要内容摘要，并强调该文件属于绝密文件，不能记录，不要传播。被告人[redacted]将此重要内容摘要作了记录。[redacted]发现[redacted]在作记录，就提醒[redacted]不能作记录，但[redacted]仍在记录本上作了详细记录。当日晚23时32分许，被告人[redacted]为向境外敌对分子通风报信，利用其独自在办公室值班之机电话上网，通过其个人的电子邮箱 huoyan-1989@yahoo.com.cn 向境外敌对分子[redacted]的电子邮箱[redacted]发送了其记录的上述中办发[2004]11号文件的重要内容摘要，并将提供者化名为"198964"，同时要[redacted]尽快想办法发出去，但不要用[redacted]的名字。当日，署名为"198964"提供的上述中办发

[2004]11 号文件的重要内容摘要在《民主通讯》上刊登发表，此后又被“博讯”、“中国民主正义党”等境外网站转载发表。

证明上述事实的证据有：1、国家保密局作出的密级鉴定书，证实被告人[redacted]为境外非法提供的国家秘密的材料内容与“中办发[2004]11 号文件（绝密级）中的小标题内容基本一致，泄露了中办发[2004]11 号文件的基本内容，应当属于绝密级国家秘密；2、书证：①、被告人[redacted]于 2004 年 4 月 20 日 23 时使用其个人的电子邮箱 huoyan-1989@yahoo.com.cn 通过互联网将中办发[2004]11 号文件内容摘要发送给境外敌对分子[redacted]的电子邮箱[redacted]的电子邮件一封，内容大意为[redacted]要[redacted]尽快想办法将中办发[2004]11 号文件发出去，但提供者不要用[redacted]的名字，而是化名为“198964”，后附有文件摘要内容；②、通过互联网下载的在《民主通讯》、“博讯”、“中国民主正义党”等境外网站和电子刊物刊登发表的署名为“198964”者提供的中办 11 号文件摘要的资料，该资料经被告人[redacted]辨认，确认与其所提供的国家秘密的内容一致；③、从互联网上下载的敌对分子[redacted]的身份资料，证实[redacted]是中国台湾人，居住在美国纽约，系“民主亚洲基金会”的筹设人之一，系境外网站“民主论坛”及电子刊物《民主通讯》的主编；3、取证笔录、物证笔记本，证实 2004 年 12 月 6 日，被告人[redacted]的妻子[redacted]从其家中找到的[redacted]记录有中办 11 号文件摘要内容的笔记本交给公安机关的事实，及被告人[redacted]的笔记本上记载有“4 月 20 日开会

传达宣传部文件（绝密文件）（中办 11 号文件），中办关于当前稳定工作的通知。”等文字，后附有文件摘要内容。该笔记本经被告人[redacted]的辨认，确认系其所作的记录；4、雅虎香港控股有限公司出具的关于用户资料的证明材料，证实 IP 地址：218.76.8.201，时间：2004 年 4 月 20 日 23 时 32 分 17 秒的对应用户资料如下：用户电话：0731-4376362，湖南《当代商报》社。地址：长沙市开福区建湘新村 88 栋 2 楼；5、现场照片及相关物证、书证照片；6、物证：①、境外敌对分子[redacted]作为稿费寄给被告人[redacted]的支票一张及信封一件；②、被告人[redacted]的另一本笔记本，上记载有境外敌对分子[redacted]的电子邮箱号码；③证人[redacted]、[redacted]的笔记本，上均记载有中办 11 号文件的摘要内容；7、证人[redacted]、[redacted]、[redacted]的证言，证实 2004 年 4 月 20 日下午 5 时许，[redacted]在专门召集报社部门负责人开会的会议上，口头传达了中办发[2004]11 号文件的重要内容摘要，并强调该文件属于绝密文件，不要传播。被告人[redacted]参加会议并作了记录，[redacted]发现[redacted]在作记录，就专门提醒[redacted]不要作记录的事实以及被告人[redacted]在当晚值班的事实；8、证人[redacted]、[redacted]、[redacted]、[redacted]的证言，证实报社负责人在传达省委宣传部的重要精神的文件时，如强调不能传播，是绝密文件，作为一名新闻工作者均会将该文件视为国家秘密的事实；9、抓获经过材料；10、被告人[redacted]的身份证明材料；11、当代商报社招聘人员登记表，证实被告人[redacted]于 2004 年 2 月 11 日至 2004 年 4 月 22

日受聘于湖南当代商报社的事实；12、被告人[redacted]的手写自诉材料及供述，均对其故意为境外非法提供国家秘密的犯罪事实供认不讳。上述证据相互印证，足以认定本案事实。

本院认为，被告人[redacted]为向境外敌对分子通风报信，故意非法将其所知悉的属于绝密级的国家秘密提供给境外的机构，危害国家安全，属情节特别严重，其行为已构成为境外非法提供国家秘密罪。故公诉机关指控被告人[redacted]的行为构成为境外非法提供国家秘密罪的罪名成立。被告人[redacted]辩解："其为境外非法提供国家秘密的犯罪行为不属于情节特别严重。"经查，最高人民法院《关于审理为境外窃取、刺探、收买、非法提供国家秘密具体应用法律若干问题的解释》第二条第（一）项中规定，为境外窃取、刺探、收买、非法提供绝密级国家秘密的，属于"情节特别严重"，被告人[redacted]为境外非法提供的国家秘密已经国家保密局鉴定为绝密级国家秘密，其行为应认定为情节特别严重，故此辩解本院不予采纳。其辩护人辩称："鉴于被告人[redacted]的行为并未给国家安全和利益造成极其严重的危害后果和认罪态度好，请求对其从轻处罚。"经查，与事实相符，故此辩护意见本院予以采纳。据此，依照《中华人民共和国刑法》第一百一十一条、第五十五条第一款、第五十六条第一款之规定，判决如下：

被告人[redacted]犯为境外非法提供国家秘密罪，判处有期徒刑十年，剥夺政治权利二年。

（刑期从判决执行之日起计算，判决执行以前先行羁押的，

羁押一日折抵刑期一日，即自 2004 年 11 月 24 日起至 2014 年 11 月 23 日止）

如不服本判决，可在收到本判决书后的第二日起十日内，通过本院或直接向湖南省高级人民法院提出上诉，书面上诉的，应提交上诉状正本一份，副本两份。

审 判 长 [redacted]

审 判 员 [redacted]

代理审判员 [redacted]

二〇〇五年 [redacted] 十七日

本件与原本核对无异

书 记 员 [redacted]

Changsha Intermediate People's Court of Hunan Province
Criminal Verdict

Changsha Intermediate Criminal Division One First Trial Case No. 29 (2005)

Prosecuting organ is the Changsha People's Procuratorate of Hunan Province.

