報章剪輯

NEWSPAPER CUTTINGS

供立法會議員爲立法會程序的目的作參考用
For the personal use of Legislative Council Members for the purposes of the proceedings of the Legislative Council

立法會秘書處
Legislative Council Secretariat

Taskforce set up to probe internet leak of police complaint files

Norma Connolly

The Independent Police Complaints Council has set up a four-man taskforce to investigate how its files, containing details of thousands of complainants, were released on the internet.

Council chairman Ronny Wong Fook-hum said the team, which he would head, would deliver a preliminary report on Tuesday into how the leak occurred, how to remedy it and how to ensure there would be no recurrence.

Meanwhile, the information – 20,000 names, addresses and ID numbers of complaints since 1996 – remains on the internet among Google's archived files, despite requests from the IPCC to the search engine company to remove it.

After an emergency meeting yesterday morning, Mr Wong admitted that the incident had dealt a blow to the public's confidence in the IPCC. "The IPCC rests on the confidence of the public, and this incident damaged ... the mechanism in place for considering complaints against police," he said. The IPCC database was a standalone system that could be accessed only by members of the IPCC secretariat and a system maintenance contractor, he added.

He would not confirm if there was a connection between China Motif – the registered owner of website china2easy.com, on which the data appeared – and the maintenance contractor. But he added: "We don't rule out any possibility at this juncture."

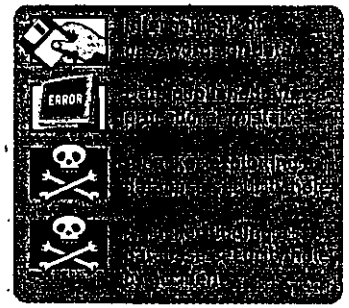
He said the company, and others involved in the inquiry, were co-operating. He would also not confirm if the contractor who carried out the maintenance work was responsible for the leak.

"We are not targeting any particular person," he said.

Yesterday Police Commissioner Dick Lee Ming-kwai distanced the police from the incident, saying: "The IPCC is an independent organisation, outside the police force. It is up to the IPCC to take steps to ensure its data is well protected."

The police Technology Crime Division is conducting an investigation into the potential criminal element involved and the privacy protection issues arising from the leak, at the request of the Security Bureau and the IPCC.

DATA TRAIL
How the files could have ended up on the internet



SMP Graphic

"So far we have asked the internet service provider to delete the information on the website. Unfortunately, some of the data has already been on the Web," Mr Lee said. "As far as the police systems are concerned, we have very extensive preventive measures to ensure that all our information and data are well protected."

He said police officers against whom complaints had been made were concerned about the security breach.

Mystery still surrounds exactly how the information, which was housed in a standalone database system not accessible over the internet, found its way onto the Web.

IT experts said yesterday there were several possible scenarios, ranging from an internal leak within the IPCC to procedural errors to hackers infiltrating the organisation's computer systems.

David Cheung Wai-lok, head of the computer science department at the University of Hong Kong, said that if the database was accessible on an intranet, it was possible that a password could have been passed to someone outside the IPCC.

The IPCC has set up a hotline, 2524 3841, for anyone concerned that their personal data has been released over the internet.

SEARCHES MEAN DATA MAY LIVE ON IN CYBERSPACE

The names, ID numbers and addresses of 20,000 people who have made complaints against police since 1996 could remain on the internet indefinitely.

The interest aroused in the leak of the Independent Police Complaints Council's (IPCC) confidential database has led media outlets, complainants and the public to search for the information online.

IPCC member Lo Wing-lok yesterday urged people not to search the Web for the information, saying this could make it impossible to ever remove the data.

"[I would advise] the public, members of the press and anyone interested in this matter to try to refrain from searching for this particular file on the internet," he said.

"The more you search, the more copies will be left on the internet. Then that information will never be deleted."

Lee Chan-hee, associate professor of computer science at City University, agreed that once it was widely accessed over the internet, it would be stored in the cache of various servers.

"That will make it difficult to completely wipe out," he said.

Even if deleted from Google's cached files, people who have accessed the webpage will still have the data on their servers.

IPCC chairman Ronny Wong Fook-hum warned that people who copied or stored the data could be traced. *Norma Connolly*

Details of 600 insurance holders found on Google

Records relate to policies bought from ING Life

Robin Kwong

More evidence emerged yesterday of security breaches making personal particulars available on the internet, as police chiefs scrambled to plug a loophole that allowed private details of complainants against the police to be leaked.

