HONG KONG LAW JOURNAL
香港法律學刊

VOLUME 43 ■ PART 3 ■ 2013

Applying the Personal Data (Privacy) Ordinance to Employee Monitoring

❐

Eric A Szweda

Applying the Personal Data (Privacy) Ordinance to Employee Monitoring

❐

*Eric A Szweda**

Changes in the ways we work and communicate increasingly challenge the ability of organisations to evaluate performance and control conduct. Monitoring personnel in some form or fashion, which increasingly means the monitoring of communications, as well as conduct occurring outside of the traditional workplace, is necessary. However, the scope and methods can present difficult questions due to a variety of considerations, which sometimes conflict. Developing a monitoring plan that balances the various considerations has never been more difficult. In this paper, these issues are evaluated under the legal landscape in Hong Kong. Regulatory codes, guidance and investigation reports, as well as administrative appeal decisions, court cases, and commentary bearing on these issues, are compiled and assessed. The author in turn attempts to charm out a useful construct, to be used as a tool for decision-making in connection with the development of a workplace monitoring plan compliant with the Personal Data (Privacy) Ordinance.

1. Introduction

Changes in the ways we work and communicate increasingly challenge the ability of organisations to evaluate performance and control conduct. Monitoring personnel in some form or fashion, which increasingly means the monitoring of communications, as well as conduct occurring outside of the traditional workplace, is necessary. Societal expectations have given rise to robust compliance functions in large organisations. Developing a monitoring plan that balances various and sometimes competing considerations, however, has never been more difficult.

* Managing Partner, Troutman Sanders, Hong Kong. The author is a dual qualified Hong Kong solicitor and American attorney. Mr Szweda is a graduate of Cornell University's School of Industrial and Labor Relations and Vanderbilt University's School of Law. The author is grateful for comments made to drafts of this paper by former Hong Kong Privacy Commissioner for Personal Data, Roderick B Woo, Dr Anne SY Cheung, Professor of Law and Co-Director, Law and Technology Centre, University of Hong Kong School of Law, and the author's colleagues, Ashley Hager and John Hutchins. The statements expressed herein, however, are the responsibility of the author alone.

Recent events demonstrate that under monitoring as well as over monitoring can be highly detrimental. On one hand, an expanding array of regulatory obligations necessitates greater monitoring. For example, certain elite investment banks were sharply fined recently by the United Kingdom's financial regulators because of their failure to actively monitor and control the conduct of their traders. Their employees had manipulated the data sent to the Bank of England upon which the LIBOR rates are set, well evidenced by the banks' internal employee e-mails.[1] Or, the failure to at least put into place systems to adequately monitor executives engaged in securing governmental contracts can likewise lead to increased liability in bribery investigations.[2] Apart from regulatory obligations, the failure to monitor the delivery truck driver with a habit of texting on company provided devices while driving the company delivery truck or the decision not to monitor the Facebook posts of the high speed train driver could prove dire. Moreover, the increasing importance of intellectual property to many organisations, rising hand in hand with the increasing ease at which intellectual property can be stolen electronically, means that many companies must be more vigilant as to the preservation of competitive knowledge, against internal and external threats.

On the other hand, monitoring requires compliance with an expanding body of data protection and privacy regulations emerging across Asia-Pacific today, as well as other laws. The failure of organisations to properly manage personal data or otherwise respect what may be considered the privacy of others has led to resignations of chief executive officers, including in Hong Kong in the case of the Octopus smart card company and in America with respect to Hewlett-Packard, as discussed herein.

Apart from legal compliance, a flawed monitoring plan can negatively affect internal morale as well as the public's view of the organisation. However, employee monitoring also can be seen as beneficial by

[1] By way of example, the UK's Financial Services Authority (the "FSA") fined UBS AG ("UBS") the sum of £160,000,000, finding that "the practice of attempts to manipulate LIBOR and EURIBOR submissions to benefit trading positions was often conducted between certain individuals in open chat forums and in group emails…". *See* FSA's Final Notice, para 19, 19 December 2012. The FSA further found: "UBS, because of a poor culture in its interest rate derivatives trading business and weak systems and controls, failed to prevent the deliberate, reckless and frequently blatant actions of its employees." FSA's Final Notice, para 189; see also N Summers, The UBS Libor-Fraud E-mails Are a Gift for Regulators, 19 December 2012, available at http://www.businessweek.com/articles/2012-12-19/the-ubs-libor-fraud-emails-are-a-gift-for-regulators.

[2] For example, the UK's Bribery Act, which came into force in July 2011, and applies extraterritorially to organisations falling within its coverage, criminalises the "failure of a commercial organisation to prevent bribery". An organisation has a possible defence, however, if it can demonstrate it had implemented procedures designed to prevent bribery. Likewise, American authorities make plain that organisations undertaking to monitor their personnel effectively will be in a better position to defend themselves. *See*, for example, Department of Justice, Office of Public Affairs, "Former Morgan Stanley Managing Director Pleads Guilty for Role in Evading Internal Controls Required by FCPA" Justice News (25 April 2012), available at http://www.justice.gov/printf/PrintOut3.jsp.

employees. For example, in a 2011 household survey conducted in Hong Kong, fifty per cent of the respondents agreed with the statement: "As a whole, my company has benefitted from workplace surveillance".[3]

To monitor effectively and in compliance with applicable laws is increasing operating burdens. Among other things, greater coordination between the business units, human resource management, information technology, security and legal functions is increasingly necessary. Once information is collected, additional costs and regulatory obligations arise. Even organisations attuned to careful collection and use of personal data may find their databases being harvested, hacked or made subject to the demands of governments seeking to develop more information about their citizens, giving rise to additional concerns over the maintenance, security and retention of data.[4] Data breaches are detrimental for individuals in terms of dealing with the harms of identity theft and for organisations in terms of costs and reputational damage. While much of this is beyond the scope of this article, all of it underscores the increasing importance and many facets of information management today.[5]

The focus of this article is the Personal Data (Privacy) Ordinance (the Ordinance) as it relates to employee monitoring. The Ordinance was one of Asia's first comprehensive data protection statutes, enacted in 1995 and amended in 2012.[6] As will be seen herein, Hong Kong's regulatory system is built around a set of enumerated principles, which organisations must determine how to apply to their specific circumstances.

2. Statutory and Regulatory Framework

> "The Personal Data (Privacy) Ordinance, Cap. 486, seeks to protect the privacy of all persons in relation to information personal to them. If an employer (a data user) wishes to collect in a recorded form personal data of its employees (data subjects), it may only do so to the extent provided for, and in a manner specified, in the Ordinance".[7]

[3] University of Hong Kong "Report of the Survey on Personal Data and Privacy Awareness in Hong Kong, 2011", (February 2012) (hereinafter, "HKU Privacy Awareness Survey"), available at http://www.lawtech.hk/wp-content/uploads/2012/04/Survey-on-Privacy-Awareness-in-HK-HKU-2012.pdf; *see* also n 40 below.

