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

電郵服務提供者向中國執法機構披露電郵用戶的個人資料

案件編號：200603619

本報告乃有關本人根據《個人資料(私隱)條例》(第 486 章)(下稱「條例」)第 38 條對雅虎香港有限公司進行的調查，並根據條例第 VII 部行使本人獲賦予的權力而發表。條例第 48(2)條訂明「*…專員在完成一項調查後，如認爲如此行事是符合公眾利益的，可—*

(a) 發表列明以下事項的報告—

(i) 該項調查的結果；

(ii) 由該項調查引致的、專員認爲是適合作出的關乎促進有關資料使用者所屬的某類別的資料使用者遵守本條例條文(尤其是各保障資料原則)的任何建議；及

(iii) 由該項調查引致的、專員認爲適合作出的任何其他評論；及

(b) 以他認爲合適的方式發表該報告。」

吳斌
個人資料私隱專員

(註：本報告乃翻譯本，一切以英文文本爲準。)

目錄

第一章

簡介

前言

1.1 本報告是個人資料私隱專員(下稱「**專員**」)依據《個人資料(私隱)條例》(第 486 章)(下稱「**條例**」)第 38 條就「雅虎香港有限公司(前稱「雅虎香港控股有限公司」)(下稱「**雅虎香港控股**」)向中華人民共和國機關披露一名電郵用戶的個人資料，因而違反條例規定」的指稱而進行調查的結果。

事件

1.2 2005 年 10 月，本地報章廣泛報導一名居住於中國的記者(下稱「**X 先生**」)被湖南省長沙市中級人民法院(下稱「**人民法院**」)裁定犯了爲境外非法提供國家秘密罪，違反《中華人民共和國刑法》第一百一十一條[1]，被判入獄十年。

1.3 根據新聞報導，雅虎香港控股向中國政府機關披露"*yahoo.com.cn*"電郵用戶 X 先生的個人資料，導致 X 先生被捕。

1.4 根據人民法院於 2005 年 4 月 27 日作出的判決書[2] (下稱「**判決書**」)，X 先生於 2004 年 4 月 20 日晚上約 11 時 32 分，「*向境外敵對分子通風報信，利用其獨自在辦公室值班之機電話上網，通過其個人的電子郵箱 huoyan-1989@yahoo.com.cn 發送了其記錄的[屬於絕密級國家秘密的中共中央辦公廳、國務院辦公廳《關於當前穩定工作的通知》]中辦發[2004]11 號文件的重要內容摘要，並將提供者化名爲"198964"…*」

1.5 判決書列出爲證明罪行所搜集的證據，其中包括：

---

[1] 《中華人民共和國刑法》第一百一十一條訂明：「*爲境外的機構、組織、人員竊取、刺探、收買、非法提供國家秘密或者情報的，處五年以上十年以下有期徒刑；情節特別嚴重的，處十年以上有期徒刑或者無期徒刑；情節較輕的，處五年以下有期徒刑、拘役、管制或者剝奪政治權利。*」

[2] 請參閱本報告附件 A。

「*雅虎香港控股有限公司出具的關於用戶資料的證明材料，證實 IP 地址：218.76.8.201，時間：2004 年 4 月 20 日 23 時 32 分 17 秒的對應用戶資料如下：用戶電話：0731-4376362，湖南《當代商報》社。地址：長沙市開福區建湘新村 88 棟 2 樓。*」

1.6 向境外傳送被列爲國家秘密資料的電郵帳戶是「*huoyan-1989@yahoo.com.cn*」(下稱「**電郵帳戶**」)。

1.7 從判決書可以清楚得知雅虎香港控股曾向中國政府機關披露某些電郵用戶資料，但雅虎香港控股在調查過程中向中國政府機關披露了多少資料，判決書並非最終定論。根據判決書，人民法院亦有考慮其他證據，包括 X 先生的手寫自訴材料及供述，供認「其故意爲境外非法提供國家秘密的犯罪事實」。

1.8 上述事件(下稱「**事件**」)引起公眾注意，以及對個人資料私隱的關注，尤其是關於電郵服務提供者向香港以外的執法機構披露電郵用戶的資料，此舉有否違反條例的規定。公眾如此關注，是因爲電郵服務提供者在提供服務的過程中，會收集並持有大量個人資料，如不適當處理用戶的個人資料，會對資料當事人的個人資料私隱造成嚴重後果。

雅虎香港控股發出的新聞稿

1.9 2005 年 10 月 18 日，雅虎香港控股發出新聞稿，以回應公眾的關注，文中明確地反駁該公司涉及披露有關用戶資料的說法。新聞稿指出：「*雅虎香港…奉行香港特別行政區所有本地法律規條及雅虎香港嚴謹的私隱政策。內地政府部門從未接觸過或要求雅虎香港提供任何客戶資料。就管理及營運而言，雅虎香港及雅虎中國均獨立自主運作，雅虎香港及雅虎中國從未互相透露或交換用戶資料。*」

個人資料私隱的關注問題

1.10 事件引發下列與條例有關的問題：

1.10.1 雅虎香港控股是否向中國政府機關披露了條例所指的「個人資料」；

1.10.2 特別考慮的是 X 先生的個人資料(如有)是否由雅虎香港控股收集及披露，雅虎香港控股的披露作爲是否受條例囿制；以及

1.10.3 如該作爲或行爲是受條例囿制，究竟雅虎香港控股向中國政府機關披露資料是否違反保障資料第 3 原則？如果有違反的話，條例有沒有豁免條文讓雅虎香港控股援引？

第二章

初步查詢

對雅虎香港控股的初步查詢

2.1 2005 年 10 月 21 日，專員主動接觸雅虎香港控股，搜集進一步資料，以便確定有否違反條例的規定。

2.2 2005 年 10 月 29 日，雅虎香港控股向專員作出書面回應，堅稱：

2.2.1 雅虎香港控股並無涉及有關 X 先生的資料被披露予中國政府機關或其任何代理的事宜；

2.2.2 有關披露是與一名在雅虎中國網站(下稱「**雅虎中國**」)註冊、持有「.cn」電郵帳戶的中國用戶有關；

2.2.3 有關披露是由雅虎中國作出的；

2.2.4 雅虎香港網站(下稱「**雅虎香港**」) 及雅虎中國是各自獨立管理及營運的；

2.2.5 雅虎香港及雅虎中國並不會交換用戶的帳戶資料；以及

2.2.6 雅虎香港控股只有在收到依據香港法律發出的有效及正式書面要求後，才會向香港執法機構作出回應；對於要求披露電郵內容的指令，除非收到香港法庭發出的搜查令，否則雅虎香港控股是不會向執法機構發放任何資料的。

立法會議員提出的關注

2.3 2005 年 11 月 1 日，立法會資訊科技及廣播事務委員會(下稱「**事務委員會**」)召開特別會議，討論事件。專員獲邀出席會議。專員在會上就「個人資料」的定義、條例的管轄範圍，以及保障電郵用戶

的個人資料等事宜發言。

2.4 事務委員會關注「個人資料」的定義，特別是它是否涵蓋互聯網協定位址(下稱「IP 位址」)，以及互聯網服務供應商披露用戶資料的合法性。鑑於電子媒體已廣泛應用於通訊方面，事務委員會要求立法會秘書處的法律事務部就「個人資料」的涵蓋範圍進行研究及擬備文件[3]。

雅虎香港控股提供的進一步資料

2.5 2005 年 11 月 19 日及 2005 年 12 月 9 日，雅虎香港控股回應專員的查詢，提供與事件有關的進一步資料：

2.5.1 與事件有關的資料是由中國的雅虎中國收集，雅虎中國在關鍵時間是由雅虎香港控股擁有的；

2.5.2 有關資料似乎是與一名身處中國的雅虎中國用戶有關；

2.5.3 向雅虎中國註冊的用戶姓名並非 X 先生，雅虎中國並不知道該用戶其實就是 X 先生；

2.5.4 有關資料是中國的雅虎中國根據中國法律向中國政府機關披露的；

2.5.5 與事件有關的行爲(資料的收集、儲存及披露)沒有一項是在香港發生，而有關各方(即雅虎中國、X 先生及中國政府機關)沒有一方是來自香港的；

2.5.6 即使條例規管完全發生在香港以外但在中國境內的行爲，雅虎香港控股認爲條例第 58(2)條的豁免條文適用於有關資料的發放；

2.5.7 雅虎中國的擁有權在 2005 年 10 月 24 日轉予阿里巴巴公司(下稱「**阿里巴巴**」)之前是由雅虎香港控股全資擁有的；

[3] 請參閱本報告附件 B 的立法會 LS 21/05-06 號文件。

2.5.8 雅虎中國是由一個名爲北大方正集團(下稱「**北大方正**」)的中國單位透過北京雅虎網諮詢服務有限公司(下稱「**北京雅虎**」)經營的，而北京雅虎是由雅虎香港控股全資擁有；