Defendant [redacted] a.k.a. "198964," male, born on July 25, 1968 in Yanchi County in Ningxia Hui Autonomous Region, Han ethnicity, university graduate, unemployed, resided [redacted] in Taiyuan, Shanxi Province. Because he was suspected of committing the crime of illegally providing state secrets to foreign entities, he was taken into custody on November 24, 2004, placed under criminal detention on the following day, and arrested on December 14 of the same year. He is currently being held in custody at the Changsha Detention Center.

Authorized defense attorney is [redacted], a lawyer with the Tianyi Law Firm in Shanghai.

In Changsha Procuratorate Criminal Indictment No. 13 (2005), the Changsha People's Procuratorate charged defendant [redacted] with committing the crime of illegally providing state secrets to foreign entities, and on January 31, 2005 it sent the case to this court for prosecution. This court formed a collegiate bench according to law and held a closed trial to hear this case. The Changsha People's Procuratorate sent procurator Su Shuangji to court to support the prosecution. Defendant [redacted] and his defense attorney [redacted] were also in court to participate in the proceedings. This trial has now been concluded.

The Changsha People's Procuratorate charged that, from February 11 to April 22, 2004, defendant [redacted] was employed by Hunan's *Contemporary Business News*, where he held the position of head of the Editorial Department. At around 5:00 on the afternoon of April 20, after a routine newspaper review meeting and a pre-editorial meeting, assistant editors-in-chief of *Contemporary Business News* [redacted] and [redacted] convened a special meeting of the heads of the newspaper's Front Page News Department, the Mobile Hotline Department, and the Editorial Department. During this special meeting, [redacted] verbally communicated a summary of the main contents of a top-secret document issued by the General Office of the Central Committee of the Communist Party of China (CPC) and the General Office of the State Council entitled "A Notice Regarding Current Stabilizing Work" (CPC General Office Document No. 11 [2004]). He also emphasized that this was a top-secret document and that notes must not be taken on it and that it should not be disseminated. However, defendant [redacted] secretly did take notes on the summary of the document's main content. Between approximately 7:00 pm on that day and approximately 2:00 am the following morning, defendant [redacted] used his personal email account (huoyan-1989@yahoo.com.cn) in his office to send the notes he had secretly taken on the above-mentioned summary of the main contents of CPC General Office Document No. 11 (2004) to the email account of [redacted], one of the founders of the "Asia Democracy Foundation" located in New York, USA and editor-in-chief of the foreign web site "Democracy Forum" and the electronic publication "Democracy News." He gave "198964" as the alias of the person who provided the document and asked [redacted] to find a way to distribute it as quickly as possible without using [redacted]'s name. That day, the above-mentioned summary of the main contents of CPC General Office Document No. 11 (2004) was posted for publication on the "Democracy Forum" under the name of "198964." It was later reposted for publication on other foreign web sites such as "Boxun News" and the "China Democracy & Justice Party."

Regarding the above-mentioned facts as charged, the prosecuting organ provided such corroborating evidence as the oral testimony of witnesses, a secrecy-degree verification certificate, related material and written evidence, materials on the process of taking [redacted] into custody, photos of the crime scene and photos of material evidence, information proving the defendant's identity, and the defendant's confession. The procuratorate maintains that defendant [redacted]'s actions violated Article 110 of the "Criminal Law of the PRC" and that his actions constitute the crime of illegally providing state secrets outside of the country. It has sent the case to this court for prosecution, requesting that a verdict be passed according to law.

Neither defendant [redacted] nor his defense attorney raised any objections to the criminal facts as charged in the indictment or to the characterization of this case. Defendant [redacted] argued in his defense: "My criminal act of providing state secrets to foreign entities did not involve especially serious circumstances." His defense attorney stated: "Considering that defendant [redacted]'s actions did not cause extremely serious damage to state security or interests and that his attitude in admitting his crimes was good, please punish him leniently."

In the course of the trial it was determined that: In April 2001, defendant [redacted] made the acquaintance of [redacted] (from China's Taiwan Province, resident of New York in the USA, and one of the founders of the Asia Democracy Foundation), editor-in-chief of the foreign web site "Democracy Forum" and the electronic publication "Democracy News." At approximately 5:00 on the afternoon of April 20, 2004, after a routine newspaper review meeting and a pre-editorial meeting, assistant editors-in-chief of *Contemporary Business News* [redacted] and [redacted] convened a meeting of senior staff of the newspaper's Front Page News Department, the Mobile Hotline Department, and the Editorial Department. [redacted] then head of the newspaper's News Center and Editorial Center, attended the meeting. During the meeting, [redacted] verbally communicated a summary of the main contents of a top-secret document issued by the General Office of the Central Committee of the Communist Party of China (CPC) and the General Office of the State Council entitled "A Notice Regarding Current Stabilizing Work" (No. 11 [2004] issued by the CPC General Office). He emphasized that this was a top-secret document and that notes must not be taken on it and that it should not be disseminated. Defendant [redacted] took notes on this summary of the document's main contents. When [redacted] discovered that [redacted] was taking notes, he reminded [redacted] that he was not allowed to take notes. However, [redacted] still made detailed notes in his notebook. That night at approximately 11:32 pm, defendant [redacted] leaked this information to an overseas hostile element, taking advantage of the fact that he was working overtime alone in his office to connect to the internet through his phone line and use his personal email account (huoyan-1989@yahoo.com.cn) to send his notes on the above-mentioned summary of the main contents of CPC General Office Document No. 11 (2004). He also used the alias "198964" as the name of the provider and asked [redacted] to find a way to distribute the information as quickly as possible without using [redacted]'s name. That day, the above-mentioned summary of the main contents of CPC General Office Document No. 11 (2004) was posted for publication on the "Democracy Forum" under the name of "198964." It was later reposted for publication on other foreign web sites such as "Boxun News" and the "China Democracy & Justice Party."

