

**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: R05-7230
Date issued: 8 December 2005

報告編號：R05-7230
發表日期：2005 年 12 月 8 日



香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

**The practice of collection of employees' personal data
by pinhole cameras without proper justification is excessive and unfair
in the circumstances of the case**

Case number: 200507230

This report in respect of an investigation carried out by me pursuant to section 38(b) and section 38(ii) of the Personal Data (Privacy) Ordinance, Cap 486 (“the Ordinance”) against Hongkong Post is published in the exercise of the power conferred on me by Part VII of the Ordinance. Section 48(2) of the Ordinance provides that *“the Commissioner may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, publish a report –*

(a) setting out –

(i) the result of the investigation;

(ii) any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and

(iii) such other comments arising from the investigation as he thinks fit to make; and

(b) in such manner as he thinks fit.”

Roderick B. WOO
Privacy Commissioner for Personal Data

The Incident

It was reported in local newspapers on 18 June 2005 that pinhole cameras were found installed by Hongkong Post in the working areas, near the toilets and changing rooms of the Cheung Sha Wan Post Office (“CSW Office”). Hongkong Post’s response was that pinhole cameras were installed for the purpose of detecting crime as a result of a series of stamp theft cases occurring at CSW Office. They believed that the use of pinhole cameras was an effective way for them to identify the culprit(s) and gather evidence.

Investigation conducted by the Privacy Commissioner for Personal Data

2. The matter raises privacy concern as the staff being unaware of the extensiveness and intrusiveness of the covert monitoring undertaken, feared that their personal data might be unfairly and unreasonably collected. In determining whether such act or practice contravenes the requirements of the Ordinance, the Privacy Commissioner for Personal Data (“the Commissioner”) exercised his regulatory function and declared an investigation against Hongkong Post on his own volition.

3. A site visit was paid by the investigation staff of the Commissioner at CSW Office ascertaining the locations of the pinhole cameras and footages of the recorded video tapes were viewed. Hongkong Post gave submissions on the use of pinhole cameras and furnished the Commissioner with departmental rules, information and documents relevant to the questions raised.

The Law

4. The Ordinance aims to protect the privacy of individuals in relation to personal data and the following requirements in relation to collection of personal data and transparency of the policies and practices are of particular relevance to the present case.

Data Protection Principle (“DPP”) 1(1) provides that personal data shall only be collected for a lawful purpose directly related to the function or activity of the data user and that the data

collected should be necessary, adequate but not excessive.

DPP1(2) provides that personal data shall be collected by means which are lawful and fair in the circumstances of the case.

DPP5 provides that a data user shall take all reasonably practicable steps to ensure that its policies and practices in relation to the kind of personal data held and their purposes of use should be made generally available.

The Privacy Guidelines: Monitoring and Personal Data Privacy at Work

5. The Privacy Guidelines: Monitoring and Personal Data Privacy at Work (“the Guidelines”) were issued by the Commissioner in December 2004 under section 8(5) of the Ordinance indicating the manner in which the Commissioner proposes to exercise his functions and powers in relation to the activity of employee monitoring.

6. Before deciding to undertake employee monitoring where personal data are to be collected, the Commissioner views it as important that there should be careful **assessment** of the appropriateness of such activity by evaluating the business risks to be managed and the likely adverse impact that monitoring may have on the personal data privacy of employees. Due consideration should be given to the use of other equally cost effective but less privacy intrusive **alternatives** and the employers be **accountable** for the actions embarked. Indiscriminate monitoring activities such as randomly subjecting all employees to universal and continuous monitoring is privacy intrusive, much so if it is carried out covertly. Covert monitoring is not to be practised unless justified as last resort measures and being absolutely necessary in detecting or gathering evidence for unlawful activity which should be limited in scope and duration.

7. The transparency of the monitoring practice will ease employees’ privacy concerns and the employers shall as far as practicable, formulate a **clear** employee monitoring policy by making known and **communicating** to the employees the purposes of monitoring, the circumstances under which monitoring will take place and the kind of personal data that will be collected.

Personal data collected shall be carefully **controlled** on their proper use, accuracy, retention and access.

Result of the investigation

Breach of DPP1(1): excessive collection

8. The site inspection revealed that six pinhole cameras were installed at different working locations of CSW Office, one of which was located on the wall outside the female toilet entrance overlooking the corridor outside. As the cameras were either discreetly concealed inside a socket-like box on the ceiling/wall or the ceiling tile atop the area subject to monitoring, it was difficult for anyone to notice their existence.

