

EXHIBIT A

**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	1
Introduction	1
Preamble	1
The Incident	1
Press Release Issued by YHHK	3
Issues of Personal Data Privacy Concern	3
CHAPTER TWO	4
Preliminary Enquiries	4
Preliminary Enquiries Raised with YHHK	4
Concerns Raised by Members of the Legislative Council	5
Further Information from YHHK	5
CHAPTER THREE	7
The Complaint	7
CHAPTER FOUR	8
Operation of Yahoo! China and Corporate Structure of YHHK	8
Operation of Yahoo! China	8
Corporate Structure of YHHK	10
CHAPTER FIVE	11
Legal Requirements	11
CHAPTER SIX	15
Investigation and Evidence Gathering	15
The Business Structure	15
Disclosure of User Information to the PRC Authorities	16
Testimony and Declaration of the Senior Vice President and General Counsel of Yahoo! Inc.	18
No Access to Yahoo! China's User Accounts by YHHK	20
No Further Submissions from Mr. X's Authorized Representative ..	21
Verification from Public Records	21
CHAPTER SEVEN	22
PRC Laws Application	22
Issues Relating to PRC Laws	22

First Issue: Article 45 and the Obligation to Comply 22
 Other Consequences on Failure to Supply Information to SSB..... 23
 Second Issue: Non-disclosure of the Requested Data to the
 Commissioner 24

CHAPTER EIGHT 28

The Commissioner’s Findings 28
 Focus of Investigation 28
 Undisputed Facts..... 28
 Whether IP Address is “Personal Data” within the Definition of the
 Ordinance 29
 Whether Personal Data were Disclosed by YHHK to SSB?..... 31
 Whether YHHK is a “Data User” in relation to the Information
 Disclosed to SSB 33
 Whether the Ordinance has Extra-territorial Application to the Act
 Complained Of..... 35
 If the Ordinance had Jurisdiction over the Act Complained of, had
 YHHK Contravened DPP3? 37
 Exemption in Section 58 39
 Conclusion..... 41

CHAPTER NINE 42

Comments Arising from the Investigation..... 42
 Scope of Application of the Ordinance 42
 Extraterritorial Application of the Ordinance..... 42
 The Definition of “Crime” 45
 Consideration by Policy Bureau 46

GLOSSARY

ANNEXURES

- Annex A - Changsha Intermediate People’s Court of Hunan Province Criminal Verdict dated 27 April 2005**
- Annex B - “Scope of ‘personal data’ under the Personal Data (Privacy) Ordinance (Cap. 486) and related issues”, paper issued by the Legal Services Division of the Legislative Council Secretariat**
- Annex C - Testimony of the Senior Vice President and General Counsel, Yahoo! Inc. before the Subcommittees on Africa, Global Human Rights and International Operations, and Asia and the Pacific dated 15 February 2006**

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 PRC¹ 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 2005², 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 paper³ 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