2.5.9 雅虎中國的互聯網內容供應商許可證是由中國政府簽發，並由北大方正持有；

2.5.10 與事件有關的記錄是由雅虎中國保存的，而雅虎中國其後被售予阿里巴巴；

2.5.11 根據判決書，電郵帳戶的用戶姓名是「huoyan-1989」，而不是 X 先生；以及

2.5.12 雅虎香港控股無權監控雅虎中國用戶資料的收集及/或披露。

第三章

投訴

3.1 2006 年 3 月 30 日，專員收到 X 先生在香港的獲授權代表的投訴。投訴指稱雅虎香港控股未經 X 先生同意，便向中國政府機關披露與其電郵帳戶有關的個人資料，因此違反條例的規定。

3.2 X 先生的投訴並無附上證據作爲支持。儘管公署多番要求，X 先生或其獲授權代表並沒有提供進一步資料或證據予專員考慮。

3.3 X 先生的獲授權代表所依賴的唯一證據是判決書的內容，判決書確認雅虎香港控股曾向中國政府機關提供某些電郵用戶資料，導致 X 先生最後被捕及被定罪。

3.4 專員根據對事件初步查詢所得的事實和證據，於 2006 年 5 月 9 日決定依據條例第 38 條展開調查。

第四章

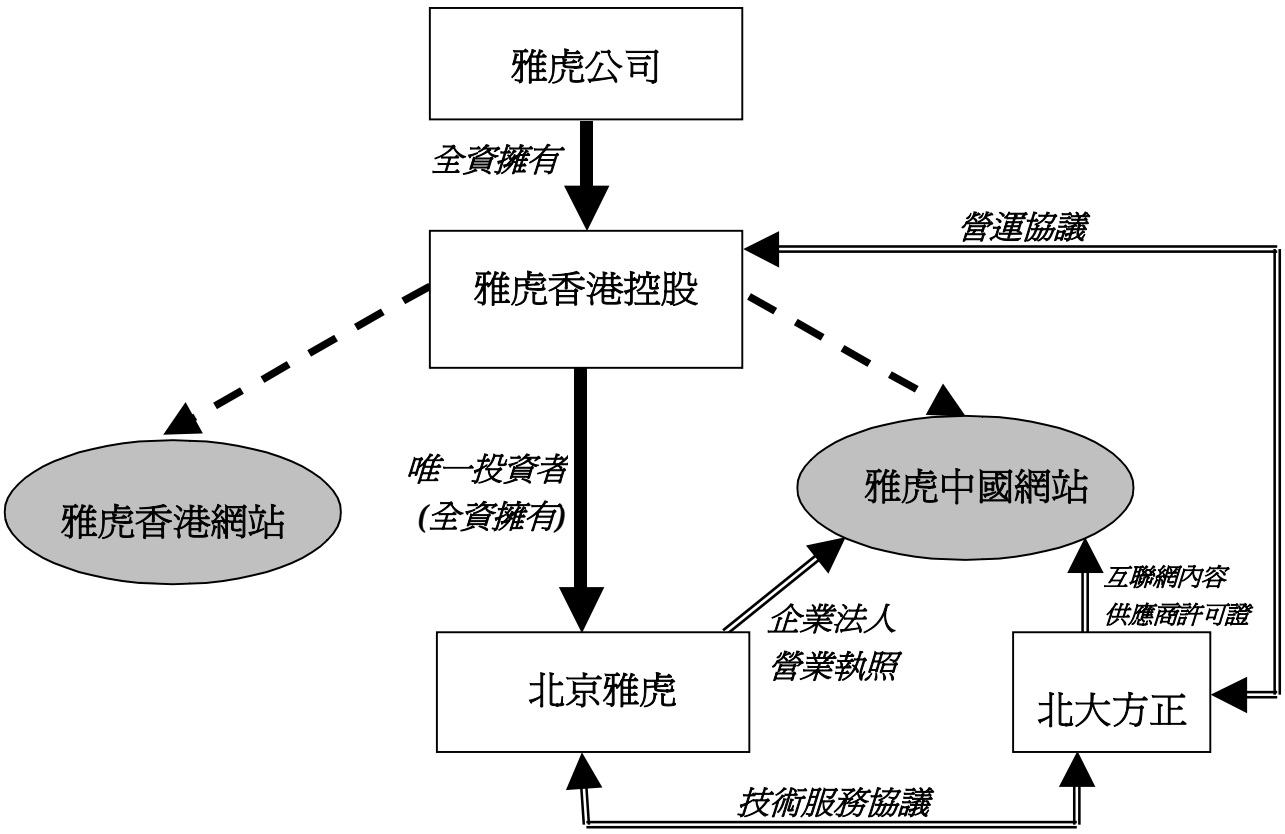
雅虎中國的營運模式及雅虎香港控股的公司架構

4.1 專員認爲要評估雅虎香港控股在事件中的角色及法律責任，首先要了解雅虎香港及雅虎中國的營運模式，以及雅虎香港控股的公司架構。

雅虎中國的營運模式

4.2 雅虎香港控股確認有關披露是雅虎中國於 2004 年 4 月 22 日作出的。雅虎中國在關鍵時間的營運模式見下圖：

雅虎中國的營運架構(2004 年 4 月)



4.3 從上圖可見，雅虎香港及雅虎中國雖然由雅虎香港控股擁有，但兩者的營運模式是不同的。雅虎香港控股是根據《中華人民共和國外資企業法》，透過其全資擁有的中國公司—北京雅虎經營雅虎中國。根據北京市人民政府於 2002 年 4 月 29 日簽發的《中華人民共和國台港澳僑投資企業批准證書》，雅虎香港控股是北京雅虎的投資者，提供所有註冊資本。北京雅虎是企業法人營業執照的持有人，企業形式是「全資外資企業(香港)」。根據北京雅虎的公司章程，雅虎香港控股有權委任及更換北京雅虎董事局的每位成員，包括主席。

4.4 爲了取得在中國經營雅虎中國所需的互聯網內容供應商許可證，雅虎香港控股於 2003 年 2 月 19 日與北大方正簽訂一項營運協議(下稱「**營運協議**」)，以便利用其互聯網內容供應商許可證。北京雅虎根據於 2003 年 2 月 19 日簽訂的技術服務協議(下稱「**技術服務協議**」)，向北大方正提供技術服務，協助雅虎中國網站的營運。

4.5 專員從雅虎香港控股取得與雅虎中國營運有關的營業執照、公司文件、營運協議及技術服務協議。專員沒有相反的證據令他懷疑這些文件的真實性。

4.6 事實上，在 2005 年 10 月 24 日之前，雅虎中國是由雅虎香港控股全資擁有，並透過北大方正及北京雅虎經營的。

4.7 從 2005 年 10 月 24 日起，阿里巴巴成爲雅虎中國的擁有人及經營者。

雅虎香港控股的公司架構

4.8 雅虎香港控股是根據香港法律成立的香港公司，是雅虎香港的擁有人及經營者。

4.9 雅虎香港控股的最終母公司—雅虎公司是一間美國公司，以加利福尼亞州爲基地。雅虎公司是最終實益擁有雅虎香港控股的所有已發行股本。

4.10 雅虎香港控股及雅虎公司目前共持有阿里巴巴約百分之四十的已發行股份。

4.11 雅虎香港控股已於 2006 年 6 月 22 日改名爲雅虎香港有限公司。

第五章

法律規定

5.1 下述條文與調查有關：

5.1.1 條例**第 2(1)條**訂明：

「「個人資料」指符合以下說明的任何資料—
(a) 直接或間接與一名在世的個人有關的；
(b) 從該等資料直接或間接地確定有關的個人的身分是切實可行的；及
(c) 該等資料的存在形式令予以查閱及處理均是切實可行的；」

「「資料使用者」，就個人資料而言，指獨自或聯同其他人或與其他人共同控制該等資料的收集、持有、處理或使用的人；」

「「切實可行」指合理地切實可行；」

5.1.2 條例附表 1 的**保障資料第 3 原則**訂明：

「如無有關的資料當事人的訂明同意，個人資料不得用於下列目的以外的目的—
(a) 在收集該等資料時會將其使用於的目的；或
(b) 直接與(a)所提述的目的有關的目的。」