9. The Commissioner was satisfied that Hongkong Post has a legitimate purpose to protect its and its customers' property from theft and agreed that public confidence in mail security is of cardinal importance. However, in evaluating the extent of business risk of theft that it faced, the Commissioner looked at all the relevant circumstances and concluded that the evidence available did not show the existence of risk of loss to such extent as to justify the engaging in vast scale video monitoring activities, in particular the use of pinhole cameras which is highly privacy intrusive. Organizational data user like Hongkong Post is required to display a high standard in proper personal data management given the number of employees who may be affected as a result.

10. Hongkong Post could not produce any documents, whether written or otherwise, evidencing the assessment process, if any, undertaken on the impact that such employee monitoring activities might have on employees' personal data privacy. No evidence was submitted showing that Hongkong Post had given due consideration to the use of other less privacy intrusive alternatives, such as relocating the existing overt CCTV cameras (which were installed for general security purpose), reviewing the workflow or conducting closer supervision of staff, etc. so as to identify or narrow down the scope of suspects before deciding at its own volition to embark on covert monitoring. The dimension and extensiveness of the monitoring activity carried out was out of proportion to attaining the purpose of collection and the inference that could

lawfully be drawn is that Hongkong Post was intent upon engaging in continuous and universal preventive monitoring.

11. The Commissioner is therefore of the view that the engaging in employee monitoring activity in such dimension and scale by Hongkong Post to collect evidence of crime given the vast amount of personal data that could be captured without the knowledge of the employees is excessive for their functions and activities, and thus in breach of DPP1(1).

Breach of DPP1(2): collection by unfair means

12. Assuming that employee monitoring activity was necessary to be undertaken by Hongkong Post, the manner in which it was carried out, i.e. the use of covert pinhole cameras was not shown to be fair and reasonable in the circumstances of the case for collecting evidence of crime.

13. There was no evidence showing that the use of covert means is absolutely necessary and that use of other overt means would necessarily frustrate the purpose of collection. Evidence before the Commissioner only showed that Police were aware of the use of pinhole cameras by Hongkong Post but there was no evidence that Hongkong Post acted upon the Police's request to install pinhole cameras. There was no evidence before the Commissioner that the utility of overt monitoring had ever been put to test such as, for example, by locating the existing CCTV cameras to the same or nearby locations as the pinhole cameras to detect any surreptitious or abnormal behaviour which might prove effective in narrowing down the scope of suspects.

14. The Commissioner also finds the period in which covert monitoring was engaged objectionable. The pinhole cameras were found ineffective in identifying the culprit in the last incidence of theft case (in February 2005) but Hongkong Post continued with the practice without reviewing its effectiveness. It was only after the widespread media reporting that Hongkong Post ceased such practice. Though Hongkong Post contended that they intended to cease the covert monitoring when they could either catch the culprit or conclude that it failed to achieve the purpose of such installation, there was no evidence that any specific review plan or policy existed on how long such covert monitoring would last and when it would cease. The universal and continuous covert

monitoring without a definite plan or policy for its duration is highly privacy intrusive, aggravating the harm, if any, that may be inflicted upon innocent parties.

15. During the investigation, no evidence was found showing that covert monitoring was practised in places where there is reasonable expectation of privacy, such as toilets or changing room. However, based on the reasoning above, the Commissioner finds the covert monitoring was carried out by Hongkong Post in an unreasonable and unfair manner, contravening the requirements of DPP1(2).

Contravention of DPP5: lack of transparent policy and practice

16. Where employee monitoring is to be undertaken, reasonable practicable steps should be taken to formulate and communicate a clear privacy policy statement (preferably in written form) to persons affected by the monitoring activity.

17. According to information supplied by Hongkong Post, there was no personal data privacy policy in place in respect of employee monitoring. The issues such as the purpose of collection and use, the circumstances under which monitoring would take place, the manner in which monitoring may be conducted and the kind of personal data that may be collected were not properly addressed.

18. An effective employee monitoring policy is imperative especially for organizational data users like Hongkong Post and where personal data are envisaged to be collected for the purpose of detection of crime or gathering of evidence of unlawful acts, these should as far as practicable be explicitly spelt out. Since Hongkong Post had already engaged in overt CCTV cameras for security reason through which personal data might be collected, there is a real need to implement an effective monitoring policy which should be brought to the attention of the employees affected. Hongkong Post was found not to have taken reasonably practicable steps to comply with DPP5.