The evidence demonstrating the above criminal facts is as follows: 1. A secrecy-degree verification certificate issued by the State Secrecy Bureau, which confirms that the sub-headings of the state secret materials illegally provided by defendant [redacted] to foreign entities were basically the same as those in CPC General Office Document No. 11 (2004) (top-secret level) and that the basic content of CPC General Office Document No. 11 (2004) that was leaked should be classified as top-secret level state secrets. 2. Material evidence: (i) An email sent by [redacted] at 11:00 p.m. on April 20, 2004 using his personal email account (huoyan-1989@yahoo.com.cn), in which he sent the summary of the contents of CPC General Office Document No. 11 (2004) to the email account of overseas hostile element [redacted] [redacted]. The general idea of the email was that [redacted]

wanted [redacted] to find a way to distribute CPC General Office Document No. 11 (2004) as quickly as possible but that he should use "198964", rather than [the name] [redacted], as the name of the document's provider; the summary of the document was attached at the end. (ii) The summary of CPC General Office Document No. 11 (2004), downloaded from the Internet, where it was posted on foreign web sites and electronic publications such as "Democracy Forum," "Boxun News," and "China Democracy & Justice Party" under the name of "198964." These materials were identified by defendant [redacted], confirming that these materials were the same as the state secrets that he provided. (iii) Materials downloaded from the Internet that identify hostile element [redacted] and confirm that [redacted] is from China's Taiwan Province, resides in New York in the USA, is a founder of the Asia Democracy Foundation, and is editor-in-chief of the foreign web site "Democracy Forum" and the electronic publication "Democracy News." 3. Notes on evidence-taking and the material evidence of a notebook, confirming the fact that on December 6, 2004, defendant [redacted]'s wife [redacted] provided the state security organ with a notebook found in their home containing [redacted]'s notes on the summary of CPC General Office Document No. 11 (2004). There was also a note recorded in [redacted]'s notebook reading"Meeting on April 20 to relay Propaganda Department document (top-secret) (CPC General Office Document No. 11 [2004]), notice from the CPC General Office regarding current stabilizing work," with a summary of the document appended at the end. This notebook was identified by defendant [redacted], confirming that he was the person who made the notes. 4. Account holder information furnished by Yahoo Holdings (Hong Kong) Ltd., which confirms that for IP address 218.76.8.201 at 11:32:17 p.m. on April 20, 2004, the corresponding user information was as follows: user telephone number: 0731-4376362 located at the *Contemporary Business News* office in Hunan; address: 2F, Building 88, Jianxiang New Village, Kaifu District, Changsha. 5. Photos taken at the scene and photos of related material evidence and written evidence. 6. Material evidence: (i) One envelope and one check sent by overseas hostile element [redacted] to defendant [redacted] as payment for a manuscript. (ii) Another notebook of defendant [redacted]'s, in which was written the email address of overseas hostile element [redacted] (iii) The notebooks of witnesses [redacted] and [redacted], in both of which was written information on CPC General Office Document No. 11 (2004). 7. The testimony of witnesses [redacted], [redacted], and [redacted], confirming that at approximately 5:00 on the afternoon of April 20, during a meeting especially convened by [redacted] of the newspaper's department heads, he verbally communicated a summary of the main contents of CPC General Office Document No. 11 (2004) and emphasized that it was a top-secret document that should not be disseminated; that defendant [redacted] attended the meeting and took notes; that when [redacted] discovered that [redacted] was taking notes, he especially reminded [redacted] of the fact that he was not supposed to take notes; and that defendant [redacted] worked the night shift that night. 8. The testimony of witnesses [redacted], [redacted], [redacted], and [redacted], confirming that, when the department heads of the newspaper passed on the main points of a document issued by the Provincial Committee's Propaganda Department, if it had been emphasized not to circulate it and that it was a top-secret document, as newspaper employees they would all have regarded that document as a state secret. 9. Materials on the process of taking [redacted] into custody. 10. Defendant [redacted]'s identity papers. 11. A *Contemporary Business News* employee registration form, confirming that defendant [redacted] was employed by Hunan's *Contemporary Business News* from February 11, 2004 to April 22, 2004. 12. Written statements given by [redacted], and his confession, confirming that he confessed completely to the fact

that he intentionally and illegally provided state secrets to foreign entities. The above items of evidence corroborate with each other and are sufficient to establish the facts of this case.