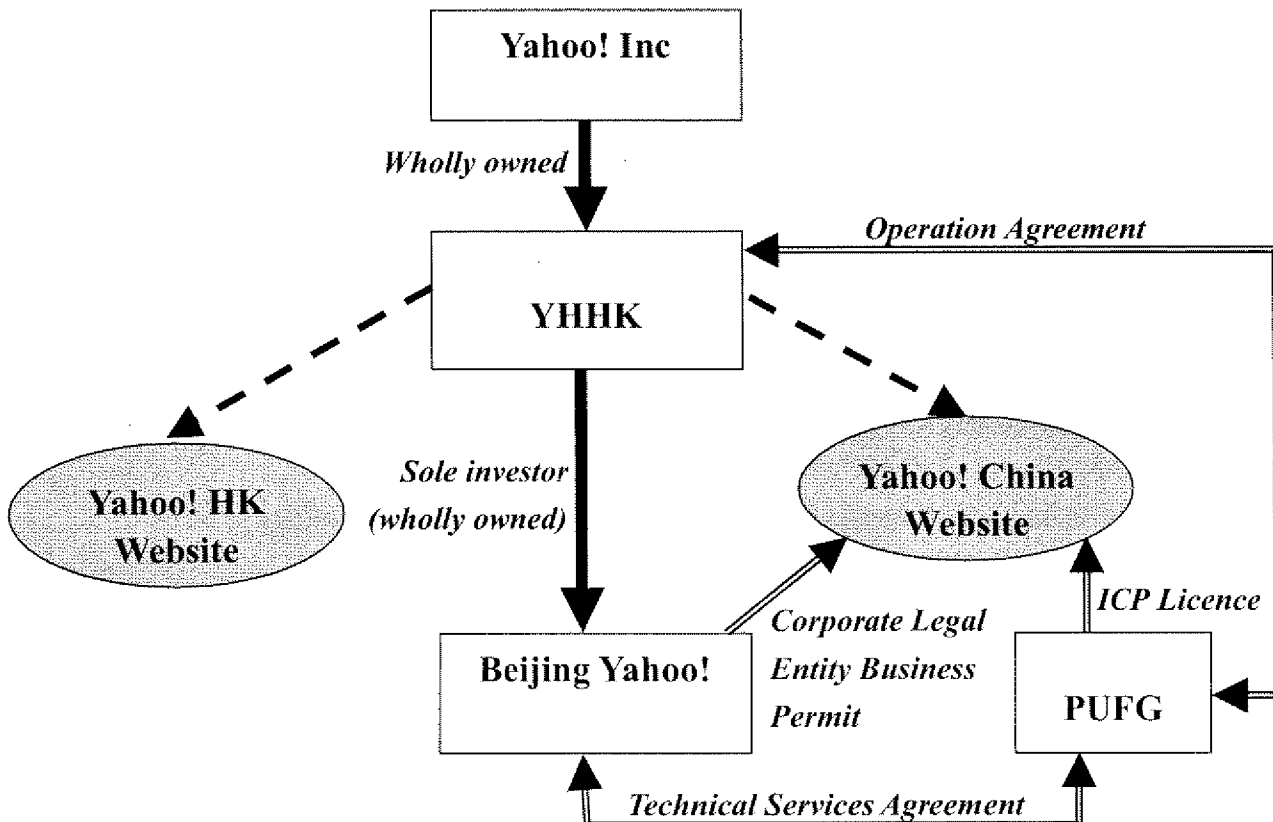
Operation of Yahoo! China and Corporate Structure of YHHK

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")

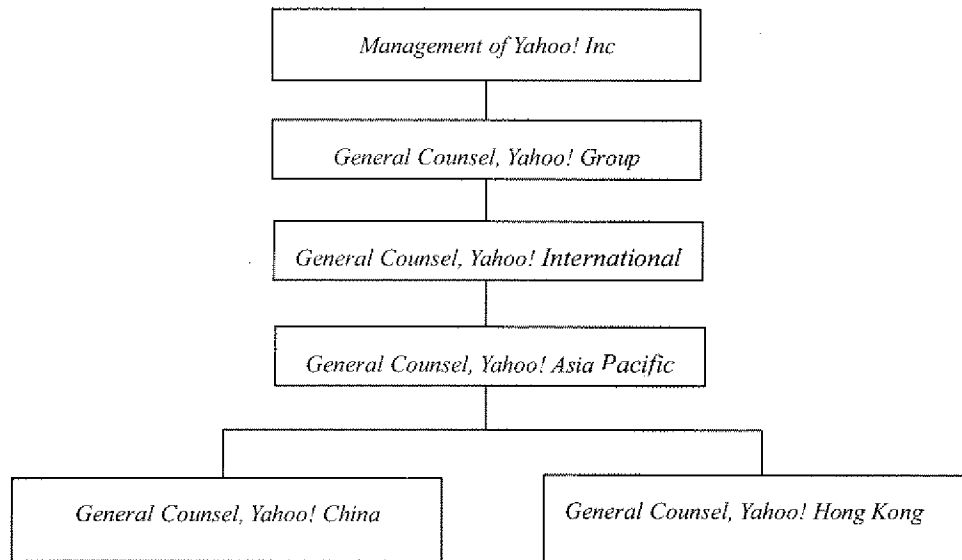
6.14 In support of YHHK's claim that disclosure of the Information

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 2006⁴ 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 views⁶ 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 Industry⁸. The Regulation on Telecom also imposes a duty on the business operator to terminate the transmission of such information immediately and report to relevant authorities⁹.

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 investigation¹⁰. The failure to comply with the requirement may render the entity to be subject to administrative sanctions, including admonition and fine¹¹.

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 Revealmnt 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 department¹².

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 consequences¹³.

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 arising¹⁵.

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 Secretariat¹⁶, 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 legislations²⁰.

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 provision²¹ 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 agency²².

9.10 In the United Kingdom ("UK"), the Data Protection Act 1998 confines its application to a data controller which is "*established*" in the UK²³ 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.