19. On the basis that the Hongkong Post does not have a privacy policy to address employee monitoring activity by using video recording system and given the functions and activities carried out by Hongkong Post, the

Commissioner finds that Hongkong Post had contravened the requirements of DPP5.

The Enforcement Action

20. In view of the likelihood that such contravention will be continued or repeated, the Commissioner, in exercise of the powers vested upon him under Section 50 of the Ordinance, issued an enforcement notice to Hongkong Post directing them, *inter alia*, to:

- ➔ immediately cease the practice of covert monitoring by removing the six pinhole cameras installed at CSW Office;
- ➔ completely destroy the records, if any, collected by these pinhole cameras;
- ➔ formulate a general privacy policy statement in relation to video monitoring activities carried out in compliance with DPP5;
- ➔ regularly bring the video monitoring privacy policy developed to the notice of the staff, and implement effective measures (such as provision of regular training and supervision) to ensure compliance with the policy by persons duly authorized to carry out the monitoring activities.

Progress of enforcement actions followed by Hongkong Post

21. Subsequently, Hongkong Post confirmed to the Commissioner that they:

- ➔ had ceased the practice of covert monitoring and all the pinhole cameras had been dismantled;
- ➔ had destroyed all the records collected by these pinhole cameras;
- ➔ had formulated a personal data privacy policy on staff monitoring after consulting staff representatives of their departmental consultative committee. The policy would be incorporated in their departmental rules

and promulgated by issuing a notice to all their staff in the weekly circular;

- ➔ would re-circulate the privacy policy once every six months to remind their staff. Their Management Control Teams would conduct checks at the offices during their regular inspection in these offices. In the meantime, their designated departmental Personal Data Protection Officer had recently given a briefing to all their post office managers on this subject to assist them in complying with the new policy.

Recommendations arising from the investigation

22. This incident, which was widely discussed among the public, raised privacy concerns about the act or practice of employee monitoring activities carried out by the employers at the workplace. The Law Reform Committee's report, "Civil Liability on Invasion of Privacy" issued on 1999 recommended the Commissioner to give consideration to the issuance of "... a code of practice on all forms of surveillance in the workplace...". In response to that and having consulted public opinion on the matter, a self regulatory approach was found to be more appropriate to address the issue and practical guidance was given by the Commissioner in relation to the four common types of monitoring activities, i.e. video, telephone, e-mail and internet monitoring practised by employers to facilitate their compliance with the requirements of the Ordinance. The Guidelines, gazetted and published in December 2004 aims at setting recommended standards of personal data management in the context of employee monitoring.

23. Employee monitoring activities which result in the collection of personal data are caught by the Ordinance. The Ordinance, however, does not apply to situation where there is no collection¹ of personal data. Thus, where CCTV is installed without turning on its recording function or where the position or viewing range of camera does not focus on any particular individual, it is likely that there is no collection of personal data. However, if it is the intention of the employers also to record or compile information about any individual upon happening of certain event, such as, when crime occurs, they

¹ According to case law, there is no collection of personal data unless the collecting party is thereby compiling information about an individual whom he has identified or intends or seeks to identify and that his identity is an important item of information.

should give due consideration to the proper personal data management required by the Ordinance. The collection of personal data by covert means is a highly privacy intrusive act and is not to be encouraged. However, an employer may in exceptional circumstances find it necessary and justifiable to engage in covert video monitoring for the purpose of detecting or gathering evidence of crime against an unlawful act. In deciding to undertake covert monitoring, factors such as the need to carry out such monitoring activities, the fairness and reasonableness of the activities as well as the transparency of the practice are major issues that the employers should carefully consider so that the employees' personal data privacy is not indiscriminately invaded.

24. It is therefore recommended that:-

(A) Evaluation be made on the need to carry out covert video monitoring and on its scope and manner:

- (1) Covert video monitoring without the knowledge of the data subjects is generally viewed as an unfair means of collection unless justified by the existence of special relevant circumstances such as when there is reasonable suspicion that an unlawful act was, is or will be committed and it is absolutely necessary to undertake covert video monitoring for detection of unlawful activities or gathering of evidence of crime. The adverse impact that such activity may have on the personal data privacy rights of the employees should be carefully assessed, for instance, covert video taping is not to be practised in places where there is genuine expectation of personal privacy, such as toilets or changing room.
- (2) Overt means or other less privacy intrusive alternatives of collection of personal data should as far as practicable be first resorted to in order to test for its utility in particular where the number of employees who may be affected by such practice is substantial unless it is shown to be futile or would likely to prejudice the detection of crime or the successful gathering of evidence.