[4] *See* for example R MacKinnon, "Shi Tao, Yahoo!, and The Lessons of Corporate Responsibility" (Working Paper, Journalism and Media Studies, University of Hong Kong, 30 December 2007), available at http://rconversation.blogs.com/YahooShiTaoLessons.pdf.

[5] *See* also World Economic Forum, Personal Data: The Emergence of a New Asset Class (2011).

[6] For an excellent discussion of the changes effected by the Personal Data (Privacy) (Amendment) Ordinance 2012, *see* Roderick B Woo, "Hey, Don't Fool Around with My Personal Data!" (October 2012) *Hong Kong Lawyer* 39.

[7] *Cathay Pacific Airways Ltd v Administrative Appeals Board* [2008] 5 HKLRD 539, 541.

Section four of the Ordinance directs that when an employer collects and uses its employees' personal data, it must do so in accordance with a set of Data Protection Principles enumerated in the Ordinance. Under s 65 of the Ordinance, employers are liable for the actions of their employees taken in the course of their employment, whether or not such acts were engaged in with the approval or knowledge of the employer. Employers are also liable for the acts of their agents.[8]

Hong Kong's Office of the Privacy Commissioner for Personal Data (the Privacy Commissioner or Commissioner) is charged with promoting and supervising compliance with the Ordinance. To this end, in 2000, the Commissioner published a "Code of Practice on Human Resource Management" (HRM Code), in which the Commissioner states:

> "Failure to abide by the mandatory provisions of this code will weigh unfavorably against the data user concerned in any cases that come before the Commissioner. Where any data user fails to observe any of the mandatory provisions of this code, a court, or the Administrative Appeals Board, is entitled to take that fact into account when deciding whether there has been a contravention of the Ordinance".[9]

In 2004, the Privacy Commissioner published "Privacy Guidelines: Monitoring and Personal Data Privacy at Work" (Monitoring Guidelines). These guidelines are not mandatory like a code, but in the Commissioner's words, "constitute an approach that should be seen to be illustrative of best practices while at the same time acknowledging that there will always be certain exceptions to the rule".[10] Given technological change, the HRM Code and Monitoring Guidelines may have lost some usefulness. Since these publications, the Commissioner has published targeted guidance, including "Guidance on Collection of Fingerprint Data" (Guidance on Fingerprint Data), amended in May 2012, which is discussed herein in the section entitled "Emerging Technologies".

Apart from statutory law and regulations, under the common law employers must act in good faith in discharging their duties.[11] The

[8] *See* Office of Privacy Commissioner for Personal Data, "Outsourcing the Processing of Personal Data to Data Processors" (September 2012), available at http://www.pcpd.org.hk/english/publications/files/ dataprocessors_e.pdf.

[9] Office of Privacy Commissioner for Personal Data, "HRM Code" (September 2000) 1, available at http://www.pcpd.org.hk/english/ordinance/files/hrdesp.pdf.

[10] Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (December 2004) 3, available at http://www.pcpd.org.hk/english/ordinance files/monguide_e.pdf.

[11] *Sujal v Cathay Pacific Airways Ltd* (unrep., HCA 2220/2005, [2008] HKEC 1133), [31].

Commissioner has stated that the Monitoring Guidelines "do not affect the application of the common law duty of confidence that may arise in relation to employee monitoring".[12] The Basic Law, essentially Hong Kong's constitution, also sets forth a right to privacy in communications.[13]

3. Determining Whether and How Monitoring Can be Conducted

The Privacy Commissioner recognises "many legitimate reasons for monitoring employees" including specifically, managing workplace productivity, service or quality control, enforcement of company policies, protecting the safety of employees, business assets, intellectual property or other propriety rights, preventing vicarious liability where the employer assumes legal responsibility for the actions and behaviours of employees, and complying with statutory or regulatory obligations that provide or give reasonable cause for preventive monitoring of employees.[14]

Under the Data Protection Principles, the means by which data is collected must be "lawful" and "fair in the circumstances".[15] In the Monitoring Guidelines, the Privacy Commissioner sets forth a number of factors that should be evaluated by employers in deciding whether an employee monitoring plan constitutes a "fair practice".[16] The Commissioner's view is that compliance with the Data Protection Principles requires organisations to engage in an analysis designed to produce measures proportionate to the risk, taking into consideration the impact on those affected, and to develop a plan that can be managed properly across the life cycle of the collected data.[17] "In exercising employee monitoring, employers should seek to strike a balance between the pervasiveness of monitoring and the magnitude of the employers' risk that the monitoring aims to reduce. The issue therefore

[12] Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), p 7.

[13] "The freedom of privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in accordance with legal procedure to meet the needs of public security or of investigation into criminal offences.", Art 30 of the Basic Law. *See* also Art 14 of the Hong Kong Bill of Rights.

[14] Office of the Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), para 2.2.4,; *see* also Office of the Privacy Commissioner for Personal Data, Report on the *Collection of Employees' Personal Data by Covert Recording Device by Hong Yip Service Company Limited* (Report No R12-4839, 14 February 2012) ("Hong Yip" or "Hong Yip Report"), available at http://www.pcpd.org.hk/english/ publications/files/R12_4839_e.pdf.

[15] *See* Data Protection Principle 1 of Sch 1 of the Ordinance.

[16] Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), para 2.2.8.

[17] Office of Privacy Commissioner for Personal Data, "Hong Yip Report" (n 14 above), para 29.

is deciding what constitutes an acceptable level of monitoring".[18] The following sets forth potential factors to consider when developing a monitoring plan.

a. Is the Ordinance Triggered?

The Ordinance's obligations are triggered only if there is "collection" of "personal data". The Privacy Commissioner has stated that the following activities do not trigger the Ordinance: real time viewing of closed circuit television images, if not recorded; incidental recording of employees by a CCTV system installed for general security purposes; recording customer telephone conversations, if the sole purpose is to create a record of a customer transaction; and fingerprint data stored on a smart card and held only by the employee.[19]

"It may be difficult, in some situations, to ascertain whether a monitoring activity would amount to 'collection' of personal data and hence fall within the scope of these [Monitoring] Guidelines".[20] Therefore, it is necessary to pay particular attention to the definition of terms used in the Ordinance. Under section two of the Ordinance, *data* "means any representation of information (including an expression of opinion) in any document, and *includes a personal identifier*". (emphasis added) *Document* is broadly defined to include a disc, tape or other device, on which data or visual images are "embodied" and capable of being reproduced. In the Ordinance, *Personal data* is defined to mean any data:

(a) relating directly or indirectly to a *living individual*;
(b) from which it is *practicable for the identity* of the individual to be directly or indirectly *ascertained*; and
(c) in a form in which *access to or processing of the data is practicable*.