5.1.3 根據條例第 2(1)條，「**使用**」一詞就個人資料而言，包括「*披露*」或「*移轉*」該等資料。

5.1.4 根據條例第 2(3)條，「**訂明同意**」指「*該人自願給予的明示同意*」，而沒有以書面通知予以撤回。

5.1.5 條例**第 39(1) (d)條**訂明：

「(1) 即使由本條例賦予專員的權力有其概括

性，在以下情況下，專員可拒絕進行或拒絕繼續進行由投訴引發的調查—

…

(d) 就該項投訴所指明的作爲或行爲而言，以下所有條件均不獲符合—

(i) 在有人作出或從事有關作爲或行爲(視屬何情況而定)的任何時間—

(A) 投訴人(如投訴人是就某名個人而屬有關人士的有關人士，則指該名個人)是居於香港的；或

(B) 有關的資料使用者能夠在香港控制有關的個人資料的收集、持有、處理或使用或能夠從香港行使該項控制的；

(ii) 在有人作出或從事有關作爲或行爲(視屬何情況而定)的任何時間，投訴人(如投訴人是就某名個人而屬有關人士的有關人士，則指該名個人)是在香港的；

(iii) 專員認爲有關的作爲或行爲(視屬何情況而定)可能損害投訴人(如投訴人是就某名個人而屬有關人士的有關人士，則指該名個人)強制執行在香港獲取或產生的權利或行使在香港獲取或產生的特權；」

5.1.6 條例**第 58(1)及(2)條**訂明：

「(1) 爲—

(a) 罪行的防止或偵測；

(b) 犯罪者的拘捕、檢控或拘留；

….

而持有的個人資料

(2) 凡—

(a) 個人資料是爲第(1)款所提述的目的而使用(不論該等資料是否爲該等目的而持有)；及

(b) 第3 保障資料原則的條文就該等使用而適用便相當可能會損害該款所提述的任何事宜，則該等資料獲豁免而不受第 3 保障資料原則的條文所管限，而在爲任何人違反任何該等條文而針對他進行的法律程序中，如該人證明他當時有合理理由相信不如此使用該資料便相當可能會損害任何該等事宜，即爲免責辯護。」

5.1.7 條例**第 65(1)及(2)條**訂明：

「(1) 任何人在其受僱用中所作出的任何作爲或所從事的任何行爲，就本條例而言須視爲亦是由其僱主所作出或從事的，不論其僱主是否知悉或批准他作出該作爲或從事該行爲。

(2) 任何作爲另一人的代理人並獲該另一人授權(不論是明示或默示，亦不論是事前或事後授權)的人所作出的任何作爲或所從事的任何行爲，就本條例而言須視爲亦是由該另一人作出或從事的。 」

第六章

調查及搜集證據

6.1 除非另有說明，否則本章內所有資料是雅虎香港控股或雅虎公司在專員調查本個案時提交的。調查重點是找出雅虎香港控股披露了甚麼個人資料(如有)及有關披露的情況。

業務架構

6.2 雅虎香港控股進一步闡釋了雅虎中國的營運模式。據雅虎香港控股所述，雅虎香港的業務是由香港一組管理人員負責，而雅虎中國的業務則由另一組在北京的管理人員負責。雅虎中國的一切營運、管理、策略及業務決定均由雅虎中國按照雅虎公司或其委任的國際營運管理隊伍的指示而作出。

6.3 雅虎香港控股的董事局只是履行與雅虎香港控股有關的法定職能，例如批核法團印章的使用及經審計的帳目。雅虎香港控股董事局進行的活動或通過的決議中沒有一項是與雅虎中國的日常管理運作有關。

6.4 至於與披露雅虎電郵用戶的個人資料有關的事宜，主要是由相關網站的法律組處理。雅虎中國的法律組(下稱「**雅虎中國法律組**」)是直接向雅虎公司的法律組負責的。

6.5 根據這樣的權責劃分，雖然雅虎中國在法律上是由雅虎香港控股擁有，但從營運角度來看，雅虎中國在架構上最終是由雅虎公司的管理層管理及管控。

6.6 因此，雅虎香港控股不能管控雅虎中國的事務。實際上雅虎中國的事務是由雅虎公司全權管控。

向中國政府機關披露用戶資料

6.7 專員要求雅虎香港控股詳細提供披露與電郵帳戶有關的用戶資料的情況，以及就有關披露而尋求的法律意見(如有)。

6.8 雅虎公司代表雅虎香港控股作出回應，提供披露與電郵帳戶有關的用戶資料的過程：

6.8.1 2004 年 4 月 22 日之前，雅虎中國收到中國國家安全局(下稱「**國安局**」)一個電郵，要求取得與電郵帳戶有關的用戶資料。雅虎中國於是要求國安局發出正式的調取證據通知書。

6.8.2 2004 年 4 月 22 日，國安局以專人送來依據《中華人民共和國刑事訴訟法》第四十五條(下稱「**第四十五條**」)而發出的調取證據通知書(下稱「**通知書**」)。該通知書蓋有北京市國安局的官方印章，是關於*「向境外非法披露國家秘密」*的刑事調查。

6.8.3 雅虎中國法律組檢查通知書的有效性及合法性，確定雅虎中國在法律上有責任遵從通知書的規定。

6.8.4 雅虎中國的客戶服務組(下稱「**雅虎中國客戶服務組**」)從雅虎中國的用戶資料庫(存放在位於中國的伺服器內)中提取所需的資料。.

6.8.5 雅虎中國法律組確認所提取的資料與通知書要求的資料相符，並批准披露。

6.8.6 雅虎香港控股的公司印章 (下稱「**雅虎香港控股印章**」)是由北京辦事處的雅虎中國法律組蓋於國安局要求並披露予國安局的資料文件上。

6.8.7 在或大約在 2004 年 4 月 22 日，雅虎中國向國安局披露與電郵帳戶有關的資料。

6.8.8 2004 年 4 月 22 日之後，國安局與雅虎中國曾就與電郵帳戶有關的進一步資料聯絡數次。

6.8.9 雅虎中國客戶服務組按通知書要求，向國安局提供進一步資料。

6.9 雅虎公司確認雅虎中國曾向國安局提供：*(i)用戶註冊資料，*

(ii)互聯網協定登入資料及(iii)某些電郵內容(下稱「**該等資料**」)。雅虎公司進一步表示，電郵服務用戶在註冊時通常會被要求提供姓名、性別、出生日期等資料。不過，不能保證他們所提供的資料是真確的，因爲很多用戶都不以真實資料來註冊。

6.10 第四十五條訂明：「*人民法院、人民檢察院和公安機關有權向有關單位和個人收集、調取證據。有關單位和個人應當如實提供證據。對於涉及國家秘密的證據，應當保密。凡是僞造證據、隱匿證據或者毀滅證據的，無論屬於何方，必須受法律追究。*」

6.11 雅虎中國並不知道國安局調查的確實性質或詳情，但國安局的通知書列明是關於*「向境外非法披露國家秘密」*的刑事調查。

6.12 雅虎中國並不知道國安局在要求用戶資料時是否知悉電郵帳戶的用戶身份。

6.13 在專員詢問雅虎公司向國安局披露該等資料之前有否徵詢法律意見時，雅虎公司聲稱，他們就第四十五條從其中國內部律師取得的法律意見如下：

6.13.1 公安機關有權從有關單位或個人收集或取得證據；

6.13.2 涉及國家秘密的證據必須保密；

6.13.3 凡是僞造證據、隱藏證據或毀滅證據的，無論屬於何方，必須受法律追究；

6.13.4 根據《中華人民共和國刑法》第二百七十七條(下稱「**第二百七十七條**」)，拒絕提供合法要求的證據會被視爲阻礙國家職務，可處三年以下監禁、拘役、管制或者罰金；以及