This court finds that, in order leak information to hostile elements outside of the country, defendant [redacted] intentionally and illegally provided information that he knew to be top-secret level state secrets to an entity outside of the country. Having endangered state security and involving especially serious circumstances, his actions constitute the crime of illegally providing state secrets to foreign entities. Therefore, the court accepts the prosecution's charge that [redacted]'s actions constitute the crime of illegally providing state secrets to foreign entities. Defendant [redacted] argued in his defense: "My criminal act of providing state secrets to foreign entities did not involve especially serious circumstances." This was investigated and it was found that, according to Item 1 of Article 2 of the Supreme People's Court's "Explanation on Certain Questions Regarding the Specific Application of the Law when Trying Cases of Stealing, Gathering, Procuring, or Illegally Providing State Secrets or Intelligence Outside of the Country," stealing, gathering, procuring, or illegally providing state secrets are crimes with "especially serious circumstances." The state secrets that defendant [redacted] illegally provided outside of the country were verified by the State Secrecy Bureau as being top-secret level state secrets, and his actions should be considered to involve especially serious circumstances. Therefore, the defense argument cannot be accepted by this court. [redacted]'s defense attorney stated: "Considering that defendant [redacted]'s actions did not result in causing extremely serious harm to state security or interests and that his attitude in admitting his crimes was good, please punish him leniently." This was investigated and found to conform with the facts; therefore, the opinion of the defense can be accepted by this court. In view of the above, and in accordance with Article 111, Paragraph 1 of Article 55, and Paragraph 1 of Article 56 of the "Criminal Law of the PRC," the following verdict is passed:

Defendant [redacted] is sentenced to 10 years' imprisonment with two years' subsequent deprivation of political rights for committing the crime of illegally providing state secrets to foreign entities.

(The prison term is to be calculated starting on the day the verdict is implemented, with each day spent in detention prior to the implementation of the verdict to count as one day of the prison term; therefore, the term will run from November 24, 2004 to November 23, 2014).

If this verdict is not accepted, an appeal may be filed between two and ten days from the receipt of this verdict, either to this court or directly to the Hunan Province Higher People's Court. In case of a written appeal, the original appellate petition must be submitted together with one copy.

Presiding judge: [redacted]
Judicial officer: [redacted]
Deputy judicial officer: [redacted]

April 27, 2005

Secretary: [redacted]

立法會

Legislative Council

LC Paper No. LS21/05-06

Paper for the Panel on Information Technology and Broadcasting

Scope of "personal data" under the Personal Data (Privacy) Ordinance (Cap. 486) and related issues

Purpose

At its meeting held on 1 November 2005, the Panel on Information Technology and Broadcasting discussed issues related to the protection of personal information of e-mail account subscribers arising from a recently reported incident on alleged disclosure by an e-mail service provider in Hong Kong of its account subscriber's personal information. To assist members of the Panel in their further consideration of the matter, this paper provides information on the scope of "personal data" as defined under the Personal Data (Privacy) Ordinance (Cap. 486) ("PD(P)O") and other related issues.

Definition of "personal data" under PD(P)O

2. Section 2(1) of PD(P)O defines "personal data" as meaning any data relating directly or indirectly to a living individual and from which it is practicable for the identity of the individual to be directly or indirectly ascertained, and such data is in a form in which access to or processing of the data is practicable. In other words, to constitute "personal data", the data must satisfy the requirements of identifiability and retrievability. "Data" is defined to mean any representation of information (including an expression of opinion) in any document, and includes a personal identifier. Under PD(P)O, a personal identifier means an identifier that is assigned to an individual by a data user for the purpose of the operations of the user and that uniquely identifies that individual in relation to the data user, but does not include an individual's name used to identify that individual.

3. The above definition of "personal data" under PD(P)O is similar to the definition of the term under the data protection laws of other jurisdictions. In Australia and New Zealand, the concept of "personal information" instead of "personal data" is adopted. Under Australia's Privacy Act 1988, "personal information is defined to mean "information or an opinion... about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion". In New Zealand, the definition is in similar terms where "personal information" is defined as "information about an identifiable individual".[1] The definition of "personal data" under the European Union's Directive on the Protection of Personal Data and on the Free Movement of Such Data ("the EU Directive") is also comparable. Under the EU Directive, "personal data means "any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified directly or indirectly".[2] The Preamble to the EU Directive states additionally that in order "to determine whether a person is identifiable, account should be taken of all means likely reasonably to be used either by the controller or by any other person to identify the said person".[3] Member states of the European Union such as the United Kingdom and Germany have enacted data protection laws with a view to implementing the EU Directive.

Interpretation of "personal data" by courts and quasi-judicial bodies

4. Although there are data protection laws in a number of jurisdictions, there have been few judicial decisions which turn on the interpretation of data protection statutes. Commentators considered that this may be due to the existence and regulatory strategies of data protection authorities and the fact that decisions of most data protection authorities or complaints which authorities fail to resolve do not go directly to courts for adjudication but to quasi-judicial bodies first.[4] Examples of such bodies are the Complaints Review Tribunal in New Zealand and the Data Protection Tribunal in the United Kingdom. Under PD(P)O, a complainant may lodge an appeal against the refusal of the Privacy Commissioner for Personal Data to carry out an investigation of a complaint to the Administrative Appeals Board. A summary of the relevant cases decided by the courts and quasi-judicial bodies is set out in the Annex for members' reference.

---

[1] Privacy Act 1993, New Zealand, section 2.
[2] Directive 95/46/EC, art 2(a).
[3] Recital 26.
[4] [redacted], 'Where have all the judges gone? Reflections on judicial involvement in developing data protection law – Part 1, *Privacy Law and Policy Reporter* [2000] PLPR 19.

5. An analysis of the relevant cases indicates that the courts and other relevant authorities appear to have adopted a rather restrictive approach in interpreting data protection legislation. The decisions in these cases have led to diverse comments from commentators and legal academics. For example, the decision of the Court of Appeal in *Eastweek Publisher Ltd. v Privacy Commissioner for Personal Data*[5] has been criticised by commentators for restricting the reach of privacy protection by imposing a judicial requirement for an intention to identify by the data collector which is not prima facie present in the legislation.[6] There has also been criticism that the court in *Eastweek* has failed to examine the identifiability test which covers both direct and indirect ascertainment of an individual's identity, nor has it considered the reasonable practicability of identifying the complainant from the photograph.[7]

6. On the other hand, commentators have expressed the view that the narrow interpretation of the term "personal data' adopted by the English Court of Appeal in *Durant v Financial Services Authority*[8] misconceives the role of the definition of "personal data" or "personal information" in determining the scope of the information privacy law since the basic assumption of all information privacy laws is that the privacy of the data subject is threatened by the processing of any information which identifies the data subject, or is capable of identifying the data subject, regardless of the nature of the information.[9]