Collection is not a defined term in the Ordinance, but its meaning was litigated in the case of *Eastweek Publisher Limited and Privacy Commissioner for Personal Data*.[21] Photographers for Eastweek tabloid

[18] Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), para 2.2.7.
[19] Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), para 1.3.4. For a fuller discussion as to fingerprint data, *see* Office of Privacy Commissioner for Personal Data, "Guidance on Fingerprint Data" (May 2012) 2, available at http://www.pcpd.org.hk/english/publications/ files/Fingerprint_e.pdf.
[20] Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), para 1.3.4.
[21] (unrep., CACV 331/1999, [2000] HKEC 702).

took pictures of people, unknown to them, while out in public. Eastweek published an article critiquing, and in some instances ridiculing, the fashions of the people it photographed. While Eastweek did not know the identity of the individuals it photographed and then critiqued, the individuals photographed were readily recognised by friends, family and co-workers. Suffering humiliation, one of the individuals critiqued complained to the Privacy Commissioner. The Privacy Commissioner agreed that her photo could not be taken and used in the Eastweek publication without her consent. Eventually the matter came to the Court of Appeal, which rejected the Privacy Commissioner's interpretation of the Ordinance. The Court ruled that the Ordinance does not apply to collection of data unless the data sought is being collected about a person the collector has identified or intends to identify.

b. Assessing the Organisation's Need to Monitor

Monitoring must be justified based on consideration of the interests of the organisation and the individual.[22] The Privacy Commissioner has ruled repeatedly that Hong Kong employers have violated the Ordinance by implementing a particular form of monitoring justified only on asserted administrative savings to the employer, which were found lacking.[23] As to assessment of risk to the organisation, the Privacy Commissioner advises that "[m]ere perception of risk unconnected with the nature of the business would not be sufficient to justify employee monitoring".[24] To this end, the Privacy Commissioner recommends that "[i]n assessing the risks that are to be managed, employers should not only identify the risks but also justify, in a realistic manner, the existence and extent of those risks".[25] Monitoring can be used to protect the interests of third parties, such as clients or customers.[26] Monitoring must, however, align with legitimate business needs.[27]

The greater the risk of harm from failing to monitor, especially to the public, the greater the ambit of the employer to obtain and assess personal data. For example, while recognising that private medical reports are of

[22] Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), para 2.2.1.
[23] *Ibid.*, para 2.2.3.
[24] *Ibid.*, para 2.2.2.
[25] *Ibid.*
[26] *Ibid.*, para 2.2.3.
[27] *Ibid.*, para 2.2.4.

a highly sensitive nature, the Hong Kong Court of Appeal overruled the Privacy Commissioner and the Administrative Appeals Board, holding that it was lawful for an airline to collect current and historical medical records of its cabin crew employees. The rationale was that the airline is under a duty to ensure that cabin crew members remain medically fit under Hong Kong Civil Aviation Directions.[28]

c. Assessing Options and Alternatives with Reference to the Individuals Likely to be Subject to Monitoring

Once a legitimate organisational need has been established, reasonably identifying and assessing the universe of monitoring options and alternatives should be undertaken. Monitoring should be tailored to the need. "The indiscriminate collection of personal data, in particular, if it involves sensitive personal data, is likely to be viewed by the Privacy Commissioner as a contravention of Data Protection Principle 1(1), in that it may be considered not directly related to, or even excessive for, the organisation's function and activity".[29] The Privacy Commissioner also urges that the assessment of options include an analysis of likely adverse impacts of those affected, including potential risks of mismanagement or misuse of the data collected as part of what is sometimes referred to as a privacy impact assessment.[30] The Privacy Commissioner further urges that the expectations of employees should be taken into consideration, including possibly doing so through a consultative process.[31] As to the analysis of adverse impacts, the Privacy Commissioner suggests that employers evaluate the potential intrusiveness on an employee's privacy by addressing the following:

(a) To what extent will personal data relating to an employee's private life be monitored?
(b) What categories of personal data will be collected? Will the personal data privacy of third persons be affected?
(c) What harm may be inflicted upon employees as a result of improper management of personal data?

[28] *Cathay Pacific Airways Ltd v Administrative Appeals Board* (n 7 above).
[29] Office of Privacy Commissioner for Personal Data, "Data Protection Principles in the Personal Data (Privacy) Ordinance – from the Privacy Commissioner's Perspective (2nd Edition)" (2010), para 5.5, available at http://www.pcpd.org.hk/tc_chi/publications/files/Perspective_2nd.pdf.
[30] *Ibid*. *See* also A Chiang, Keynote Speech on *Information Highway – Linking Hong Kong to the Global Village and How Accountants Add Value* (Hong Kong Institute of Certified Public Accountants IT Conference 2010, 27 November 2010) 7.
[31] *See*, for example, Office of Privacy Commissioner for Personal Data, "Hong Yip Report" (n 14 above), para29.

(d) To what extent will the mutual trust essential for good employee relations be affected?

As to alternatives to, or otherwise limiting the scope or extent of monitoring, the Privacy Commissioner suggests the following factors:

(a) Can monitoring be confined to areas of high risk?
(b) Can monitoring be restricted to certain personnel if there is a reasonable suspicion of seriously improper conduct?
(c) Would selective or random checking, rather than continuous monitoring, be sufficiently effective?
(d) Can communications monitoring be restricted to the log records rather than the contents of communications?

Lastly, as provided in Data Protection Principle No 1(2), the means of collection must be "lawful" and "fair". "To the Commissioner, an obvious example of data being obtained by unfair and perhaps also unlawful means is personal data being obtained through deception or coercion…".[32]

d. Providing Notice, Managing Expectations and the Role of Consent

> "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".[33]

The following should be considered when developing and implementing a notification plan: Data Protection Principle No 1(3) provides that "all practicable steps" must be taken to ensure that the data subject is explicitly or implicitly informed, on or before collecting the data, as to whether it is obligatory or voluntary for him to supply the data and if obligatory, the consequences for failing to supply the

[32] Office of Privacy Commissioner for Personal Data, "Data Protection Principles" (n 29 above), para 5.16. *See* also Office of Privacy Commissioner for Personal Data, "HRM Code" (n 9 above), para 2.3.3. A noteworthy example of an activity found in another jurisdiction to be unlawful was Hewlett-Packard's use of what is called "pretexting", which involves the use of false pretences to deceptively obtain information. Hewlett-Packard hired investigators who assumed false identities to obtain information in order to identify the person leaking sensitive information from Board meetings. As with the Octopus scandal in Hong Kong, this scandal resulted in HP's CEO having to resign. HP also paid a fine exceeding US$14 million to the State of California.