6.13.5 國安局是根據中國法律要求該等資料，因此披露該等資料並不屬於自願行爲。

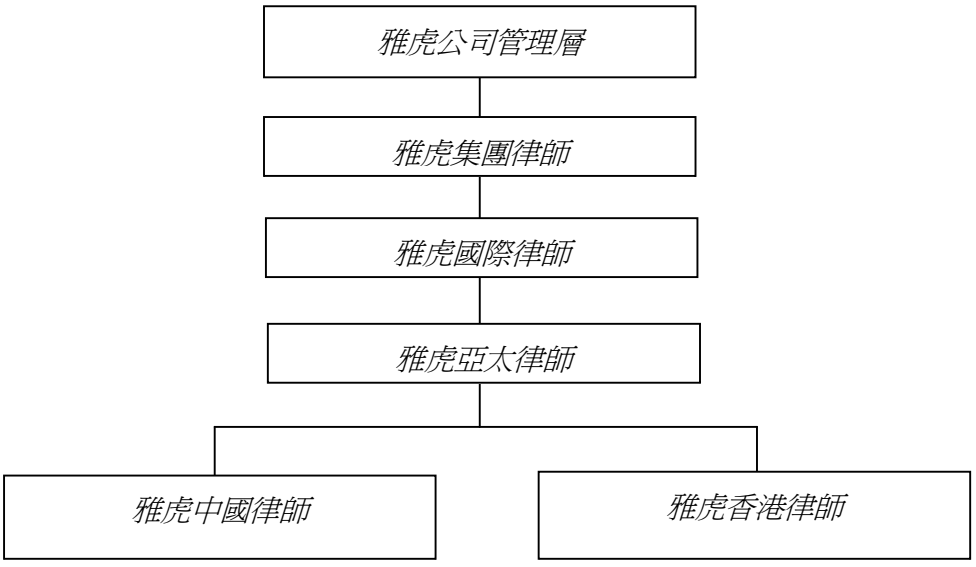
雅虎公司高級副總裁兼總法律顧問(下稱「Y 先生」) 的證供及聲明

6.14 爲了支持雅虎香港控股所言，披露該等資料是遵從中國法律

的規定，專員收到一份 Y 先生於 2006 年 2 月 15 日代表雅虎公司就有關 X 先生個案的事實向美國國會提供的證供[4]作爲參考。

6.15 Y 先生在證供中作供：「*當北京的雅虎中國被要求提供有關用戶(我們其後知道是[X 先生])的資料時，我們並不知道調查的性質。更確切的說，我們並不知道該個案的詳細情況，直至傳媒報導。…很多時，對於政府要求取得其資料的人士，雅虎並不知道他們的真正身份，因爲很多時用戶不是以真實姓名來使用我們的服務。…當我們在經營業務的國家收到執法機構根據該國法律發出的通知書時，我們必須遵從。…在中國不遵從規定可能令雅虎中國及其僱員被刑事起訴，包括監禁。…在本個案，中國政府命令雅虎中國提供用戶資料，而雅虎中國遵守中國法律。*」

6.16 按專員的要求，Y 先生亦於 2006 年 8 月 23 日在美國加利福尼亞州聖塔克拉拉縣就支持雅虎公司的陳詞向專員作出有法律約束力的聲明。他聲明：「*…根據我對香港個人資料(私隱)條例中何謂『個人資料』的理解，[X 先生]在向雅虎中國註冊的過程中並無提供個人資料。按公司的標準程序，執法要求是由地區性人員處理，雅虎香港是不會獲告知執法行動的詳情。…爲了提供適當的制衡機制及確保完整地履行法律職能，法律部是獨立於業務營運之外。每個國家的律師並非向當地的業務組負責，亦不隸屬於當地的業務組。當時的統屬關係如下：*



[4] 請參閱本報告附件 C。

只有雅虎中國的法律部才能覆核有關[X 先生]個案的執法命令、執行所需程序及授權把雅虎中國的用戶資料披露予北京市國安局，以及在披露文件中使用[雅虎香港控股]的印章，而根據公司政策及措施，正如以上所述，雅虎中國的法律部並不是由[雅虎香港控股]管控。」

雅虎香港控股不能存取雅虎中國的帳戶資料

6.17 專員要求雅虎香港控股直接確認雅虎公司所作的回應。雅虎香港控股表示他們不能控制雅虎中國用戶的個人資料的收集、持有、處理或使用，因此雅虎香港控股並沒有亦從來沒有存取過電郵帳戶的記錄。

6.18 爲了說明雅虎香港控股是不能存取雅虎中國的帳戶資料，雅虎香港控股向專員示範其內部帳戶管理系統的運作，當他們嘗試存取雅虎中國的帳戶資料時，即會彈出訊息：「*你不准開啓用戶：…*」。

X 先生的獲授權代表沒有提出進一步的陳詞

6.19 儘管我們多次要求取得 X 先生電郵帳戶的用戶註冊資料，以及披露予國安局的該等資料，但是 X 先生的獲授權代表並沒有向專員提供進一步資料。

公眾記錄的查證

6.20 根據在香港對雅虎香港控股進行的公司查冊，在雅虎香港控股 1,000 股已發行股本中，雅虎公司持有 10 股已發行股份，而 Yahoo! International Subsidiary Holdings, Inc.則持有 990 股。

6.21 雅虎公司確認，Yahoo! International Subsidiary Holdings, Inc. 的所有已發行股份在關鍵時間曾經並仍然由雅虎公司擁有。因此，雅虎公司最終全資擁有雅虎香港控股，因而有權代表雅虎香港控股就本投訴作出回應。專員獲提供一張由 Yahoo! International Subsidiary Holdings, Inc.向雅虎公司發出的股票副本作爲證據。

第七章

中國法律的應用

有關中國法律的問題

7.1 在調查過程中，專員需要解決兩個有關中國法律的適用性問題。第一個問題是雅虎中國在法律上是否必須依據第四十五條向國安局發放該等資料。第二個問題是關於雅虎香港控股在調查過程中拒絕向專員披露某些資料。

7.2 有關這兩個問題及爲了評估雅虎香港控股陳詞的分量及相關性，專員向兩名中國法律專家(下稱「**中國法律專家**」)徵詢獨立的法律意見。

第一個問題：第四十五條及遵守責任

7.3 專員關注的第一個問題是雅虎中國在法律上是否必須向國安局披露該等資料。有關國安局發出的通知書的合法性、遵守責任及不遵守的後果這些問題都是值得考慮的。

7.4 專員就第四十五條在本個案的適用範圍，向中國法律專家徵詢意見。根據中國法律專家的意見，由於雅虎香港控股是在中國經營業務，他們必須就其在中國經營的業務遵守中國的法律，包括《中華人民共和國刑事訴訟法》。通知書由國安局簽署或蓋章後正式發出被視爲符合簽發的法律程序。任何人或單位都有法律責任，提供真實證據。

7.5 由於判決書清楚表明有關的用戶資料是由雅虎香港控股提供，並由控方呈交人民法院考慮，專員並無理由或相反資料，質疑國安局爲調查而向雅虎香港控股發出的通知書的存在或真確性。

7.6 中國法律專家亦請專員參考《國家安全法》第十八條(下稱「**第十八條**」)[5]的條文，該條規定市民及組織必須向國家安全機關提供與

[5] 第十八條訂明：「*在國家安全機關調查了解有關危害國家安全的情況、收集有關證據時，公民和有關組織應當如實提供，不得拒絕。*」

其調查有關的資料。

7.7 至於不遵從調取證據通知書的後果，第二百七十七條訂明：「*…故意阻礙國家安全機關、公安機關依法執行國家安全工作任務，未使用暴力、威脅方法，造成嚴重後果的，…處罰*」，並會「*…處三年以下有期徒刑、拘役、管制或者罰金*」。

7.8 雖然中國法律專家對於拒絕向國安局提供要求資料是否構成第二百七十七條所指的「阻礙」，在法定解釋方面持有不同的觀點[6]，但專員在聽取法律意見後認爲，雅虎中國及雅虎香港控股在這個案的情況下，如不遵從通知書的規定，真的擔憂很可能會違反第四十五條或第二百七十七條而受罰。

不向國安局提供資料的其他後果

7.9 除了拒絕向國安局提供該等資料所遭受的刑事處罰之外，中國法律專家認爲根據雅虎香港控股在中國經營的業務性質，雅虎香港控股亦須遵守其他有關法律、規則及規例，其中之一是《中華人民共和國電信條例》(下稱「**電信條例**」)。

7.10 電信條例禁止組織或個人製作、複製、發布或傳播含有危害國家安全、洩露國家秘密等內容的信息[7]。如有違反，情節嚴重的，信息產業部會吊銷電信業務經營許可證[8]。電信條例亦規定業務經營者立即停止傳輸有關信息，並向有關機關報告[9]。

7.11 此外，雅虎香港控股在中國經營業務亦須遵從中國的互聯網信息服務條例，其中有條文規定互聯網電郵服務提供者須積極配合國家有關機關開展調查工作[10]。有關單位沒有遵從這項規定會遭受行政處罰，包括警告及罰款[11]。

---

6 一學派認爲第二百七十七條適用於擾亂公安的罪行，但不包括拒絕按要求提供證據的作爲。另一學派則認爲拒絕按要求提供證據是屬於第二百七十七條第四段中「未使用暴力」的阻礙作爲。

7 電訊條例第五十七條。

8 電訊條例第七十八條。

9 電訊條例第六十二條。

10 《互聯網電子郵件服務管理辦法》第十八條訂明：「*互聯網電子郵件服務提供者、爲互聯網電子郵件服務提供接入服務的電信業務提供者，應當積極配合國家有關機關和互聯網電子郵件舉報受理中心開展調查工作。*」