7. When commenting on the two cases decided by the New Zealand's Complaints Review Tribunal, namely, *C v ASB Bank Ltd.*[10] and *Proceedings Commissioner v Commissioner of Police*[11], another commentator was of the view that the Tribunal adopted different approaches to the issue of "identifiability".[12] In the former case, the Tribunal rejected the identifiability of an individual by way of combination with other information known about the particular individual. This approach is different from the approach adopted in *Proceedings Commissioner v Commissioner of Police* where the Tribunal held that so long as information had the capacity to identify the individual to some members of the public, it was personal information for the purposes of New Zealand' Privacy Act. The latter approach has

---

[5] [2000] 1 HKC 692

[6] [redacted], 'Internet privacy – regulatory cookies and web bugs', *Privacy Law and Policy Reporter* [2002] PLPR 26

[7] [redacted] and Professor [redacted], *Hong Kong Data Privacy Law* (Sweet and Maxwell Asia, 2003).

[8] [2003] EWCA Civ 1746.

[9] [redacted], 'Misunderstanding 'personal information' : Durant v Financial Services Authority', *Privacy Law and Policy Reporter* [2004] PLPR 13.

[10] (1997) 4 HRNZ 306.

[11] [2000] NZAR 277.

[12] [redacted], "Information" about individuals', *Privacy Law and Policy Reporter* [2002] PLPR 31.

been considered to be consistent with the international standards set out in Article 2(a) of the EU Directive, which defines "personal data" as information concerning "an identified or identifiable" individual. The reference to "identifiable" could be interpreted to involve the use of linked data leading to the individual's identification whereas "identified" entails identification through the information itself.[13]

8. Based on the decided cases on the interpretation of data protection legislation set out in the Annex, it seems that the following principles are relevant in determining what amounts to "personal data" under PD(P)O:

(a) In general, information about companies is not personal information because it is not information about a natural person, and this is so even though the information relates to a one-person company;

(b) To qualify as "personal data" or "personal information", the data or information concerned must relate to an individual in the sense that it has an idiosyncratic connection with the individual;

(c) A primary piece of information may be regarded as personal if the identity of an individual can be reasonably ascertained by the use of other collateral information; and

(d) There is an intention on the part of the data collector to identify the individual.

Application of data privacy laws to the Internet

9. Information gathered on the Internet from Internet users may be provided by the users voluntarily or involuntarily. Information may be provided voluntarily through registration pages, contest sign-ups, applications or order forms. Users will often give crucial information such as name and address believing that the information is being collected for a specific purpose.

---

[13] [redacted], *I.b.i.d.*

10. On the other hand, some information is collected by the covert operation of technology. Such information include a user's Internet Protocol address ("IP address"), the type of computer and browser used and limited information about the browsing activity (notably the time and date of access and the referring website's Internet address). An IP address is basically a specific machine address assigned by the Web Surfer's Internet Service Provider ("ISP") to a user's computer and is therefore unique to a specific computer.[14] Whenever a transaction requesting or sending data occurs on the Internet, this unique address accompanies the data. Moreover, the deployment of cookies by a website would allow the website to recognize a computer's IP address and to recall details of the user's browsing activity.

11. In the matter under consideration by the Panel, the Panel has taken note of the Changsha Intermediate People's Court of Hunan Province Criminal Verdict (2005) in relation to the trial of [redacted] in which it was reported that Yahoo Holdings (Hong Kong) Limited ("Yahoo Holdings") had confirmed the user information corresponding to an IP address. Since the user information is apparently derived from the relevant IP address, it may be useful to consider whether an IP address is "personal data" under PD(P)O in considering whether the alleged disclosure amounts to a contravention of PD(P)O.

12. According to Yahoo! Hong Kong's privacy policy (Exhibit B to LC Paper No. CB(1)186/05-06(03)), Yahoo! Hong Kong will automatically receive and record information such as IP address and the information recorded in Yahoo! cookie and the web pages visited. It is not known whether the IP address allegedly disclosed in the trial of [redacted] was disclosed by Yahoo Holdings. It is possible that cookies may be used by third parties uninvolved in the transaction between the user and Yahoo Holdings and whose existence is unknown to the user.

13. According to our research, there has not been any judicial authority on whether an IP address is personal data or personal information within the scope of data protection laws. Some commentators suggest that it is quite possible that IP addresses can constitute "personal data" as defined in Article 2(a) of the EU Directive as an IP address which discloses the location of a computer used to access a website can be traced to an identifiable individual.[15] Some have argued that it is a question of fact whether an individual's identity can be ascertained from transactional details

---

[14] [redacted], 'Personal Privacy on the Internet: Should it be a Cyberspace Entitlement?' *The Trustee of Indiana University Law Review* 2003, 36 Ind. L. Rev. 827

[15] [redacted], 'Data Protection Law – Approaching its Rationale, Logic and Limits, 316 *Kluwer Law Journal*, 2002.

where only an IP address was collected, and it is a further question of fact whether it can "reasonably" be so ascertained.[16] However, in the light of the restrictive approach adopted by courts, it appears unlikely that the courts in Hong Kong are prepared to rule that IP addresses constitute "personal data" as defined under PD(P)O. Indeed, applying the principles set out in paragraph 8 above, it could be said that an IP address lacks an idiosyncratic relationship with the user because the information is about an inanimate computer, not the individual.