[33] *See* Office of the Privacy Commissioner for Personal Data, Report on *The Practice of Collection of Employees' Personal Data by Pinhole Cameras Without Proper Justification is Excessive and Unfair in the Circumstances of the Case* (Report No R05-7230, 8 December 2005) (Hongkong Post Report), para 16a available at https://www.pcpd.org.hk/english/infocentre/files/R05-7230_e.pdv.

data. As to the content of the notice, Data Protection Principle 1(3) further provides that the data subject be explicitly informed of the purpose for which the data is to be used and the classes of persons to whom the data may be transferred, and informed of his access rights.[34] Also Data Protection Principle 5 requires that all practical steps shall be taken to ensure that a person can ascertain a data user's policies and practices in relation to personal data, including the kind of personal data held and the main purposes for which such personal data are to be used.[35]

As to the form or method of notice, the Privacy Commissioner advises in the Monitoring Guidelines that:

> "Employers who seek to monitor employees' activities relating to the use of work-related communication facilities are recommended to include in the Employee Monitoring Policy a clear statement regarding the conditions of use of such facilities ("house rules"). Declaring the 'house rules' will enable employees to be informed of the consequences of their actions and, once informed, respond with appropriate behaviors".[36]

In the HRM Code, the Privacy Commissioner provides:

> "As a matter of good practice, an employer should comply with the [HRM Code] notification requirements by means of a written Personal Information Collection Statement ("PICS"). This statement may, for example, be attached to, or printed as an integral part of standard employment forms used to collect data e.g., a job application form".[37]

As noted above, the Commissioner states that assessment of employee expectations is necessary in order to determine whether the subject monitoring is fair in the circumstances.[38] What is a reasonable expectation? How is it determined or judged? Determining societal expectations as to privacy may at times be difficult because it could be a moving target. Various Privacy Commissioners have noted that there is growing concern in Hong Kong society over the protection of personal information, but they also note the apparent lack of concern

[34] *See* also Office of Privacy Commissioner for Personal Data, "HRM Code" (n 9 above), para 1.2. *See* also *Cathay Pacific Airways Ltd v Administrative Appeals Board* (n 7 above), paras 51–52. *See* further Section four of this paper.

[35] Office of Privacy Commissioner for Personal Data, "HRM Code" (n 9 above), para 1.4.3; HKU Privacy Awareness Survey (n 3 above). *See* also Office of Privacy Commissioner for Personal Data, "Hongkong Post Report" (n 33 above), paras 16–19.

[36] Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), para 3.2.4.

[37] Office of Privacy Commissioner for Personal Data, "HRM Code" (n 9 above), para 1.2.1.4.

[38] Office of Privacy Commissioner for Personal Data, "Hong Yip Report" (n 14 above), para 30.

on the part of some younger workers with privacy in connection with their personal electronic communications. Nevertheless, the intense reaction in Hong Kong to the news that the Octopus smartcard provider had sold data on certain users should leave little doubt that concerns over data protection are widespread and deep in Hong Kong society today.[39] These concerns may arise increasingly in workplaces as well.[40] In any event, as the Commissioner has explained, employers can manage expectations by communicating a privacy policy pertaining to employee monitoring, such that its employees should expect that certain activities will be monitored. In this regard, it is in the employer's interest to provide robust notice, if at all possible.

Proper consent, informed and freely given, may eliminate issues as to whether the collection of data was "fair in the circumstances" under Data Protection Principle No. 1. "Generally speaking, if a data subject agrees to the collection of his personal data, the means of collection appears to be fair on the face of it".[41]

While in most circumstances organisations have a "duty" to ensure that a privacy policy pertaining to employee monitoring is developed and brought to the notice of employees before monitoring is introduced, notice is not required in all circumstances.[42] Notification requirements do not apply if notice would prejudice the purpose for which the data is to be collected and that purpose falls within the purposes specified in Part VIII of the Ordinance, namely specified exemptions.

[39] In 2010, this issue was among the top ten news stories in Hong Kong. *See* A Chiang, Keynote Speech at *Symposium on Personal Data and Privacy Protection: A Comparative Perspective* (University of Hong Kong, 10 February 2012) 7; *see* also "Octopus C.E.O. Brought Down by Scandal" *China Daily eClips*, 5 August 2010, available at http://www.cdeclips.com/en/hongkong/Octopus_CEO_brought_down_by_ scandal/fullstory_49093.html.

[40] *See* Anne SY Cheung, "An Evaluation of Personal Data Protection in Hong Kong Special Administrative Region (1995–2012)" *International Data Privacy Law*(Oxford University Press, November 2012) 13, (Professor Cheung notes that the majority of all complaints to the Office of the Privacy Commissioner are employment or otherwise work-related); *see*, for example, Ming Pao Daily, Bus Drivers Doubt Intention of Installing Video System in Buses, 49 (14 March 2013), available at http://news.mingpao.com/cfm/Search2.cfm?Keyword=%A4%45%A4%DA%A8%AE%AA%F8%A6%EC%B8%CB%C4%E1; *see* also n 3 above.

[41] Office of the Privacy Commissioner for Personal Data, Report on the *Employer Collecting Employees' Fingerprint Data for Attendance Purpose* (Report No R09-7884, 13 July 2009), available at http://www.pcpd.org.hk/english/publications/files/report_Fingerprint_e.pdf; *see* also Office of Privacy Commissioner for Personal Data, Report on *Collection and Use of Personal Data of Members under the Octopus Rewards Programme run by Octopus Rewards Limited* (Report No R10-9866, 18 October 2010), available at http://www.pcpd.org.hk/english/publications/files/R10_9866_e.pdf. In the Octopus Rewards Limited Report, the Commission found that the use of "small print" failed to constitute sufficient notice under Data Protection Principle 1(3).