11 《互聯網電子郵件服務管理辦法》第二十五條訂明的刑罰包括由信息產業部予以警告，並處最高一萬元的罰款。

7.12　專員在考慮雅虎香港控股的陳詞，以及中國法律專家就中國法律及規例的適用性和遵守責任提供的意見之後，信納雅虎香港控股依據通知書向國安局披露該等資料是雅虎香港控股的法律責任，拒絕遵從可能會遭受刑事及行政處罰。

第二個問題：拒絕向專員披露要求資料

7.13　在調查過程中，專員要求雅虎香港控股提供：(i)電郵帳戶的用戶資料；(ii)與國安局的往來書信；(iii) 通知書，以及(iv)該等資料(統稱「**要求資料**」)。

7.14　雅虎香港控股在回應專員的要求時聲稱，他們對專員所要求的大部分資料或文件並不知情或無權存取。他們不能向專員提供披露的文件副本，因爲根據他們的中國內部律師的意見，該等文件根據《中華人民共和國國家秘密法》第二條(下稱「**第二條**」)可能會被視爲國家秘密，因爲該等文件與中國一宗刑事調查直接有關。

7.15　第二條訂明：「*國家秘密是關系國家的安全和利益，依照法定程序確定，在一定時間內只限一定範圍的人員知悉的事項。*」法律爲「國家秘密」下了較爲廣闊的定義，它包括「*維護國家安全活動和追查刑事犯罪中的秘密事項*」。至於甚麼資料被列爲「國家秘密」則由國家保密工作部門決定[12]。

7.16　在專員要求進一步詳情時，雅虎香港控股確認他們從其中國內部律師所得的法律意見是：

7.16.1　有關政府機構爲調查刑事罪行而要求的資料被視爲「國家秘密」；以及

7.16.2　如遇上難以界定某一項目是否國家秘密的情況，披露的一方必須視該項目爲國家秘密。

7.17　專員在考慮是否根據條例援引其權力迫使對方交出要求資料時，曾就雅虎香港控股以《國家秘密法》的有關條文作爲拒絕理由而徵詢中國法律專家的意見。中國法律專家認爲在洩漏國家秘密的審訊中獲法院確認的證據或資料，即使審訊結束，亦不會影響其爲國家秘

[12] 《中華人民共和國國家秘密法》第十一條。

密的性質，此等證據或資料必須繼續受《國家秘密法》保護。

7.18 對於就調查罪行而向國安局提供的所有證據及資料(不論有沒有使用過)是否能夠確切地符合「國家秘密」的定義，中國法律專家的意見各有不同。不過，中國法律專家一致認爲違反國家秘密法即屬犯罪，會遭受嚴重刑罰[13]。

7.19 在有關情況下，專員認爲必須考慮下列因素：

7.19.1 雅虎中國向國安局提供的該等資料曾經或可能曾用於調查有關罪行；

7.19.2 「國家秘密」的廣闊定義及有關中國政府機關界定資料的權力；

7.19.3 X 先生的個案並非公開審訊，亦沒有審訊的謄本。判決書載列的不具爭議的事實，是專員可以放心依賴的唯一證據；

7.19.4 沒有證據顯示要求資料並非被界定爲「國家秘密」；以及

7.19.5 違反《國家秘密法》在中國屬於嚴重罪行。

7.20 經考慮上述因素後，專員接納雅虎香港控股對違反《國家秘密法》的擔心是真實及合理的。專員因此沒有行使權力，強迫雅虎香港控股出示要求資料。

[13] 例如《中華人民共和國刑法》第一百一十一條列明關於向中國境外機構或個人提供國家秘密的刑罰。被定罪的人會被處五年以上十年以下有期徒刑。

第八章

專員的調查結果

調查的重點

8.1 專員在調查中主要關注的法律問題包括：

8.1.1 **個人資料**：向國安局披露的該等資料是否屬於條例所界定的「個人資料」？

8.1.2 **資料使用者**：就條例而言，雅虎香港控股是否資料使用者？

8.1.3 **境外管轄權**：如披露個人資料的作爲全部是在香港境外作出，條例是否適用？

8.1.4 **保障資料第 3 原則**：指稱中依據國安局的通知書而披露用戶資料是否符合原本的收集目的或與之直接有關？

8.1.5 **第 58 條的豁免**：爲了調查外地罪行而向香港以外執法機構披露個人資料是否可以根據條例第 58 條獲得豁免？

不具爭議的事實

8.2 以下是不具爭議的事實：

8.2.1 電郵帳戶(一個.cn 帳戶)是經雅虎中國在中國註冊的；

8.2.2 電郵帳戶是由一名中國用戶登記使用的；

8.2.3 該等資料是由雅虎中國依據通知書在中國披露的；

8.2.4 雅虎香港控股在關鍵時間是雅虎中國的合法擁有人；以及

8.2.5 雅虎公司擁有雅虎香港控股。

IP 位址是否條例所界定的「個人資料」

8.3 要構成條例中的「個人資料」，有關資料必須符合條例規定的三個條件，即(a)直接或間接與一名在世的個人有關；(b)從該等資料直接或間接地確定有關的個人的身分是切實可行的；及(c)該等資料的存在形式令予以查閱或處理均是切實可行的。「切實可行」一詞在第 2(1)條獲進一步界定爲「合理地切實可行」。

8.4 根據判決書，雅虎香港控股向國安局提供的電郵用戶資料是：

> 「*雅虎香港控股有限公司出具的關於用戶資料的證明材料，證實 IP 地址：218.76.8.201，時間：2004 年 4 月 20 日 23 時 32 分 17 秒的對應用戶資料如下：用戶電話：0731-4376362，湖南《當代商報》社。地址：長沙市開福區建湘新村 88 棟 2 樓。*」

8.5 判決書內提述的資料是否構成「個人資料」，尤其是有關資料是否符合定義中的(a)及(b)項都引起了疑問。由於條例並沒有提供「間接」辨識資料的規定測試，這個詞語本身傾向概念性。

8.6 在詮釋法律方面，專員對法例釋義採取目的原則，以「*按其真正用意、涵義及精神，並爲了最能確保達致其目的*」[14]，避免「*荒謬*」的結果出現[15]。

8.7 專員認爲在定義的第一個條件，與個人「直接」有關的資料是直接講述該人或得出有關該人信息的資料。與個人「間接」有關的資料是當此等資料與其他資料一併閱讀時，該人的信息是要從資料推斷或間接推斷出來。

8.8 至於第二個條件中的直接或間接辨識，如果只從有關資料(包

[14] 請參閱《釋義及通則條例》(香港法例第 1 章)第 19 條。

[15] 法例釋義的黃金原則「*避免荒謬的假設*」可參考 Benion, *Statutory Interpretation*, third edition, Butterworths。

括從資料推斷的信息)便可以確定身份，有關確定是「直接」的。如要依賴資料使用者容易得到的其他資料才能確定身份，有關辨識是「間接」的。這是要由個案的事實決定。資料使用者不能容易地得到的資料，並不納入合理地切實可行的範圍。

8.9 由於本個案的用戶資料包括 IP 位址，專員必須考慮 IP 位址就其本身而言是否屬於條例中的「個人資料」。

8.10 基本上，IP 位址是互聯網服務供應商編配予用戶電腦的特定機器位址，因此對於每部電腦來說都是獨一無二的。每當在互聯網收發資料時，這個獨一無二的位址便會隨著資料傳輸。位址資料是關於沒有生命的電腦，而非關於個人。單是 IP 位址是不能顯示有關電腦的確切位置，亦不能顯示電腦使用者的身份。

8.11 根據「個人資料」定義的兩個條件，IP 位址並不包含與個人「有關」的資料，而註冊用戶的資料亦不容易地取得，例如透過公共域內的資料取得。因此，專員認爲 IP 位址就其本身而言並不符合「個人資料」的定義。

8.12 專員曾向資深大律師求證及徵詢意見，資深大律師完全同意單是 IP 位址並不屬於「個人資料」，但若與例如個人的辨識資料結合一起時，「個人資料」是可以包含 IP 位址的。究竟它在某一個案中是否屬於部分的個人資料，則須視乎個案的事實和上述「個人資料」定義中的兩個條件。

8.13 此外，立法會秘書處法律服務部發出一份文件[16]，名爲「《個人資料(私隱)條例》(第 486 章)所訂「個人資料」的涵蓋範圍及相關事宜」亦表達類似的觀點，認爲法庭對於 IP 位址是否構成「個人資料」普遍採取嚴緊的準則。根據以上論據，判決書所述的「*IP 位址 218.76.8.201*」本身並不構成「個人資料」。