14. In respect of the alleged disclosure by Yahoo Holdings, there is the additional difficulty that the user information corresponding to the relevant IP address relates not to a natural person but to an entity instead. Given the narrow approach adopted in *Durant*, *Smith* and *C v ASB Bank*, it appears unlikely that the courts in Hong Kong would regard the user information allegedly disclosed by Yahoo Holdings as relating to a living individual under PD(P)O. However, if the courts are prepared to take a broader approach in construing the legislation, it could be argued that whether the corresponding user information relates to a natural person or an entity is not relevant; what is relevant is that the IP address discloses the physical location of the computer concerned. The question then is whether it is reasonably practicable to identify an individual from the location of the computer in the circumstances of the case. If the approach in *Proceedings Commissioner v Commissioner of Police* decided by the New Zealand' Complaints Review Tribunal is followed, it would be a question of fact for the courts to decide whether some members of the public, with prior knowledge about the individual, are able to identify the individual from the location of the computer.

Approaches adopted by some overseas jurisdictions to address privacy and data protection issues on the Internet

15. Unlike in the traditional processing of personal data where there is usually a single authority or entity responsible for protecting the privacy of data subjects, there is no such overall responsibility on the Internet assigned to a specific entity. Moreover, it seems that the use of Internet services does not allow adequate anonymity as the covert operation of the technology would facilitate surveillance of communications by methods such as cookies and the monitoring of IP addresses.

---

[16] [redacted] 'Privacy principles – irrelevant to cyberspace?' *Privacy Law and Policy Reporter* [1996] PLPR 58

16. Some jurisdictions have taken action to address the issues of privacy and data protection on the Internet. For example, Germany has included in its Teleservices Data Protection Act 1997 provisions dealing with issues associated specifically with the use of Internet, namely, transactional anonymity, cookies, processing of clickstream data.[17] The Council of Europe has published guidelines for the protection of privacy on the Internet.[18] In the Directive on Privacy and Electronic Communications adopted by the European Union in 2002, there are provisions dealing with the confidentiality of communications made over a public electronic communications network, the use of cookies and the inclusion of personal data in public directories.

Protection of information of ISP customers under the Telecommunications Ordinance

17. According to the paper provided by the Administration (LC Paper No. CB(1)173/05-06(01)), ISPs are licensed through the Public Non-exclusive Telecommunications Service ("PNETS") licence granted by the Telecommunications Authority ("TA") under the Telecommunications Ordinance (Cap. 106) ("TO"). In addition to the prescribed general conditions, TA has, in exercise of the power conferred by section 7A of TO, attached a special condition to PNETS licences to protect the information of customers of ISPs licensed in Hong Kong.[19] The relevant special condition, as drafted, is not confined to protecting personal information of customers but to protecting information of an ISP customer and information provided by the customers of an ISP or obtained in the course of provision of service to its customers. Under TO, a breach of licence conditions can result in financial penalties and even revocation of the licence in exceptional cases.

---

[17] Clickstream data is the generic name given to the information a website can know about a user simply because the user has browsed the site.

[18] The guidelines were adopted by the Committee of Ministers on 23 February 1999.

[19] Special Condition 7 of the PNETS licence provides that (a) the licensee shall not disclose information of a customer except with the consent of the customer, which form of consent shall be approved by TA, except for the prevention or detection of crime or the apprehension or prosecution of offenders or except as may be authorized by or under any law; (b) the licensee shall not use information provided by its customers or obtained in the course of provision of service to its customers other than for and in relation to the provision by the licensee of the service under the licence.

Conclusion

18. It can be seen from the decided cases that a restrictive approach is generally adopted in the interpretation of data protection laws as applied to the traditional processing of data. It remains to be seen as to whether the courts are prepared to adopt a broader approach when applying the data protection laws to data collected on the Internet, especially in respect of the identifiability of an individual from information which apparently relates to a computer.

19. From the policy point of view, Members may wish to consider the following matters in deciding how the issues arising from the alleged disclosure by Yahoo Holdings should be dealt with:

(a) whether it is necessary to ask the Administration to review whether PD(P)O offers adequate protection to personal data collected on the Internet having regard to the development of technology; and

(b) whether specific legislation or additional privacy principles are necessary to address the issues of privacy and data protection on the Internet with reference to the approaches adopted by some overseas jurisdictions.

20. Apart from considering the matter from the perspective of personal data protection under PD(P)O, members may, in the light of paragraph 17 above, ask the Administration to consider whether any action could be taken under the licensing framework provided in TO.

Encl.

Prepared by

Legal Service Division
Legislative Council Secretariat
January 2006

Summary of cases on the interpretation of "personal data/information" by courts and quasi-judicial bodies in Hong Kong and overseas jurisdictions

Jurisdiction	Case	Case Summary
Hong Kong	*Eastweek Publisher Ltd v Privacy Commissioner for Personal Data* [2000] 1 HKC 692	• The case concerned a complaint made by a woman whose photograph appeared in a magazine published by Eastweek. The photograph was taken without the complainant's knowledge or consent. The main issue before the Court of Appeal was whether the publisher had collected personal data using unfair means and whether the published photograph constituted "personal data". • In deciding that the publisher had not collected personal data, the Court took into account the complainant's anonymity and the irrelevance of her identity so far as the photographer, the reporter and the publisher were concerned and the fact that the publisher had no intention to identify the complainant.
United Kingdom	*Durant v Financial Services Authority* [2003] EWCA Civ 1746	• A narrow interpretation of the term "persona data" under the Data Protection Act 1998 of the United Kingdom was adopted by the English Court of Appeal. The Court concluded that "personal data" was information affecting the privacy of the data subject, whether in his or her personal, business or professional capacity. • The Court laid down two tests for distinguishing protected from unprotected information, namely that the information must be "biographical in a significant sense", and that the data subject must be the focus of the information.
United Kingdom	*Smith v Lloyds TSB Bank Plc.* [2005] EWHC 246, Ch.	• The narrow interpretation of "personal data" adopted by the English Court of Appeal in *Durant* has recently been followed in *Smith v Lloyds TSB Plc.* • The court held that documents held by Lloyds concerning certain loans between Lloyds and a company of which Smith was the managing director and controlling shareholder were not personal data for the purposes of the Data Protection Act 1998. Although Smith was mentioned in those documents, the courts considered that this was only because he was acting on behalf of the company and hence were not biographical about Smith to a significant extent and did not significantly affect his privacy.

