The Independent Police Complaints Council (IPCC)'s Report on Leakage on the Internet of Personal Data of People who have Complained against the Police

This paper presents to Members a report on the incident relating to the leakage on the internet of personal data of people who have complained against the Police.

Background

2. The IPCC came to know about the incident from the South China Morning Post (SCMP)'s report on 10 March 2006 that the personal data of about 20,000 people who had made complaints to the Police had been posted on the internet. Although the information was pulled from the two websites concerned after the SCMP had contacted the operators of the two websites, the information could still be accessed with the use of Google's cache – a memory of the search engine.

3. The IPCC held an urgent meeting on 11 March 2006 to discuss the matter and met with the press after the meeting. To actively follow up on the various issues arising from the incident, a four-member Task Force was set up to look into the leakage, consider the remedies and take immediate action to prevent recurrence. The Task Force worked over the weekend and submitted a preliminary report of its findings to the Council on 13 March 2006. The preliminary findings were also explained to the media following the Council meeting.

The Concerned Database

4. The IPCC Secretariat maintains a standalone system containing information about complaints against the Police, for statistical and record purposes. The system was set up by a contractor for the IPCC Secretariat. The same contractor has also been engaged to undertake maintenance for the system. The system is not linked to the internet.

5. Hitherto, access to the information on the database was confined to staff of the IPCC Secretariat who have operational needs to access the information, and to the system maintenance contractor in the course of system maintenance.

6. Since about 2003, the Complaints Against Police Office (CAPO) has been providing information to the IPCC in the form of a CD disc containing cumulative and updated information of complaints. The IPCC Secretariat had difficulties in accessing such information. Conversion of the CAPO electronic files was necessary for such data to be read by the IPCC Secretariat's computer. In 2003/04, the system maintenance contractor was called upon to render services to enable the IPCC Secretariat to access such information.

Initial Findings on Cause of Leakage

7. According to the contractor, he converted the data at his office/home. For his own convenience, he uploaded onto an FTP server the data he received from a disc which he obtained from the IPCC Secretariat. He thought that a password was required to upload the data, and did not realize that no password was required to access or download the same. He returned to the IPCC Secretariat a converted file and executable files, all stored in a CD disc.

Seriousness of the Problem

8. As mentioned earlier, although the information was pulled out of the two websites concerned, it had remained for some time in the cache of one of the major search engines and may have been accessed by others, although recent search shows that the information is no longer accessible in the original file name. More recently, it is found the information is still accessible and has been posted to newsgroups for downloading using the BT technology.

9. According to the information of the IPCC, most of the leaked data are past data, with seven on-going cases which are subject to review and in one extreme case to the 9th review. The data dates back to before 2004.

Immediate Remedial Actions

10. With immediate effect, IPCC has instructed that access to the database is confined to the Secretary, or to such persons with her express permission.

11. The IPCC has set up a hotline (2524 3841) manned by the staff of the Secretariat to handle public enquiries in connection with this incident since 11 March 2006. As at 12:00 a.m. on 16 March 2006, 181 calls have been received.

12. The IPCC has also decided to set up two sub-committees respectively headed by Mr Ronny WONG, Chairman and Hon Alan LEONG, Vice-chairman of the Council to meet those who have expressed genuine concern on the incident. These people must properly identify themselves and their identities will be verified. The sub-committees will see what measures can be taken to address those concerns.

13. The Privacy Commissioner has also been contacted and he will initiate an investigation into the matter. The Chairman and staff of the Secretariat have already met the Privacy Commissioner to provide initial details, and will fully co-operate in the investigation. In the meantime, the Privacy Commissioner has advised the public that, in accordance with Data Protection Principle (DPP) 1 of the Personal Data (Privacy) Ordinance (Cap 486) (the Ordinance), all personal data shall only be collected for lawful purposes, in a lawful and fair manner in the circumstances of the case. In addition, DPP3 provides that personal data shall only be used for the purposes for which they were originally collected or a directly related purpose. As the information contained in the IPCC database is for internal use only, any collection or use of such information will be in breach of DPP1 and/or DPP3 of the Ordinance. We understand the Commissioner's Office will carry out an investigation promptly on any illegal use of such information and offenders will have to bear civil or criminal liabilities. It is hoped that the explanation of the position of the law will help deter any further unauthorized access and use of the information.

14. To actively stop further circulation of the information on the internet, the IPCC has contacted Google and other search engine companies and Information Service Providers to appeal for their assistance in erasing the cache with the information. The cooperation from most of them has been obtained. The IPCC is also working with the Commercial Crime Bureau of the Police to provide intelligence through cyber monitoring and to see if further unauthorized posting of the information on the internet constitutes any crime committed (e.g. under section 161 of the Crimes Ordinance (Cap 200) "Access to computer with criminal or dishonest intent"), and for action to be taken.

15. The IPCC has sought the Chief Government Information Officer's urgent advice on steps which can be taken to continuously track and delete the remaining traces of the data on the internet, and to prevent further spreading of the data and ways to mitigate the damage.

Other Remedial Actions

16. The following actions have been proposed:

(a) upgrading the capability of the computer containing the database so that more advanced software can be installed. This in turn provides better protection on the database;

(b) limiting the right of access to the database to officers with the rank of Assistant Secretaries (AS) or above and persons with their written authorization;

(c) the IPCC Secretariat should engage an officer who has IT expertise to handle the database;

(d) the computer used for data processing should be placed in a separate room with locks. Only the IT officer should have the key to this room which serves as his/her office as well;

(e) maintain a log book attached to the computer. Any person who wishes to utilize the database should sign his/her name together with the title, date, starting and completion time on accessing the database, etc. This log book should be reviewed by the supervising officer of the IT officer on a weekly basis to ensure that no mishandling has taken place, and to monitor who has been accessing the information;

(f) reiterate that the disc(s) containing the database provided by CAPO should be locked in a cabinet housed inside the office of the AS mentioned above. Only he/she and the IT officer have the keys to the cabinet;

(g) security checks should be conducted on outside workers performing regular maintenance on this specific computer. He/she should be accompanied by IPCC staff at all times while working on the computer to ensure that no information has been downloaded without being noticed;

(h) make it clear again that sensitive data must not be copied onto discs;

(i) ensure that the computer in question is never linked to the internet; and

(j) back up the data from this computer, and the AS keeps the back-up discs securely.

17. These are provisional measures which will be forwarded to the Privacy Commissioner as part of our response to his investigation. The IPCC will comply with the Privacy Commissioner's recommendations given in due course.

Legal Action

18. The Council is aware that litigation would incur massive public resources and is of the view that it may be inappropriate to institute legal proceedings without careful consideration at this juncture, and actions in other avenues.

The Council's Appeal

19. The Council understands the damage of this incident and has offered a sincere and unreserved apology to the general public, and in particular, to those people who have been affected by the leakage.

20. Although the IPCC is doing its utmost to limit the circulation on the internet, given the present state of information technology, the IPCC's effort alone is insufficient to stop and prevent the circulation of the information on the internet. The general public's support is needed. The Council reiterates its appeal to the public and the media to stop searching or circulating such information on the internet. In a mature society, everyone has a moral duty to respect others' interests. Furthermore, as mentioned above, unauthorized use of such information is subject to criminal and civil liability.

The Independent Police Complaints Council
March 2006