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 [illegible] 月二十七日

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

Annex

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.

Annex B

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.