A *South China Morning Post* search found details of about 600 insurance policyholders freely available in the archives of the Google search engine, although the original file and website had been removed.

Meanwhile, telecommunications company CSL apologised for having leaked the personal records of some of its customers, which were also still available yesterday in the Google cache.

The *Post* found a database containing records of customers who bought insurance from ING Life between 1984 and 2004. It contained data on the type and amount of coverage bought, and beneficiaries' names, phone numbers, dates of birth and addresses.

The data was found in Google's cache in a search for database files.

Neither the original file nor the website on which it was posted, chings.no-ip.com, were still active. The search engine showed the information in the cache was retrieved on June 24 last year.

ING Life spokeswoman Carolyn Chung said she believed the records were leaked accidentally by an insurance agent.

"The agent took the file home to his personal computer. We believe his computer was hacked when he went online and that was how the file was leaked."

Ms Chung said the company learned of the incident yesterday through the agent, after a client contacted the agent about the leaked information. She said the company was investigating the matter and had contacted Google to ask that the data be removed.

"This is a very serious problem, although we do believe that it was an isolated case," Ms Chung said, adding that concerned customers could call the company's 24-hour hotline.

One of the clients, Patrick Yip Chi-wai, said he was a former assistant manager at ING Life and had trained insurance agents before leaving the company in 2003.

"We had a section that dealt with the personal data ordinance and did teach our agents to be careful with clients' data," Mr Yip said.

He said he was concerned but not shocked to learn of the leak, as ING had many agents. "So far there's no proof any harm has been done or that I've suffered any loss."

Insurance sector legislator Bernard Charnwut Chan said stricter guidelines and better enforcement were needed.

"I'm sure the agent did not intend the information to be leaked but this could serve as a very good lesson to the whole industry."

The Office of the Privacy Commissioner said it was not aware of the case but would investigate.

CSL said the data on its customers had been leaked by "manual mishandling [by] our service provider during the process of customer information arrangements".

It said it had contacted search engines to remove the relevant webpages. Last night, however, the information could still be accessed through Google's cache.

The cases have come to light since the *Post* reported on Friday that the data of about 20,000 people who filed complaints against police was available on the internet.

■ Privacy chief seeks more power – A2
■ Harry's view – A14

東方日報

保險公司600客資料網任睇

【本報訊】網上流傳個人資料風波未了，繼警監會及電訊商資料外洩後，再有六百多名保險公司客戶資料被放在網上，詳列投保人姓名、地址、電話、保單性質及保險經紀姓名等。個人資料私隱專員吳斌指出，公署已去信客戶資料外洩的流動電話網絡商「香港流動通訊有限公司」(CSL)，並呼籲各機構，尤其持有大量市民個人資料的政府部門，必須嚴格遵守私隱條例的規定。

CSL已刪外洩資料網頁

前日被揭發有五百名客戶資料外洩的CSL，昨日透過發言人回應表示，前日得悉事件已經即時跟進及刪除有關網頁，並要求搜尋器公司刪除連結紀錄，而經調查後，相信是服務供應商在部分資料處理程序上有人為疏忽。發言人強調，一向重視保障客戶資料，對事件引起部分客戶的不便深表歉意，並會作出積極檢討及跟進，避免同類事件再發生。

互聯網近日亦流傳約六百多名保險公司客戶資料，詳列投保人姓名、地址、電話、購買保單性質及保險經紀姓名等。安泰人壽發言人表示，前晚收到一名屬下保險經紀報告，指有客戶投訴接獲傳媒致電稱在互聯網上得悉其個人資料，該保險經紀估計是在家中使用電腦上網時，遭黑客入侵盜取有關檔案，內容涉及同組經紀共數百名客戶資料，已刪除有關檔案，公司亦已即時聯絡搜尋器公司刪除網頁紀錄。