New Zealand	*Harder v The Proceedings Commissioner* [2000] 3 NZLR 80	In interpreting "information about an identifiable individual" under New Zealand's Privacy Act, the Court of Appeal came to the view that in order for information to be about an individual, some idiosyncratic connection with the individual was required.
New Zealand	*C v ASB Bank Ltd.* (1997) 4 HRNZ 306	• The issue before the New Zealand Complaints Review Tribunal in this case was whether information about a company could constitute personal information for the purposes of privacy legislation. The case concerned a one-person company where the plaintiff was the sole director and owner of all but one of the shares of the company. The Tribunal was asked to decide whether the defendant bank's unauthorized disclosure of the bank statements of the plaintiff's company to the plaintiff's former wife was a disclosure of the plaintiff's personal information in terms of New Zealand's Privacy Act 1993. • It was held that the bank statements were not personal information about the plaintiff since the bank statements concerned were information about a company rather than an identifiable individual. • Although the information from the company statements, when combined with other information which the former wife held about the plaintiff might become personal information about the plaintiff, the Tribunal considered that the bank statements contained information about the financial transactions of the company and as such they stood alone. The Tribunal did not accept the use of other information to establish the link leading to the identification of the individual.
New Zealand	*Proceedings Commissioner v Commissioner of Police* [2000] NZAR 277	The Complaints Review Tribunal held that under the Privacy Act 1993, personal information was not limited to information that identified the complainant. It included information about her recorded in statements made by and about her. Thus the information contained in the statements she made about the type of injuries she sustained is information about her. It also had the capacity to identify her to some members of the public. An identifiable individual's privacy could be breached if an identification could be made as a result of prior knowledge by some members of the public of an individual, not just by strangers.
Germany	*'The Census Decision'* (1984) 5 HRLJ 94	The German Constitutional Court held that a proposal for national census was unlawful on data protection grounds. The Court expressed concern that although data gathered from the census would be published only in aggregated format, modern data processing techniques might permit the de-anonymisation of census data.

Annex B

TESTIMONY OF [redacted]
SENIOR VICE PRESIDENT AND GENERAL COUNSEL, YAHOO! INC.
BEFORE THE SUBCOMMITTEES ON AFRICA, GLOBAL HUMAN RIGHTS AND INTERNATIONAL OPERATIONS,
AND ASIA AND THE PACIFIC

FEBRUARY 15, 2006

Chairmen [redacted] and [redacted], Ranking Members [redacted] and [redacted], and Members of the subcommittees, I am [redacted], Senior Vice President, General Counsel and Secretary of Yahoo! Inc. Thank you very much for the opportunity to testify before you today.

I would like to make three fundamental points here today:

First, our principles. Since our founding in 1995, Yahoo! has been guided by beliefs deeply held by our founders and sustained by our employees. We believe the Internet can positively transform lives, societies, and economies. We believe the Internet is built on openness. We are committed to providing individuals with easy access to information. These beliefs apply in the United States. These beliefs also apply in China, where the Internet has grown exponentially over the past few years and has expanded opportunities for access to communications, commerce, and independent sources of information for more than 110 million Chinese citizens.

Second, the [redacted] case. I will discuss this in more detail later in my testimony. The facts of the [redacted] case are distressing to our company, our employees, and our leadership. Let me state our view clearly and without equivocation: we condemn punishment of any activity internationally recognized as free expression, whether that punishment takes place in China or anywhere else in the world. We have made our views clearly known to the Chinese government.

Third, this hearing. We commend you, Mr. Chairmen, for holding this hearing. It allows these issues to be raised in a public forum and provides an opportunity for companies such as those appearing here today to ask for the assistance of the U.S. government to help us address these critical issues. While we absolutely believe companies have a responsibility to identify appropriate practices in each market in which they do business, we also think there is a vital role for government-to-government discussion of the larger issues involved.

These issues are larger than any one company, or any one industry. We all face the same struggle between American values and the laws we must obey. Yahoo! intends to be a leader in the discussion between U.S. companies and the U.S. government. We appeal to the U.S. government to do all it can to help us provide beneficial services to Chinese citizens lawfully and in a way consistent with our shared values.

The Impact of the Internet In China

Before discussing these issues in detail, allow me to clarify Yahoo!'s current role in China. In October 2005, Yahoo! formed a long-term strategic partnership in China with Alibaba.com, a Chinese company. Under the agreements, Yahoo! merged our Yahoo! China business with Alibaba.com.

It is very important to note that Alibaba.com is the owner of the Yahoo! China businesses, and that as a strategic partner and investor, Yahoo!, which holds one of the four Alibaba.com board seats, does not have day-to-day operational control over the Yahoo! China division of Alibaba.com. The Alibaba.com management team runs the business; however, as a large equity investor, we have made clear our desire that Alibaba.com continue to apply rigorous standards in response to government demands for information about its users. I have personally discussed our views with senior management of Alibaba.com, as have other senior executives of Yahoo!.

Mr. Chairmen, we believe information is power. We also believe the Internet is a positive force in China. It has revolutionalized information access, helps create more open societies, and helps accelerate the gradual evolution toward a more outward-looking Chinese society.

The Internet has grown exponentially in China in ways that have increased China's openness to the outside world. More than 110 million people in China use the Internet. A growing Chinese middle class is benefiting from improved communication, technology, and independent sources of information. Online search, a core Yahoo! China service, is used by 87% of the online population in China, with more than 400 million search queries taking place every day. This represents an increase of almost 1600% over just the last three years. Unlike virtually any medium that has preceded it, the Internet allows users to access the information they want when they want it.

The number of people communicating with each other over the Internet has also increased dramatically. The number of active mailboxes has grown by 88% to 166 million, and those using instant messaging has risen to 87 million, doubling in just three years.