[42] *See* also Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), para 2.4.1(a).

e. Assessing Whether "Special Circumstances" Exist, Justifying Covert Monitoring

"Owing to its highly intrusive nature, covert monitoring should not be adopted unless it is justified by the existence of relevant special circumstances".[43] To this end, the Privacy Commissioner suggests consideration of the following factors:

(a) Is there a reasonable suspicion of unlawful activity occurring, or likely to occur?
(b) Is covert monitoring absolutely necessary given the circumstances?
(c) Is covert monitoring likely to prejudice the detection or successful gathering of evidence?
(d) Can covert monitoring be limited in scope, both in terms of area and time?[44]

> "As a matter of principle, covert monitoring that makes use of video recording devices such as pinhole cameras that target at locations where employees have a reasonable expectation of privacy should be avoided. This applies to places such as toilets and changing rooms".[45]

f. Managing Access, Correction of Errors and Other Employee Concerns

> "An employer, on or before first use of the employment-related data, should explicitly provide information of the individuals' rights of access to, and correction of, their personal data and the contact details of the person to whom any such request may be made".[46]

> "The right to make a 'data access request' (DAR) is an important right vested in data subjects under the [Ordinance]".[47]

> "An employee who is the subject of monitoring has a right to request access to his or her personal data derived from monitoring records under section 18 of the PD(P)O. Unless exempted or prohibited from doing so under the PD(P)O, the employer is required to provide a copy no later than 40 days after receiving a data access request from the employee. In the event of the employer being unable to provide the copy within the

[43] Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), para 2.3.3.
[44] *Ibid.*
[45] *Ibid.*, p 15.
[46] Office of Privacy Commissioner for Personal Data, "HRM Code" (n 9 above), para 1.2.5. *See* also Data Protection Principle 1(3).
[47] Office of Privacy Commissioner for Personal Data, "Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users" (June 2012) 1, available at http://www.pcpd.org.hk/english/ publications/files/DAR_e.pdf.

> 40-day limit, the employer must communicate that fact and the reasons in writing to the employee concerned before the expiry of that period and must provide the copy as soon as practicable thereafter".[48]
>
> "The entitlement is to a copy of the data, it is not an entitlement to see every document which refers to a data subject".[49]

Apart from specific legal requirements, to the extent Hong Kong employers prefer that employees raise concerns internally, as opposed to externally, such as to the Office of the Privacy Commissioner, unions, or the press, Hong Kong employers may be benefitted by more actively engaging employees as to internal monitoring programs. To this end, the 2011 HKU Privacy Awareness Survey[50] may be useful for employers to consider. For example, more respondents agreed with questions identifying beneficial aspects of monitoring than with the statements such as workplace surveillance is privacy intrusive, or adversely affects employee relations. However, as to lodging a complaint if they had one, 50 per cent of the respondents would turn to the Privacy Commissioner's office, while only 13 per cent said they would take up the issue with the organisation that misused their personal data. Forty per cent of those employed in commercial organisations responded that they did not know whether their organisations had in place measures to protect their personal data. Hence, the survey may suggest some possibility for employers to better promote internal protections and procedures, such that employees may be encouraged to bring complaints internally, before bringing complaints externally.

g. Managing Use and Handling of Data

Under Data Protection Principle No 4, "all practical steps" must be taken to protect against unauthorised or accidental access, processing or erasure. As such, organisations must develop sophisticated internal procedures and systems to safely handle data. Personnel entrusted with handling personal data should possess adequate training concerning procedures and systems. Also, delinking databases or collection systems may reduce risk of improper disclosure or taking of data.[51] The Commissioner urges that "regular privacy compliance assessments should be carried out throughout

[48] Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), para 3.4.7, Explanatory Notes, 26.

[49] *Wu Kit Ping v Administrative Appeals Board* [2007] 4 HKLRD 849, [32].

[50] HKU Privacy Awareness Survey (n 3 above).

[51] Roderick B Woo, "Challenges Posed by Biometric Technology on Data Privacy Protection and the Way Forward" (undated), available at http://www.pcpd.org.hk/tc_chi/files/infocentre/speech_20100104.pdf.

the lifetime of the project to ensure continuous compliance with the data protection principles".[52]

Separately, under Data Protection Principle 3, personal data cannot, without consent, be used for any purpose other than identified at the time of collection or directly related thereto.

h. Managing Retention and Purging of Data

Under Data Protection Principle 2(2), "[p]ersonal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are or are to be used". The Commissioner urges that "[i]t would be a good practice for an employer to specify the retention periods of monitoring records, taking into account the nature of the information and the purpose for which the personal data were collected".[53] "Generally retention periods of not more than six months are preferred".[54] As the sensitivity of personal data increases with technological advances, it may become increasingly important to purge data more aggressively.[55]

Under s 26 of the Ordinance, however, data cannot be erased if it is otherwise prohibited by other laws, or if it is not in the "public interest" to do so.

i. Do Other Laws Preclude the Collection or Use of the Subject Data?

Various laws may have bearing on the collection and use of personal data.[56] Anti-discrimination legislation is a prime example relevant to employment. As set forth in the HRM Code:

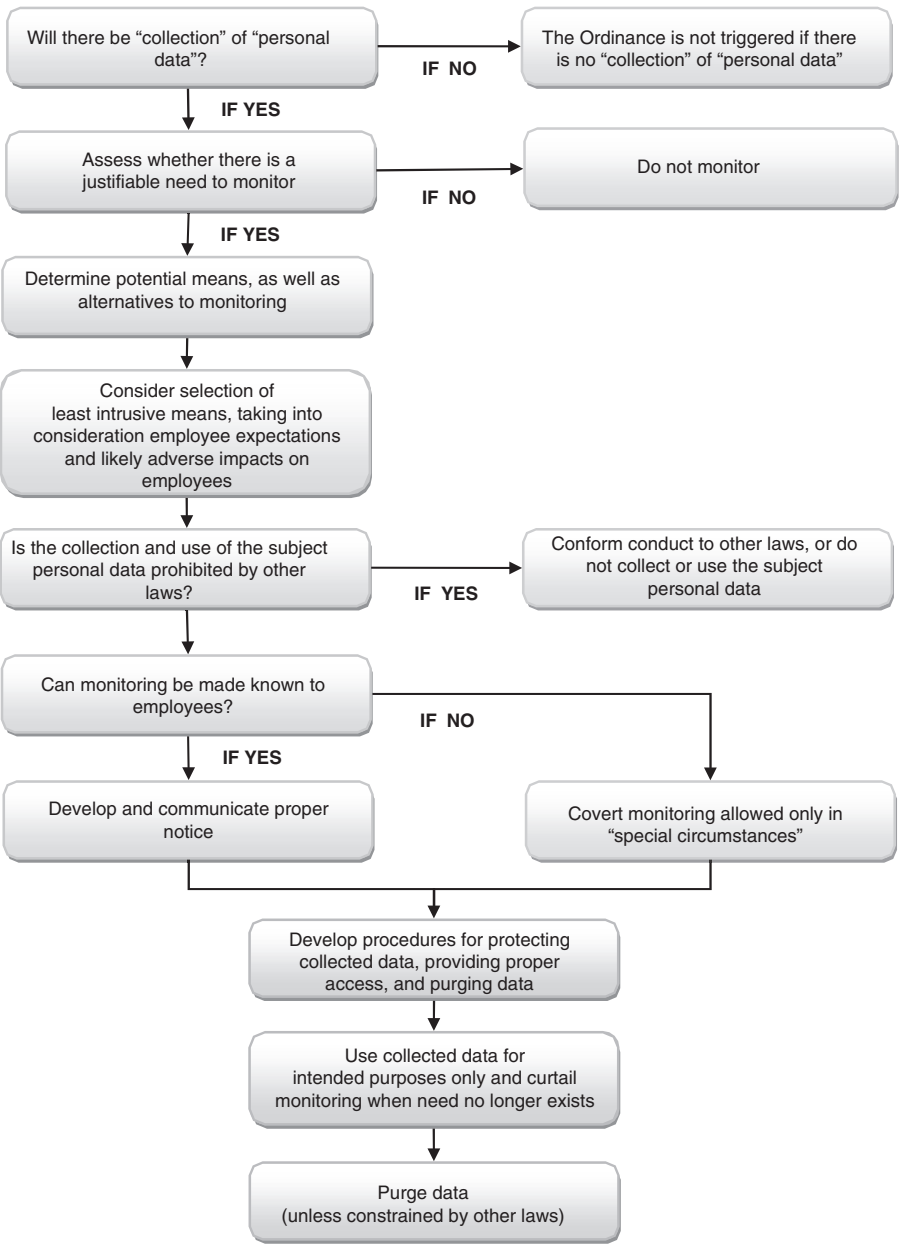
> "An employer should not... solicit the submission of personal data by candidates for the purposes of unlawfully discriminating against them on grounds of gender or marital status with the intention of excluding female employees from supervisory positions".[57]