■「one2free」涉網上泄露客戶資料。　資料圖片

CSL衛訊電訊涉泄客戶資料

再有兩家電訊網絡商，包括CSL及衛訊電訊把客戶資料在網上外泄，個人資料私隱專員公署已經去信要求網絡商，提供有關資料作跟進，暫時還未接到投訴。

日前有網友在網上搜尋到一分包括三百多個手機用户的名單，包括姓名、電話、電郵等資料，大部分是CSL轄下「1010」及「one2free」網絡的用户。

CSL：已即時刪除

CSL發言人指，昨日得悉事件後已即時跟進及刪除有關網頁，並要求搜尋器公司刪除連結記錄，公司調查後相信是服務供應商，在部分資料處理程序上出現人爲疏忽。公司對事件引起部分客户不便深表歉意，已積極檢討及跟進，避免同類事件再度發生。

另外，衛訊電訊公司發言人承認，公司內聯網的網址於上周六外泄，約五百名維修手機客户的資料包括姓氏和聯絡電話遭外泄，初步相信是密碼錯誤，導致其他人可以進入內聯網，公司發現後已即時加密網址。

政府130萬推廣資訊保安

立法會議員單仲偕（見圖）直指，自從發生警監會資料外泄後，市民憂慮政府的資訊保安措施是否足夠。工商及科技局局長王永平回應，當局會動用一百三十萬元，推廣資訊保安工作，有關款項是每年的恒常撥款數字，若評估後認爲有需要增加開支，會在內部調配資源。

本報記者

警監會7項補救措施

1	提升警監會電腦能力
2	涉及個人私隱資料機密檔案，需經助理秘書長授權
3	增聘一名熟悉電腦知識的行政主任
4	載有私隱資料的電腦需安裝在一獨立有鎖房間，不能隨便放在總務室
5	設有紀錄冊，詳細紀錄查閱時間及檢視人士身份
6	所有來自警察投訴科的投訴內容光碟，必須貯存在有鎖裝置內
7	日常檢查及維修人員都需接受保安檢查

資料來源：警監會主席黃福鑫

CSL客戶資料疑外洩

【本報訊】(記者　聶曉輝)一波未平，一波又起！警監會洩漏投訴人及客戶資料一事仍鬧得熱哄哄之際，本港竟又出現同類事件，且是「香港流動通訊有限公司」(CSL)轄下兩大流動電話網絡商「1010」及「One2free」的客戶資料！

姓名生日 一覽無遺

不少網友日前先後透過大型搜尋網站Google，在網上發現懷疑是商業機構的客戶資料，其中有網友搜尋到一份包括300多個手機用戶的名單，包括當事人的姓名、電話、電郵及曾訂購的電訊產品等資料，大部分均是網絡的用戶，更有網友在網上搜尋到近500名客戶的姓名、手機號碼、性別及出生日期等資料，私隱專員公署表示，有關資料可能被人利用某些渠道放在網絡上，公署會進一步調查是否有人刻意將個人資料放在網上，亦不排除會採取行動。

私隱公署擬採取行動

客戶資料在網上外洩，令市民人心惶惶，擔心會波及生活其他細節上。恒生銀行發言人向本報表示，該公司一向有內部守則去保障客戶的私人資料以不被外洩，系統亦非常嚴密；該公司一定會做足保安措施，故客戶可放心使用該銀行的信用卡。

警監會疑電腦公司疏忽致資料外洩

警監會就投訴人資料外洩事件公開初步調查報告，相信涉及外判電腦公司將警察投訴科的資料上載至伺服器，導致資料意外洩露，並於互聯網內流傳三年。警監會主席黃福鑫強調，不會因事件而引咎辭職。立法會議員認為，事件嚴重影響機構的公信力，促請當局全面重組投訴警察的制度，挽回公眾信心。

懷疑疏忽未為資料加密

警監會初步調查顯示，於二〇〇三至〇四年度外判的電腦公司協助警監會更新警察投訴科提供的數據時，將光碟資料轉載至伺服器上，懷疑外判的承辦商未有為資料進行加密程序，導致資料外洩。當中涉及的資料包括一九九六至二〇〇三年，其中七宗個案仍在調查。不過，警監會未有解釋為何有關資料由伺服器轉載至其他網頁，只強調四人小組仍在調查。

黃福鑫在記者會上表示，截至昨天傍晚警監會已收到超過一百名受影響人士的投訴。警監會將成立兩個小組委員會，由他本人與副主席梁家傑處理有關投訴，不過暫不會主動接觸其餘受影響人士。事件中負責的職員已自動提出放長假，而警監會亦會進行一系列措施，防止類似事件再發生。當局亦已去信Google及本地十間網絡供應商，要求停止寄存有關資料。