- (3) When covert video monitoring is to be undertaken, the scope and scale of such activities should be properly confined so that they are proportional to the extent of business risks that the employer has to handle. It should as far as practicable be targeted on likely or known suspects, at areas of high risks and for limited duration only. Universal, indiscriminate and continuous covert video monitoring for undue long period of time without cause should be avoided as far as possible.
- (4) Once the suspect is identified or evidence of crime gathered, the covert monitoring should cease immediately and all unnecessary video records be safely destroyed and not be excessively retained. Covert video monitoring should also cease when after a reasonable period of time it is found to be ineffective in achieving the purpose of collection. Close supervision on its proper implementation as well as review on its effectiveness is therefore necessary.
- (5) It is good practice that the evaluation process mentioned above and the less privacy intrusive alternatives engaged or considered be clearly documented for evidentiary purpose and to ease the employees' privacy concerns.
- (6) Lastly, it is emphasized that covert video monitoring is to be undertaken only as an exception rather than a norm and an employer is to be accountable for the lawfulness and fairness of such activities which may become a subject of complaint by the persons affected.

(B) Transparency of the video monitoring policy

- (7) A privacy policy statement in respect of the policy and practice in undertaking video monitoring activities including the purpose of collection of personal data, the circumstances under which it is to be undertaken, the kind of personal data that are to be collected and the uses to be applied for such data collected should be clearly written and communicated to persons affected. In situation where covert monitoring is to be engaged when it is

absolutely necessary for the detection of crime or gathering of evidence of the unlawful act, the nature of the exceptional circumstances under which covert monitoring is to be carried out should as far as practicable be sufficiently spelt out in the privacy policy statement and be made known, in particular where the adverse impact of such covert monitoring activities on employees' personal data privacy is significant.

- (8) The policy should also cover other useful information such as the personnel responsible to carry out the covert monitoring activities, the retention period of the video records collected and how the unused records are safely erased or disposed of. The classes of transferees of these covertly obtained records shall as far as practicable be made known as well as the adverse action, if any, that may ensue, such as the referral of the evidence to law enforcement agencies, dismissal or disciplinary action that may be taken by the employer, etc.
- (9) Where the actual practice on covert monitoring has changed or where the video monitoring policy does not adequately and completely cover the actual situation, the policy should be reviewed and revised accordingly so as to keep it accurate and up to date. The mechanism or policy to review the effectiveness of the covert monitoring activities once it is engaged should also be devised and implemented to ensure that such practice shall cease when shown ineffective to detect crime or gather evidence of unlawful act.
- (10) Consultation with the employees to ascertain their reasonable expectation of personal data privacy in the workplace and the communication with the employees of the rationale behind the undertaking of covert video monitoring will be helpful to implement and execute a video monitoring policy that is acceptable to the employees.

Conclusion

25. The Commissioner is glad to note that Hongkong Post has positively responded to this investigation and regarded it as a valuable learning experience for them to improve their management of personal data and staff relations. Appropriate measures have now been taken by them to ensure that the privacy of their individual staff in relation to personal data is well protected.

26. The Commissioner emphasizes that nothing in this report shall be construed as indicating the passing of any moral judgment on the carrying out of employee monitoring activities covertly by employers which remains a matter for them to decide. However, where such activities result in the collection of personal data, care should be taken to ensure that the act or practice complies with the requirements of the Ordinance. A careful assessment of the need, scope and extent of the monitoring activities to be conducted, the use of only fair and reasonable means for collection and the implementation of a clear policy and practice on employee monitoring activities are all seen to be conducive to building mutual trust where business thrives in a privacy friendly environment.

Office of the Privacy Commissioner for Personal Data, Hong Kong
Unit 2401, 24/F, Office Tower, Convention Plaza,
1 Harbour Road, Wanchai, Hong Kong

Tel: 2827 2827

Fax: 2877 7026

Website: www.pco.org.hk

E-mail: pco@pco.org.hk

© Reproduction of all or any parts of this document is permitted on the condition that it is done for a non-profit making purpose and due acknowledgement is made as the source.