This issue could arise as a result of screening or background checks during recruitment. For example, if an inspection of social media reveals that a candidate has a disability and that disability is used wrongly by the

[52] A Chiang, Keynote Speech on *Information Highway* (n 30 above).
[53] Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), para 3.4.3.
[54] *Ibid.*,para 3.4.4.
[55] Roderick B Woo, "Challenges Posed by Biometric Technology" (n 51 above). *See* also, for example, Federal Trade Commission, Staff Report on *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies* (October 2012) 11–12, available at http://www.ftc.gov/os/2012/10/121022 facialtechrpt.pdf.
[56] HRM Code, para 2.2.1 (n 9 above).
[57] *Ibid.*

employer as the basis for rejecting that candidate, the use of the personal data would be illegal under the Disability Ordinance. This issue is more fully discussed in the upcoming section entitled "Internet Including Social Media" in this article.

Based on the above-referenced materials, the author has developed the following flowchart. Since the flowchart incorporates materials apart from or beyond the exact provisions of the Ordinance, such as the



Commissioner's Monitoring Guidelines, this flowchart should be viewed only as one possible construct to use in developing a monitoring plan compliant with the Data Protection Principles.

4. Regulatory Guidance as to Specific Means of Monitoring

Employers can monitor electronic communications, telephone conversations, and conduct other forms of surveillance, such as video monitoring, if done in appropriate ways.

a. Electronic Communications

"The contents of e-mail sent using communications equipment supplied by the employer may be monitored for the purpose of ensuring the integrity and security of confidential business information, e.g., to prevent insider trading or the leakage of company trade secrets".[58] The Commissioner believes, however, that access to and viewing of the contents of e-mails should only take place where "exceptional" or "compelling" circumstances exist.[59]

> "Very often, the log record of E-mail communications would be sufficient if the monitoring serves to trace the time spent by employees on E-mail usage unless there are compelling circumstances that warrant access to the contents of E-mails, *e.g.*, when it is necessary to verify a possible violation of company rules on E-mail usage".[60]

The further development of software may enable organisations to monitor content without running afoul of privacy or data protection regulations. "Linguistic analysis software, which initially protects employee anonymity, can flag uncharacteristic changes in tone and language in electronic conversations, and can be tailored for particular types of employees, such as traders".[61]

The trend of employees eschewing employer-provided devices in favour of bringing their own devices to work, often referred to as "BYOD", adds further complications for information technology and human resource managers. Company data may be moved into the storage of personal devices. The organisation's perspective may be that wherever its data it

[58] *Ibid.*, p 10; *see* also HRM Code, para 2.3.2(d).
[59] Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), paras 2.3.2(d) and 3.2.2.
[60] *Ibid.*, paras 2.3.2(d).
[61] J Thompson, "Rogues Revealed By Bad Language", *Financial Times*, 7 January 2013, p 13.

located, it maintains ownership and in turn can exert its control, if it is able to do so. Some employees may have different views. With respect to the law, it is commonly required in many jurisdictions recognising "trade secrets" that the party asserting the existence and ownership of a trade secret must have been diligent in taking steps to protect the subject secret. One should consider whether data moving to personal devices fulfils this obligation. It may depend on the policies the organisation puts in place and its efforts at regulating its employees. However, the likelihood that an employer is obtaining communications having nothing whatsoever to do with the organisation when monitoring across personal devices is greater, making issues over ownership and control more problematic. Further BYOD issues include under-licensing risks and an array of security issues, including protecting against the disclosure of personal data of third parties when, for example, a personal device used in connection with work is lost by the employee.

The Privacy Commissioner has not published guidance specific to BYOD issues.[62] For organisations, implementing BYOD specific policies may be useful in better establishing legal rights.

b. Telephone Monitoring

As noted above, recording of calls for the sole purpose of keeping customer transaction records is not considered to be collection of personal data.[63] Consistent with e-mails, the Commissioner recommends reviewing call lists as opposed to the content of the calls, whenever possible. The content can be monitored, for example, "to ensure the quality and consistency of telephone service to customers".[64]

c. Video Surveillance

As noted, the recording of images of the public coming to a premise generally will not amount to the "collection" of "personal data". However, when video surveillance is used to compile information about identifiable

[62] In 2013, the UK's Information Commissioner's Office published "Bring Your Own Device (BYOD)" guidance, which may be useful for Hong Kong employers as a way of potentially anticipating regulatory reactions in Hong Kong, available at http://www.ico.gov.uk.

[63] *See* also Office of the Privacy Commissioner for Personal Data, "Whether Recording of Telephone Conversations Between Customers and Staff is in Breach of the Personal Data (Privacy) Ordinance", Case No. 2008103, available at http://www.pcpd.org.hk/english/casenotes/case_complaint2.php?id=13&casetype=B&cid=29.

[64] *Ibid.*, paras 2.2.4(a), 3.2.2(c) and 3.3.3(b).

employees, the requirements of the Ordinance will be triggered.[65] If data collected originally in a manner that does not constitute the collection of personal data is subsequently used to identify particular individuals, it may become "collection" of "personal data", thereby triggering the requirements of the Ordinance.