8.14 對於判決書所述的相關用戶資料，即「*用戶電話：0731-4376362，湖南《當代商報》社。地址：長沙市開福區建湘新村 88 棟 2 樓*」，我們不能肯定地下結論謂有關用戶資料從表面看是屬於一個在世的個人，而不是法團或非法團的團體，又或者是關於一個真實的個人，而不是虛構的個人。在有關情況下，專員沒有足夠的證據，證明「個人資料」定義的兩個條件得以符合。

[16] 請參閱本報告附件 B 的立法會 LS 21/05-06 號文件。

雅虎香港控股曾否向國安局披露個人資料？

8.15　判決書未能清楚顯示雅虎香港控股所提供的「帳戶持有人資料」確實是甚麼。雅虎公司向專員確認，他們只是向國安局提供該等資料，即*(i)用戶註冊資料，(ii)互聯網協定登入資料及(iii)某些電郵內容*。專員在調查過程中並沒有收到相反證據或指稱，令他懷疑雅虎公司所作的陳述，或令他推斷認爲有該等資料以外的個人資料被披露予國安局。

8.16　鑑於：

8.16.1　以上第 8.10 至 8.14 段所述的觀點(即單是 IP 位址不能構成「個人資料」，而判決書並無表面證據證明某一位具有真實身份的個人是電郵帳戶的註冊持有人)；

8.16.2　電郵地址 huoyan-1989@yahoo.com.cn 本身並沒有披露 X 先生的身份；

8.16.3　雅虎香港控股明確地否認電郵帳戶的用戶是以 X 先生的姓名註冊，而且他們並不知道用戶其實就是 X 先生；以及

8.16.4　沒有實質證據反駁雅虎香港控股在第 8.16.3 段所作的聲稱，

因此專員認爲作出「雅虎香港控股向國安局披露的該等資料含有 X 先生的個人資料」這個結論並不穩妥。

8.17　根據以上所述，專員的調查結果可以在此作結。不過，鑑於事件引起公眾關注，爲了學術研究，專員假設雅虎香港控股披露了 X 先生的「個人資料」(未經證實)，嘗試回答下述假設性問題：

8.17.1　關於披露予國安局的資料，雅虎香港控股是否「資料使用者」？

8.17.2　條例是否有境外管轄權，處理被投訴的作爲？

8.17.3 如條例對被投訴的作爲有管轄權，雅虎香港控股有否違反保障資料第 3 原則？

就披露予國安局的該等資料而言，雅虎香港控股是否「資料使用者」？

8.18 雅虎香港控股是否屬於應該根據條例對有關披露負責的「資料使用者」？條例中的「資料使用者」是「*指獨自或聯同其他人或與其他人共同**控制**該等資料的收集、持有、處理或使用的人*」。但條例並無爲「控制」下定義。專員認爲，控制可以指涉及收集、持有、處理或使用個人資料的具體作爲，亦可以指決定收集、持有、處理或使用資料的目的及方式的能力。

8.19 雖然嚴格來說，收集及披露有關個人資料的具體作爲可能不是由雅虎香港控股作出，而是由雅虎中國在中國作出，但根據條例第65(1)及(2)條，雅虎香港控股需要對有關作爲負責，不論該作爲是由其僱員(即向雅虎中國提供服務的僱員)或代理(即經營雅虎中國的外國投資媒介北京雅虎)作出。此外，雅虎香港控股印章蓋於披露該等資料的文件上是不爭的事實。就外部各方來說，有關作爲可被視爲獲雅虎香港控股授權。

8.20 至於決定收集、持有、處理或使用資料的目的及方式的能力，專員認爲應該考慮以下事實：

8.20.1 雅虎中國是一個網站，不是法律實體，亦不是獨立於擁有該網站的雅虎香港控股；

8.20.2 雅虎中國的私隱政策聲明[17]及服務條款[18]爲「控制」提供證明，依據有關聲明及條款，雅虎香港控股或其代理會向用戶收集個人資料，尤其是當用戶在線上註冊電郵帳戶時會這樣做；

8.20.3 用戶向雅虎中國開立電郵帳戶時，同意私隱政策聲

---

[17] 「*Yahoo!會使用資料作以下一般用途：提供更適合你的廣告及網頁內容、爲你提供你所要求的產品或服務、改善我們的服務、聯絡你、進行研究調查，及爲公司或客戶提供不記名報告。*」

[18] 「*資訊共享及披露：Yahoo!不會租用、出售、或透露你的個人資料予他人或非附屬公司，除非已得到你的同意，或爲向你提供你所要求的產品或服務，或在下列的情況下：…我們回應傳票、法庭傳令、或法律程序、…*」

明及服務條款後，即與雅虎香港控股建立合約關係；以及

8.20.4 披露該等資料的文件蓋有雅虎香港控股印章，顯示雅虎香港控股有能力控制個人資料的披露。

8.21 雅虎香港控股辯稱，因爲電郵帳戶的用戶資料是由雅虎中國管理，最終則由雅虎公司管控，所以雅虎香港控股不能「控制」用戶資料的收集、持有、處理或使用。

8.22 專員認爲雅虎香港控股的論據不具說服力，因爲在披露該等資料的關鍵時間，雅虎香港控股是擁有北京雅虎(經營雅虎中國)的全部股權。雅虎集團公司的分工(包括雅虎集團內法律組的統屬關係)只是內部及公司之間的管理安排。有關安排並不影響以下事實：雅虎香港控股仍然是法律實體，必須對其在中國作出的所有作爲(包括管理個人資料的作爲或行爲)及進行的業務負責。

8.23 雖然如此，合乎邏輯的推斷是控制測試應符合一項附帶條件：侵權作爲或行爲本身(即向國安局披露該等資料的作爲)必須是資料使用者能夠在香港控制或從香港行使該項控制。在決定某一個案中的資料使用者在或從香港是否有效控制或有能力「控制」時，我們不應該只參考香港法律，還要參考任何適用的外國法律。

8.24 雅虎香港控股認爲，向國安局披露該等資料是符合第四十五條的規定。鑑於不遵從規定會遭受刑事處罰，雅虎香港控股是必須遵從規定。

8.25 在考慮過中國法律專家就中國法律(第四十五條及其他法律及電訊條例)的適用性而提供的意見、雅虎香港控股遵從有關法律的責任(即擔任雅虎中國在中國作出的作爲及進行的業務負責的法人)，以及要求取得該等資料的情況(即透過通知書)後，專員認爲在本個案的情況下披露該等資料並不是雅虎香港控股主動作出的自願行爲，而是爲遵守中國法律而必須作出的。既然如此，中國法律的施行會使「控制」(如有)變得無效。投訴的標的物(即向國安局披露該等資料一事)因此超越雅虎香港控股的控制範圍。

8.26 由於雅虎香港控股對資料的披露沒有控制權，因此爲了本調查的目的，雅虎香港控股並不屬於條例第 2(1)條所界定的「資料使用者」。邏輯上，條例對於在中國披露該等資料的作爲並不適用。

條例是否有境外管轄權，處理被投訴的作爲？

8.27 鑑於投訴的標的物在中國出現及發生，專員亦考慮本個案中條例的境外適用問題(如有)。

8.28 條例並沒有包含境外適用的明確條文。沒有有關條文，便要應用領域原則，即一般而言，條例不能延伸至約束外國人在外國土壤所作的行爲。條例第 39(1)(d)條[19] 闡述了領域原則，該條列出專員在行使其調查權力之前必須符合的條件。

8.29 該等條件主要包含的領域聯繫是：投訴人是在香港、或在有關時間是居於香港，或專員認爲被投訴的作爲或行爲會損害投訴人在香港獲取的某些相關權利。另一條件是：「*有關的資料使用者能夠在香港控制有關的個人資料的收集、持有、處理或使用或能夠從香港行使該項控制的*」。如任何資料流轉過程在有關時間是由有關的資料使用者「*在或從*」香港控制，便足以有管轄權。

8.30 一般來說，如一個人或其外國公司持有的個人資料及作出的作爲並不影響任何在香港或與香港有聯繫的人，僅僅以該人是居於香港並能夠控制外國的業務這一點是不足以驅使或令到專員根據條例行使管轄權。要驅使或令到專員根據條例行使管轄權，還要包括以香港爲基地的人士「*在或從香港*」對個人資料作出的控制。

8.31 在引用上述的控制測試時，如資料是在境外，但控制者在管轄範圍內，「*在或從香港*」作出的控制可能會因爲外國適用法律的施行而受阻或消失。

8.32 在本個案，專員接納該等資料是依據通知書而披露予中國的國安局。有關披露是以雅虎香港控股的名義作出，並蓋有雅虎香港控股印章。有關中國法律的施行及就披露該等資料而遵從中國法律的責任問題，已於第七章討論。專員認爲雅虎香港控股對披露個人資料的控制(如有)已因爲中國法律的施行而受阻或消失。