Let me give you a couple of examples of the power of the Internet in China. In November 2002, a new respiratory illness developed in southern China. This illness spread to other areas of China and in Asia. Initially, state media did not report widely on the outbreak, limiting access to information on SARS in China. However, word spread quickly through channels on the Internet, alerting people in China and around the world of the severity of the epidemic. The Internet forced the Chinese government to be more transparent and to vigorously attack the problem.

Another example is currently highlighted on the Human Rights Watch website. Human Rights Watch, with which we have consulted on these issues, tells the compelling story of

how the Internet helped spread the word in China about the tragic death of a young college graduate named [redacted] while in police custody. A storm of online protests led to the abolition of the law used to detain [redacted]. Human Rights Watch's website states, "[t]he [redacted] case showed how Internet activists and journalists could mobilize an online uprising that produced real change."[1]

Experts in China and the United States agree on the liberalizing impact of the Internet in China. Please note the comments of a Chinese Academy of Social Sciences researcher in the *New York Times* last week. This expert stated, "At first, people might have thought it [the Internet] would be as easy to control as traditional media, but now they realize that's not the case."[2]

Finally, I would commend to you a 2002 report by the well-respected RAND Corporation that made an even bolder conclusion. It concluded that the Internet has allowed dissidents on the mainland to communicate with each other with greater ease and rapidity than ever before.[3]

But even with these extraordinary benefits, there are severe challenges for any company operating in China, and particularly for those in the Internet, media, or telecommunications industries. This Committee correctly highlights the fundamental conflict between the extraordinary powers of the Internet to expand opportunities for communication and access to information with the obligations of companies doing business in China to comply with laws that may have consequences inconsistent with our values. This brings us to the case of [redacted].

The Facts Surrounding the [redacted] Case

The [redacted] case raises profound and troubling questions about basic human rights. Nevertheless, it is important to lay out the facts. When Yahoo! China in Beijing was required to provide information about the user, who we later learned was [redacted], we had no information about the nature of the investigation. Indeed, we were unaware of the particular facts surrounding the case until the news story emerged. Law enforcement agencies in China, the United States, and elsewhere typically do not explain to information technology companies or other businesses why they demand specific information regarding certain individuals. In many cases, Yahoo! does not know the real identity of individuals for whom governments request information, as very often our users subscribe to our services without using their real names.

---

[1] Human Rights Watch, "Chinese Protest Online: The Case of [redacted]" located at [redacted]

[2] [redacted] "Despite Web Crackdown, Prevailing Winds Are Free," *New York Times*, Feb. 9, 2006.

[3] [redacted] *You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies*, RAND Corporation monograph, 2002, page 3.

At the time the demand was made for information in this case, Yahoo! China was legally obligated to comply with the requirements of Chinese law enforcement. When we had operational control of Yahoo! China, we took steps to make clear our Beijing operation would honor such instructions only if they came through authorized law enforcement officers and only if the demand for information met rigorous standards establishing the legal validity of the demand.

When we receive a demand from law enforcement authorized under the law of the country in which we operate, we must comply. This is a real example of why this issue is bigger than any one company and any one industry. All companies must respond in the same way. When a foreign telecommunications company operating in the United States receives an order from U.S. law enforcement, it must comply. Failure to comply in China could have subjected Yahoo! China and its employees to criminal charges, including imprisonment. Ultimately, U.S. companies in China face a choice: comply with Chinese law, or leave.

Let me take this opportunity to correct inaccurate reports that Yahoo! Hong Kong gave information to the Chinese government. This is absolutely untrue. Yahoo! Hong Kong was not involved in any disclosure of information about [redacted] to the Chinese government. In this case, the Chinese government ordered Yahoo! China to provide user information, and Yahoo! China complied with Chinese law. To be clear -- Yahoo! China and Yahoo! Hong Kong have always operated independently of one another. There was not then, nor is there today, any exchange of user information between Yahoo! Hong Kong and Yahoo! China.

Next Steps

Yahoo! continues to believe the continued presence and growth of the Internet in China empowers its citizens and will help advance Chinese society. The alternative would be for these services to leave China -- a move we believe would impede Chinese citizens' ability to communicate and access independent sources of information. But we recognize this cannot be a time for business as usual.

As part of our ongoing commitment to preserving the open availability of the Internet around the world, we are committing to the following:

- *Collective Action:* We will work with industry, government, academia and NGOs to explore policies to guide industry practices in countries where content is treated more restrictively than in the United States and to promote the principles of freedom of speech and expression.

- *Compliance Practices:* We will continue to employ rigorous procedural protections under applicable laws in response to government requests for information, maintaining our commitment to user privacy and compliance with the law.

- *Information Restrictions:* Where a government requests that we restrict search results, we will do so if required by applicable law and only in a way that impacts the results as narrowly as possible. If we are required to restrict search results, we will strive to achieve maximum transparency to the user.

- *Government Engagement:* We will actively engage in ongoing policy dialogue with governments with respect to the nature of the Internet and the free flow of information.

Let me make one final comment about the role of the U.S. government. We urge the U.S. government to take a leadership role on a government-to-government basis. The Internet industry in the United States, including the companies appearing before you today, have changed the way the world communicates, searches for, discovers, and shares information. No other medium in history has the potential to effect such great change so rapidly. We operate businesses that transcend boundaries, in a world of countries and borders. The strength of this industry and the power of our user base is formidable to be sure. But, we cannot do it alone. We will do everything we can to advance these principles. Ultimately, the greatest leverage lies with the U.S. government.

* * *

Chairmen [redacted] and [redacted], Ranking Members [redacted] and [redacted], and Members of the subcommittees, thank you for giving me the opportunity to appear before you. We welcome this chance to have a frank and open dialogue about this important issue. We are grateful for your willingness to understand the difficult challenges we face, and to help us as we work together to protect the ability of the citizens of the world to access communication, commerce, and independent sources of information. I would be happy to answer your questions.