Several cases have come before the Privacy Commissioner regarding hidden cameras used to gain evidence to combat theft or employees taking excessive time away from their duties.[66] According to the Commissioner, "[a]s a general rule, employee monitoring should be conducted in an overt manner. Owing to its highly intrusive nature, covert monitoring should not be adopted unless it is justified by the existence of relevant special circumstances".[67] By way of example, the Commissioner has ruled that the use of pinhole cameras by the Hongkong Post Office, installed near toilets and changing rooms, violated the Ordinance. Hongkong Post's response was that the pinhole cameras were installed for the purpose of detecting crime due to a series of thefts. Notwithstanding this legitimate purpose, the evidence available did not show the existence of a risk of loss to be sufficient to justify the scale and methods used to monitor. As such, the extent of the monitoring activity was held to be out of proportion to the purpose. Further troubling the Commissioner was that there also was no evidence showing that Hongkong Post had given due consideration to the use of other less privacy intrusive alternatives or that the use of overt means would necessarily frustrate the purpose of collection.

In short, according to the Commissioner, covert monitoring should not be used unless justified as a measure of last resort and is absolutely necessary in detecting or gathering evidence of unlawful activities, and even then the monitoring should be limited in scope and duration.[68]

[65] Office of Privacy Commissioner for Personal Data, "Hong Yip Report" (n 14 above), paras 17–20 (discussing also *Eastweek Publisher Ltd v Privacy Commissioner for Personal Data* [2000] 2 HKLRD 83).

[66] The Commissioner has recognised that CCTV monitoring can be used to protect the health and safety of employees. *See* Office of Privacy Commissioner for Personal Data "Monitoring Guidelines" (n 10 above), para 2.2.4(3). The Commissioner has published guidance specific to internal household monitoring of domestic helpers. Video surveillance has been justified in other jurisdictions as a means to identify potential workplace risks, decrease false injury claims, and curtail drug or alcohol abuse on the job. As an example, *see Napreljac v Hammons Hotels Inc.*, 505 F3d 800 (8th Cir., 10 October 2007).

[67] Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), para 2.3.3.

[68] *See* Office of Privacy Commissioner for Personal Data, "Hongkong Post Report" (n 33 above).

This approach was again applied in the Hong Yip investigation. This enforcement action is noteworthy because it deals with employees tasked with providing security at a residential property. Hong Yip Service Company installed pin hole cameras near the entrance of a changing room, capturing images of two security guards vanishing into the changing room, sometimes for over an hour. They were summarily dismissed. They complained to the Privacy Commissioner that their images were recorded without their knowledge, in violation of the Ordinance. The Commissioner agreed, finding that Hong Yip violated the Ordinance because Hong Yip did not inform its employees of the possibility of such monitoring. Additionally,

> "[i]n the circumstances of the case, Hong Yip could have chosen less privacy intrusive alternatives to monitor the Complainants, e.g., by conducting a surprise check. If Hong Yip considered it was necessary to use monitoring devices, it should be confined to overt monitoring devices because overt monitoring could equally achieve the result of preventing employee misconduct".[69]

If video surveillance is undertaken, the Privacy Commissioner advises the following as to notice:

> "Employers who use video recording equipment to monitor the activities and behaviours of employees at work are recommended to include in the Employee Monitoring Policy information relating to the operation of the equipment.... Where, for example, the purpose is to collect evidence of wrongdoing based on reasonable suspicion, an employer may take into consideration whether disclosure would prejudice such purpose of collection".[70]

d. Internet Including Social Media

In Hong Kong, as elsewhere, researching the Internet, including social media and microblogs, has become an important and widespread practice of employers, especially in recruiting. In a 2011 survey conducted in Hong Kong by the international recruiting firm, Robert Half, "71% of hiring managers admit they check potential candidates' Facebook profiles before offering them a job".[71] The use of social media research as well as

[69] Office of Privacy Commissioner for Personal Data, "Hong Yip Report" (n 14 above), para 33.
[70] Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), para 3.2.3.
[71] Robert Half International, Use of Facebook May Affect Career Prospects (30 May 2011), available at http://www.roberthalf.com.hk/id/PR-03128/facebook-use-may-affect-career-prospects.

other ways of researching behaviors outside of the workplace are likely to grow in importance.[72]

In other jurisdictions, like the United States of America, a debate is raging over whether employers should be restricted from using social media research in connection with recruitment and subsequent evaluation of their employees, resulting in legislation in some jurisdictions imposing restrictions.[73] Differing views likewise exist in Hong Kong. In 2012, the employment agency Kelly Services conducted a survey in Hong Kong in which 65 per cent of the respondents stated that their current employer had no right to view their social media pages, and 65 per cent said that neither do prospective employers have the right to view their social media pages.[74]

While there is no regulatory guidance expressly referencing social media in the HRM Code or the Monitoring Guidelines, the Privacy Commissioner has stated that employers "[m]ay collect supplementary information about potential candidates that are relevant to the nature of the job, e.g. to establish security credentials or integrity".[75] The types of data that may be collected, "include work experience, job skills, competencies, academic/professional qualifications, good character and other attributes required for the job".[76] This appears to give employers a wide ambit to research prospective candidates. However, it should be kept in mind that employers are advised by the Privacy Commissioner to ensure that data collected in the recruitment process is adequate but not excessive in relation to the purpose of the recruitment.[77] In an example

[72] For examples of recent studies and events indicating the potential relevance of conduct outside of the workplace to the workplace, including use of social media, *see* RL Hotz, "When Facebook 'Likes' Can Shed Light", *The Wall Street Journal*, Asia Edition, 13 March 2013, p 18 ("Patterns of 'Likes' posted by people on Facebook can unintentionally expose their political and religious views, drug use, divorce and sexual orientation, researches [at Cambridge University] said Monday."); R Davidson, A Dey and A Smith, "Executives' 'Off-The-Job' Behavior, Corporate Culture, and Financial Reporting Risk," Introduction (The University of Chicago, Booth School of Business' Fama-Miller Center for Research in Finance, forthcoming in the Journal of Financial Economics). (The authors "examine how and why two aspects [of] CEO behavior outside the workplace, as measured by prior legal infractions and ownership of luxury goods, are related to the likelihood of misstated financial statements."); S Taulas and D Carvajal, "Train Operator Bragged About Speed", *New York Times*, Global Edition,27 July 2013, p 5 ("Online [Facebook] boasts and jokes preceded horrific crash that killed 78 in Spain.")

[73] *See*, for example, C Bost Seaton, "Social Media Password Ownership and the Workplace", *Law 360,* 5 December 2012, available at http://www.law360.com/articles/397581.

[74] Kelly Services, When Two Worlds Collide – The Rise of Social Media in the Workplace (2012).