---

[19] 請參閱第 5.1.5 段。

8.33　由於條例第39(1)(d)條所述的條件全部不符合，以及個人資料的收集、持有、處理及使用沒有一項獲證實是在香港進行，專員總結認爲有關投訴事宜是超越條例的管轄範圍。

如條例對被投訴的作爲有管轄權，雅虎香港控股有否違反保障資料第3原則？

8.34　鑑於事件引起公眾關注，專員進一步提出問題：「如條例適用於披露的作爲，有關作爲是否違反保障資料第3原則？」在這方面，保障資料第3原則主要規定，除非得到資料當事人的訂明同意，否則個人資料只可以用於與原本的收集目的一致的目的。

8.35　毫無疑問，該等資料在披露予國安局之前，是沒有得到X先生的訂明同意的。專員要探討的問題是有關披露是否符合原本的收集目的或與該目的直接有關目的。在這方面，專員認爲首先應該參閱雅虎中國在收集電郵用戶的個人資料時發出的服務條款及私隱政策聲明。

8.36　由於雅虎香港控股及雅虎公司以可能違反中國國家秘密法爲理由，拒絕向專員提供電郵帳戶的用戶註冊資料，因此專員以雅虎中國使用的服務條款及私隱政策聲明的標準條文爲依據，假定同樣條文適用於X先生開立電郵帳戶一事。

8.37　雅虎中國採用的私隱政策聲明的標準條款(見於其網站)訂明，當用戶註冊雅虎中國帳戶或使用雅虎中國的服務時，個人資料會被收集。標準的電郵帳戶註冊版面會要求用戶在註冊時提供姓名、電郵地址、出生日期、性別、郵政編碼、職業、所在行業和個人興趣。私隱政策聲明亦訂明，從用戶瀏覽器上收集或得到的資料，包括IP位址、cookies中的信息等，會自動記錄於伺服器的記錄系統。此外，雅虎電郵會在外寄電郵的「頁眉」列出寄件者的IP位址。雅虎中國的私隱政策聲明亦訂明，用戶資料會爲了遵從法庭傳票、法律命令或法律程序而被共用。

8.38　雅虎中國電郵服務的用戶在使用電郵帳戶之前，必須接受雅虎香港控股的服務條款。服務條款明確列明，雅虎香港控股可能會爲回應法庭傳票、法律命令或法律程序而共用資料。用戶同意爲使用雅虎中國而遵守服務條款所列的行爲，包括不會披露國家秘密。用戶亦同意雅虎中國會在保存及披露資料方面須遵從中國法律。

8.39 服務條款及私隱政策聲明已列明資料的使用目的，以及資料獲准移轉予的人士類別包括執法機構。

8.40 中國法律專家給予專員的意見確認，在本個案的情況下披露資料是遵從中國法律的法定責任。專員對保障資料第 3 原則的適用性所持的觀點是，一般爲遵從法定要求而披露個人資料的做法被視爲符合收集目的，因此是保障資料第 3 原則容許的。依據這個想法並參考中國法律專家的意見後，專員信納雅虎香港控股爲遵從法定要求而披露資料是必須的，而根據服務條款及私隱政策聲明亦是適當的做法。

8.41 在有關情況下，有關的披露作爲並無明顯違反保障資料第 3 原則。

8.42 不過，如披露資料只是法律容許，而不是法律規定，而且披露個人資料可能引致執法機構對資料當事人採取不利行動，那麼資料使用者必須小心行事。即使資料使用者所提供的收集個人資料聲明擴闊至包括資料使用者自願披露資料的作爲，資料使用者在作出該作爲時，亦應該考慮條例第 VIII 部的豁免條文是否適用，以證明披露資料是合理的。

第 58 條的豁免

8.43 在本個案，雅虎香港控股就第 58(2)條豁免條文的適用性提出論據。雅虎香港控股辯稱，在本個案中，個人資料的使用目的是爲了第 58(1)條所指的罪行偵測，而第 58(1)條所述的「罪行」及「犯罪者」涵蓋在其他司法管轄區干犯的罪行及其他司法管轄區的犯罪者。因此爲了遵從該司法管轄區的法律而披露在該司法管轄區收集及控制的個人資料，憑藉第 58(2)條，必須獲豁免受保障資料第 3 原則的管限。

8.44 如符合下述條件，適當援引第 58 條的豁免條文是可以豁免受保障資料第 3 原則的管限：

8.44.1 使用有關資料是爲了第 58(1)條訂明的目的；以及

8.44.2 保障資料第 3 原則如適用於有關使用便相當可能會損害該等目的。

8.45　條例第 58(1)(a)及(b)條訂明獲得豁免的目的：「*罪行的防止或偵測*」及「*犯罪者的拘捕、檢控或拘留*」。條例並無對「*罪行*」一詞下定義，亦沒有其他條文提述處理外國法律下的罪行或犯罪或其他不合法的作爲。專員在決定是否接納雅虎香港控股建議的廣義解釋時，已研究過香港其他有關法規，亦曾就恰當的詮釋徵詢資深大律師的意見。

8.46　香港的《刑事事宜相互法律協助條例》(第 525 章)就提供和取得香港與香港以外地方之間在刑事事宜上的協助，作出規管，並爲附帶或相關事宜訂定條文。《刑事事宜相互法律協助條例》第 5(1)(g)條訂明：「*如律政司司長認爲有以下情況，對於由香港以外某地方提出的要求根據本條例提供協助的請求，須予以拒絕－ ……(g)該項請求關乎某作爲或不作爲，而假使該作爲或不作爲在香港發生，便不會構成香港罪行。*」

8.47　這反映一個重要的公共政策考慮，在解釋第 58 條的「罪行」或「犯罪者」時不能置之不理。專員認爲條例第 58(1)(a)及(b)條的「*罪行*」或「*犯罪者*」是泛指香港法律下的罪行或犯罪是明智、審慎及合理的釋義，儘管這些詞語亦可以廣義地包括《刑事事宜相互法律協助條例》適用的個案。

8.48　因此，當任何資料處理過程是在香港發生，而資料使用者就香港以外某地罪行或犯罪自願向該地執法機構提供其持有及控制的個人資料時，資料使用者須承擔風險，因爲有可能是指稱的作爲或不作爲(雖然在該地法律下屬於罪行)若在香港發生，是不會構成罪行的。

8.49　以上述說法應用於本個案，由於在目前香港的法律下 X 先生在中國所犯的罪行並不算是罪行，如雅虎香港控股在或從香港控制有關個人資料的使用，雅虎香港控股未必可以成功援引第 58(2)條，豁免受保障資料第 3 原則的管限，以證明其爲「*罪行的防止或偵測*」或「*犯罪者的拘捕、檢控或拘留*」而披露資料是合理的。

結論

8.50　本個案的投訴要點是：

8.50.1　雅虎香港控股是否披露了「個人資料」；以及

8.50.2 作爲資料使用者的雅虎香港控股在披露 X 先生的「個人資料」時是否違反條例的規定。

8.51 專員認爲特別重要的問題是與資料使用者有關的「控制」概念及條例對被投訴的作爲的境外管轄權(如有)問題。這涉及事實與法律等錯綜複雜的問題。

8.52 調查工作所遇到的困難是因爲缺乏來自 X 先生的直接證據，以及得不到要求資料。

8.53 儘管困難重重，公署已盡量從雅虎香港控股及雅虎公司收集所有其他有關資料。專員透過與海外私隱機構的討論及書信往來，把香港的法律與海外私隱法律互相比較。他亦向一位資深大律師及兩位中國法律專家徵詢法律意見。根據所得的證據及資料，專員最後認爲未能證明雅虎香港控股披露了 X 先生的「個人資料」予國安局。

8.54 在有關情況下，專員認爲雅虎香港控股並無違反條例的規定。

8.55 根據條例第 47(4)條，投訴人 X 先生有權就專員在本報告內所作的決定向行政上訴委員會提出上訴。

第九章

調查引伸的評論

條例的適用範圍

9.1 事件引起人們關注條例在下述情況的適用範圍：

9.1.1 個人資料的收集、持有、處理及使用作爲全不是在香港進行；以及

9.1.2 個人資料的披露是爲了調查香港以外某地罪行而依據該地機關訂立的合法規定作出的。

9.2 目前的條例並不能對上述問題提供簡單容易的答案。第 9.1.1 段的問題須要從「資料使用者」的定義及條例的境外管轄權(如有)著手，而第 9.1.2 段的問題須要參考條例內「罪行」的定義。這些與本投訴有關的問題已經在第八章專員的調查結果中論述。