對於事件是否涉及警監會的警覺性不足，黃福鑫認為，責任並非目前的委員會成員，重申不會因事件而引咎辭職。他承認警監會正面對嚴峻考驗，但強調他個人離任與否並非最緊迫需要處理的問題。

梁家傑表示，已經與個人資料私隱專員吳斌會面，並就事件作出結論，同意任何人在未經許可的情況下盜用有關資料，可按既有程序發出執行通知。吳斌亦表示，已收到四個投訴及三個查詢，公署將按一貫程序進行調查。他呼籲公眾別因好奇而搜尋有關資料。

警監會主席黃福鑫（左）承認，警監會面臨嚴峻考驗，但強調不會因事件事引咎辭職。

警監會即時改善措施

- 提升警監會的電腦系統
- 助理秘書長或以上職員始能運用相關資料
- 使用者必須具備相關電腦知識
- 儲存資料的電腦改放於無密碼開啟的房間
- 使用資料時須登記
- 鎖妥存放有關資料的光碟
- 更新資料前須進行保安檢查

涂謹申重提投訴科獨立

立法會保安事務委員會主席涂謹申認為，外洩事件對警監會的公信力造成極大傷害。由於警監會屬於警察投訴制度中重要的組成部分，事件將影響公眾質疑警監會監察警察投訴科的能力，而資料外洩事件引起的後果更難以估計。

他認為，目前警監會有必要向二萬多名受影響人士作出書面通知，另一方面亦提醒有關人士注意個人資料有否被盜用。

雖然黃福鑫表示希望能夠盡快將警監會法定化，彌補事件對警監會公信力的損害，但涂謹申質疑這對挽回公信力毫無幫助。他說，早於回歸前，當時立法局已通過將警監會法定化的建議，但前保安司黎慶寧最後不滿條文要求警監會擁有第二調查權而收回草案。

他批評，政府一直拒絕將警察投訴科獨立於警務處以外，以致一直需要警監會的監察。如今警監會公信力受損，他將重提警察投訴科獨立。而泛民主派亦將於下周初出席聯合國人權事務委員會上，提出有關議題。

S. C. M. P.

Watchdog in dark on Net procedure

Police did not know names could have been deleted

Norma Connolly
and **Barclay Crawford**

A police complaints body was unaware it could have taken steps to remove from the internet the personal details of 20,000 people who have complained against the force over the past decade.

The safety of the complainants may have been jeopardised by a blunder that led to their names, addresses and identity card numbers being available on the Net.

Search engine Google said yesterday it had removed archived links to the list on Sunday, three days after the *South China Morning Post* inquired about the blunder.

Google spokeswoman Debbie Frost said the material was only deleted after the company became aware of the problem.

The Independent Police Complaints Council said on Saturday it had approached Google "through the proper channels" when it became known that the list remained in the public domain even though the website on which it appeared had been deleted.

The information could have been removed from the internet days earlier using simple instructions offered by Google to webmasters on how to prevent webpages appearing on the search engine's cache.

Nevertheless, fears remain that those who downloaded the list may place it back on the internet.

Earlier, complaints council member Lo Wing-lok urged the public not to search for the data because this may lead to it remaining on the Web indefinitely.

A spokesman for the council admitted the watchdog did not know it could have removed the data from Google's cache by itself.

"We are only a small office and do not have any in-house IT specialist. We took all relevant steps to have the data removed, including contacting the police, servers in Hong Kong, and Google, asking them to remove the cache."

Kwok Lau-for, associate professor at City University's computer science department, said if the webmaster of the site china2easy.com, on which the leaked data appeared, had been authorised by a supervisor, he could have deleted the information.

"He may not have been able to get rid of it without specific instructions," Dr Kwok said.

However, he said the way to remove cached information from the search engine may not be common knowledge among IT staff, admitting he had not been aware that this was possible without intervention from Google.

The complaints council says it believes the blunder that led to the names appearing on the site was caused by an external contractor who took the information home and downloaded the names.

Computer security consultant Richard Stagg, from Handshake Networking, said yesterday the incompetence in failing to properly secure the information was staggering.

"There is no reason why this information should have been anywhere near the internet," Mr Stagg said.