[75] R Lee, Office of the Privacy Commissioner for Personal Data, "Protection of Employees' Personal Data – Code of Practice on Human Resource Management" (Presentation given at the Hong Kong Institute of Human Resource Management's Annual Conference, 10 December 2010).

[76] HRM Code, para 2.2.2 (n 9 above).

[77] *Ibid.*

from the HRM Code concerning the vetting of the credentials of security guards during the selection process, it is stated that "recording the details of a candidate's outside activities and interests might be excessive unless the employer can demonstrate that such detail is relevant to the inherent requirements of the job".[78]

Following recruitment, the use of social media by employees, whether purposefully to promote the business as well as their "personal brand" to develop business, or inadvertently disclosing confidential information about the business, may be a concern for many organisations, necessitating some form of monitoring. Issues of privacy, ownership and practicality arise. Apart from needing to guard against the loss of confidences, employers may wish to make certain that the ownership of business contacts and information relevant to the organisation, which has been obtained via use of social media, resides fully in the organisation. To this end, some organisations may wish to limit use of social media in connection with the affairs of the organisation, unless the service, be it, for example, a Weibo or Twitter, LinkedIn, Facebook or RenRen, Whatsapp or a WeChat account, has been set up by the organisation or otherwise made subject to employer access, such as by disclosure of passwords, if permissible. Employer-created accounts are one way of making organisational ownership and control more certain. Some employers also are developing policies specific to the use of cloud storage services, such as Dropbox and its progeny, due to concerns over information being moved outside of the organisation's systems. Other employers rely on existing duties at law in their jurisdictions.

As to monitoring employee use of the Internet, the regulatory guidance from the Privacy Commissioner presently is limited to the following: "The amount of time spent on web-browsing activities by employees may be monitored to prevent company resources from being substantially used for private purposes…".[79] To prevent access to websites containing unacceptable content, the Commissioner suggests use of filter software instead of logging all websites visited by employees.[80] Monitoring is appropriate to prevent vicarious liability. For example, "[t]he logging of websites visited by employees may be designed to detect activities that are prohibited when assessing the Internet such as downloading copyright protected materials without the licence of the copyright owner".[81]

[78] *Ibid.*, para 2.7.1.
[79] Office of Privacy Commissioner for Personal Data, "Monitoring Guidelines" (n 10 above), para 2.2.4(a).
[80] *Ibid.*, para 2.3.1(b).
[81] *Ibid.*, para 2.2.4(c).

e. Emerging Technologies

It often has been stated by various Privacy Commissioners that the Ordinance is "technology neutral", meaning that no particular technology to date has been found to be *per se* violative of the Ordinance if deployed. Instead, it is the "choices made in their design and use" that are regulated.[82] Also, there is no defined category of sensitive personal data under the Ordinance. However, the Commissioner has from time to time categorised certain personal data, such as fingerprints, as sensitive personal data, necessitating a higher level of care according to the Commissioner.

The use of biometric technologies for identification and security purposes in the workplace is increasingly popular in Hong Kong. Biometric technologies include methods for recognising the physical characteristics of a person's face, fingerprints, iris, DNA, voiceprint or body movements. The Privacy Commissioner has noted "a sharp rise in complaints" lodged with the office, especially concerning the use of fingerprints for attendance purposes.[83]

The Privacy Commissioner has stated that "[d]espite the advantages of using biometric data, from the perspective of data protection, it is advisable for data users to resort to less privacy intrusive but equally effective alternatives".[84] To the extent biometric systems are going to be deployed, the Commissioner advises that "extra care and caution" should be given.[85] To this end, the Commissioner urges that alternative options be provided for those unwilling to supply such data, and if willing, then the organisation should ensure that it has obtained informed "genuine" consent.[86] The Guidance on Fingerprint Data cautions against "the gravity of harm that may be caused to individuals if such data are handled improperly".[87] The Guidance on Fingerprint Data provides that "[a] data user should as far as practicable resort to other less privacy intrusive alternatives for fulfilling the purpose of fingerprint data collection".[88] "Data users who wish to collect employees' fingerprint data must ensure that their employees are given a free and informed choice whether to

[82] A Chiang, Keynote Speech on *Information Highway* (n 30 above), pp 10–11.

[83] Roderick B Woo, "Challenges Posed by Biometric Technology" (n 51 above), paras 5–6. *See*, for example, "Property Management Employees Object to Fingerprint Collection", *Apple Daily*, 20 December 2012, p A24 (reporting on the complaints made to the Hong Kong Buildings Management and Security Workers General Union from security guards of The Link REIT, which had requested their fingerprints for a new security system).

[84] Office of Privacy Commissioner for Personal Data, "Privacy Commissioner's Perspective" (n 29 above), para 5.46.

[85] *Ibid.*

[86] *Ibid.*

[87] Commissioner for Personal Data, "Guidance on Fingerprint Data" (n 19 above), p 1.

[88] *Ibid.*, p 2.

supply the data" and "employees who are unwilling or unable to supply their fingerprint data should not be penalised".[89]

In an investigation conducted by the Privacy Commissioner concerning the collection of fingerprint data, the Commissioner found the Ordinance to have been violated by the employer.[90] This investigation was triggered by the complaint of a former employee who had the position of furniture installer. During the interview process and when he accepted the employment offer, he was not informed that he would be required on his first day of work to give his fingerprint image. The purpose was for recording attendance, and not for any other reason. The fingerprint images of over 400 staff had been collected and maintained by the employer, until deleted upon cessation of employment. The Privacy Commissioner found as follows:

> "[T]he adverse impact on personal data privacy exceeds the benefits which were allegedly brought by the System. For the purpose of recording attendance, the collection of staff's fingerprint data by the Company was unnecessary and excessive, and the Company had contravened DPP1(1)".[91]

Leading up to the 2012 amendments to the Data Protection (Privacy) Ordinance, the former Commissioner, Roderick B Woo, had urged the Chief Executive and Legislative Council to adopt rules specific to biometric data. He had noted that there was a noticeable trend in complaints to his office over the required collection of fingerprints by employers in Hong Kong. The business community, however, resisted the adoption of rules specific to biometric data. The Personal Data (Privacy) Amendment Ordinance, enacted in June 2012, does not contain more stringent requirements for biometric data.

5. Conclusion

Monitoring plans increasingly must finely balance competing considerations. This often requires careful consideration in their development and robust on-going compliance upon implementation. To do so, organisations must commit more resources in a more coordinated fashion across the organisation. This paper has attempted to provide guidance as to the development and implementation of a monitoring plan under the requirements of Hong Kong's Personal Data (Privacy) Ordinance.

[89] *Ibid.*, p 4.
[90] *See* Office of the Privacy Commissioner for Personal Data, Report on the *Employer Collecting Employees' Fingerprint Data* (n 41 above).
[91] *Ibid.*, para 17.