9.3 根據專員的調查及爲了提高條例施行的效用及效率，專員認爲現在是最佳時機檢討條例在這些範疇中的條文是否足夠。

條例的境外適用性

9.4 關鍵是在「控制」一詞，這個詞語出現於條例第 2(1)條「資料使用者」的定義中，以及條例第 39(1)(d)(i)(B)對由投訴引發的調查的限制中。「控制」一詞欠缺一個清晰的法定定義。專員完全理解在電子化的年代，控制可以是無疆界，同時認爲控制不只限於在香港收集、持有、處理及使用個人資料的實質作爲，亦可以伸延至包括資料使用者能夠「*在或從香港*」決定收集、持有、處理或使用資料的目的及方式。

9.5 不過，資料使用者擁有的控制權力可以因爲資料使用者在香港境外所作出的作爲或所從事的行爲而消失或無效(如果有關作爲或行爲是由適用的外國法律規定)。一些海外私隱條例 [20] 亦有類似的觀

[20] 例如，澳洲的《1988 年私隱法令》第 13 D(1)條訂明：「…機構在澳洲及外部領地以外所作的作爲或所從事的行爲如果是外國的適用法律所要求，則不算是干擾個人私隱」。

點。

9.6 只要任何資料處理過程是由資料使用者「*在或從香港*」控制，便構成領域聯繫，落入條例的管轄範圍，需要遵從規定。立法精神在條例第 33 條有關禁止個人資料跨境移轉中反映。雖然第 33 條尚未實施，其第(1)款清楚訂明該條適用於在香港進行的個人資料的收集、持有、處理或使用；或該收集、持有、處理或使用的行爲是由主要業務地點是在香港的個體所控制的。不過，要留意的是第 33 條必須建基於個人資料在移轉至海外之前是在香港被持有的這個情況。

9.7 因此，資料使用者不能免除保障已移轉至香港境外的個人資料的責任。資料使用者須確保條例的規定獲得遵從，尤其是保障資料原則，並對個人資料的不當處理負上責任。

9.8 專員曾參考其他海外私隱法例，發現法例如要有管轄權就必須有一定的領域聯繫。例如，澳洲的《1988 年私隱法令》有明確條文[21]把法令的適用範圍延伸至機構在澳洲以外所作的作爲，但：

9.8.1 要與澳洲有某種指明的聯繫，例如成爲法團、中央管理及控制的地點在澳洲、公民身份等；以及

9.8.2 個人資料是與澳洲公民有關或與在澳洲的逗留時間不受法律規限的人有關。

9.9 新西蘭《1993 年私隱法令》的境外條文適用於機構曾「*移轉至新西蘭境外*」的資料[22]。

9.10 英國的《1998 年保障資料法令》規定法令適用於在英國「*確立*」的資料控制者[23]，而且資料是「*在該確立境況中處理*」。「*確立*」一詞則指通常居於英國的個人或根據英國法律成立的實體。

9.11 專員認爲如任何資料處理過程在香港進行，便會有領域聯繫，資料使用者如在或從香港控制任何資料處理過程，資料使用者是不會失去控制權的，例如資料是資料使用者在香港收集，但其後由資料使用者移轉至香港境外作資料處理。

---

[21] 《1988 年私隱法令》第 5B 條。
[22] 《1993 年私隱法令》第 10 條。
[23] 《1998 年保障資料法令》第 5 條。

9.12　反過來說，假如一名香港居民有能力控制其海外業務，例如在中國的業務，但就其業務而收集、持有、處理或使用個人資料的作爲沒有一項是在香港進行的，那麼這些在經營海外業務的過程中得到的個人資料應否納入條例的範圍內？這些從本投訴引發的問題值得令政府考慮修訂法例，以便釐清「控制」個人資料的意思及條例適用範圍的含糊之處。

「罪行」的定義

9.13　根據本報告第 8.43 至 8.49 段的論據，專員認爲最好爲條例中「罪行」一詞下一個清晰的定義。沒有清晰的定義，資料使用者是難以評估能否援引第 58(1)及(2)條的豁免條文，特別是例如遇到海外執法機構爲了調查外國罪行而要求披露某些個人資料的情況。

9.14　專員參考了一些海外私隱法例。例如，根據澳洲《1988 年私隱法令》私隱原則第 2.1(g)條，如私人機構「*受法律規定或獲法律授權*」，是可以披露個人資料的。《刑事事宜相互法律協助條例》容許英聯邦國家在外國要求時，就刑事事宜提供國際協助，爲此而披露資料在澳洲私隱法令來說是被視爲「獲法律授權」的。

9.15　在新西蘭，資料私隱原則第 11(e)條爲個人資料的披露提供例外情況，容許披露資料「*以避免損害公共機構維持法紀，包括罪行的防止、偵測、調查、檢控及懲罰*」。《1993 年私隱法令》第 2 條進一步爲「*公共機構*」一詞下定義，訂明該詞僅指新西蘭的公共機構。

9.16　爲了給予資料使用者較清晰的指引及爲個人資料私隱提供更佳保障，專員建議把條例中「罪行」一詞界定爲香港罪行，及包括《刑事事宜相互法律協助條例》適用的個案。因此，如有關作爲或不作爲在香港發生是不會在香港構成刑事罪行，則該項海外罪行不在條例的豁免適用範圍。清晰的定義有助資料使用者在個案的特別情況下評估及決定可否適當援引條例第 58(1)及(2)條的豁免條文，尤其是當海外執法機構或監管機構要求披露個人資料的行爲可能會引致資料當事人遭受不利行動的時候。

9.17　同樣的考慮，應施加於條例第 58(1)(b)條中「犯罪者」的含義。

政策局的考慮

9.18 專員會把本報告引發的問題通知民政事務局，希望政府會適當考慮檢討及修訂條例的需要，以便條例能有效施行，並爲資料使用者及資料當事人提供指引。

詞彙表

阿里巴巴	阿里巴巴公司
第二條	*《中華人民共和國國家秘密法》第二條*
第十八條	*《國家安全法》第十八條*
第四十五條	*《中華人民共和國刑事訴訟法》第四十五條*
第二百七十七條	*《中華人民共和國刑法》第二百七十七條*
北京雅虎	*北京雅虎網諮詢服務有限公司*
專員	*個人資料私隱專員*
保障資料原則	*個人資料(私隱)條例（香港法例第 486 章）附表 1 的保障資料原則*
電郵帳戶	*向境外傳送被列爲國家秘密資料的電郵帳戶「huoyan-1989@yahoo.com.cn」*
事件	*導致 X 先生被裁定犯了爲境外非法提供國家秘密罪的事件*
該等資料	*雅虎中國曾向國安局提供的資料，包括：(i)用戶註冊資料，(ii)互聯網協定登入資料及(iii)某些電郵內容*
IP 位址	*互聯網協定位址*
X 先生	*本調查中的投訴人*
Y 先生	*雅虎公司高級副總裁兼總法律顧問*
營運協議	*雅虎香港控股於 2003 年 2 月 19 日與北大方正簽訂的一項營運協議*

詞彙表

通知書	*依據《中華人民共和國刑事訴訟法》第四十五條(下稱「第四十五條」)而發出的調取證據通知書*
條例	*個人資料(私隱)條例 (香港法例第 486 章)*
事務委員會	*立法會資訊科技及廣播事務委員會*
人民法院	*中華人民共和國湖南省長沙市中級人民法院*
中國法律專家	*被專員徵詢法律意見的兩名中國法律專家*
北大方正	*北大方正集團*
電信條例	*《中華人民共和國電信條例》*
要求資料	*專員要求雅虎香港控股提供的資料，包括：(i)電郵帳戶的用戶資料；(ii)與國安局的往來書信；(iii)通知書，以及(iv)該等資料*
國安局	*中國國家安全局*
技術服務協議	*北京雅虎根據於 2003 年 2 月 19 日簽訂的技術服務協議，向北大方正提供技術服務，協助雅虎中國網站的營運*
判決書	*人民法院於 2005 年 4 月 27 日作出的判決書*
雅虎中國	*雅虎中國網站：* *"http://www.yahoo.com.cn"*
雅虎中國客戶服務組	*雅虎中國的客戶服務組*
雅虎中國法律組	*雅虎中國的法律組*
雅虎香港	*雅虎香港網站:* *"http://www.yahoo.com.hk"*

詞彙表

雅虎公司	*雅虎香港控股的最終母公司（以美國加利福尼亞州爲基地）*
雅虎香港控股	*雅虎香港控股有限公司（現稱雅虎香港有限公司）*
雅虎香港控股印章	*雅虎香港控股的公司印章*

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.