DATA PROTECTION IMPLICATIONS OF MODERN EMPLOYEE MONITORING SOFTWARE

A wide array of employee monitoring software products has emerged on the market. Employee monitoring software may enable employers to manage their employees more efficiently, and to protect their organisational and business interests more effectively. However, the use of employee monitoring software presents novel data protection issues, which must be addressed in order to secure employees' right to data protection, and avoid breaches of data protection law by employers. This article examines the capabilities of modern employee monitoring software available on the market, and highlights the various data protection issues that may arise from the use of such software. It will also discuss the use of employee monitoring software from a broader policy perspective.

Benjamin **WONG**[1]
LLB (Hons) (National University of Singapore),
LLM (London School of Economics);
Advocate and Solicitor (Singapore);
Sheridan Fellow, Faculty of Law, National University of Singapore.

I. Introduction

1 Employee monitoring has been a common feature of most workplaces for a long time. The closed-circuit television ("CCTV") camera is perhaps the best known "traditional" technology used by employers to monitor their employees. CCTV cameras, and other technologies such as "clocking in" or card attendance systems, rely on specialised hardware. Today, however, software solutions in the form of employee monitoring software have entered the market, and are now widely available to employers. Employee monitoring software represents a new way by which employers can undertake surveillance over their employees.

1 The author would like to thank Ong Yuan Zheng Lenon and Tan Yung Kiang Zachary for their valuable research assistance, and Daniel Seng for his helpful comments on an earlier draft. The author would also like to gratefully acknowledge the financial support generously granted by the National University of Singapore's Centre for Technology, Robotics, Artificial Intelligence & the Law. All errors are the author's own.

2 Employee monitoring software may be deployed for a wide range of purposes.[2] Employee monitoring software may be used for the purposes of data security, by preventing employees from engaging in activities that inadvertently introduce vulnerabilities to external threats, as well as by preventing deliberate malicious conduct by employees.[3] Employee monitoring software may also be used to optimise employee productivity, by tracking what employees do throughout the course of the workday, enabling intervention by employers to discourage unproductive uses of workplace time and material, to encourage productive work practices, and to organise workplaces to facilitate higher employee performance.[4] In essence, employee monitoring software aids the achievement of these and other purposes by allowing employers to know more about their employees, gaining insight into their behaviour and motivations. An additional possible advantage of using employee monitoring software is that it facilitates the gathering of evidence of employee misconduct, and such evidence may be useful in the event of litigation.

3 Whilst the benefits of using employee monitoring software are no doubt numerous, the use of this software brings into conflict two competing sets of interests: the interests of employers in managing their workplaces and workforces, and the privacy interests of employees. The use of employee monitoring software by employers almost inevitably attracts the application of data protection law. The primary objective of this article is to explore the application of Singapore data protection law to the use of employee monitoring software. It will study the existing employee monitoring software on the market, to identify their data collection capabilities. It will then look to the potential data protection implications that arise out of the collection (and subsequent use and disclosure) of personal data collected by the employee monitoring software.

---

2 For a more extensive list of the reasons for the electronic monitoring of employees in the workplace, see Gail Lasprogata, Nancy J King & Sukanya Pillay, "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada" [2004] *Stanford Technology Law Review* 4 at 2–3.

3 The Cerebral product from Veriato, for example, claims to be "an AI-powered security platform that integrates User & Entity Behavior Analytics (UEBA) with User Activity Monitoring (UAM), allowing rapid Data Breach Response (DBR)", enabling employers to proactively recognise signs of risk of insider threats, such as "changes in an employee's attitude and behavioral patterns": see Veriato, "Cerebral: AI-Driven Insider Threat Detection" <https://www.veriato.com/products/veriato-cerebral-insider-threat-detection-software> (accessed 19 January 2020).

4 For example, the firm VoloMetrix was reported to have analysed "employee emails and calendars to determine how they are spending their time": see Alexandra Bosanac, "How 'People Analytics' Is Transforming Human Resources" *Canadian Business* (26 October 2015).

4 The issue of employee surveillance through monitoring software is particularly salient in view of the present COVID-19 pandemic situation. The Singapore government has instituted a lockdown which has required a majority of the employed Singapore population to work from home. At the time of writing, the lockdown remains in effect, and even after the lockdown is lifted it may well be the case that it will have to be re-instituted in the event of a future outbreak. With more employees working remotely as a consequence of the lockdown, concerns have been raised about employers using employee monitoring software to keep track of their employees.[5]

II. Employees as a special class of data subject

5 To preface the discussion, it will be useful to provide some context about employee data protection.

6 Data protection law generally recognises that employees form a special class of individuals (or "data subjects", to use the European parlance). Under the European Union ("EU") General Data Protection Regulation[6] ("GDPR"), for example, Art 88 confers upon EU Member States the freedom to create rules to govern employee personal data:

> Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.
>
> Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

5 See Drew Harwell, "Managers Turn to Surveillance Software, Always-on Webcams to Ensure Employees Are (Really) Working from Home" *The Washington Post* (30 April 2020); Adam Satarino, "How My Boss Monitors Me While I Work from Home" *The New York Times* (6 May 2020).

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

7 Similarly, as will be discussed below, employee personal data receives special treatment under Singapore data protection law. There are several possible reasons why employee personal data is, and should be, treated differently.

8 One possible reason to afford special treatment to employee personal data lies in the nature of the employer-employee relationship. As Collins explains, there are a number of "distinctive features of the employment relation that render it unlike other market transactions".[7] In particular:[8]

> [T]he opportunity to work in return for a wage has greater significance for the employee than their other market transactions. Most people rely upon employment as their principle source of income. Pay serves as the major mechanism for the distribution of wealth in a market society. Work has to produce enough income to support an employee and his or her dependants, not only on a daily basis, but also for a lifetime. Beyond determining their material standard of living, work also provides people with a principle source of meaning in their lives. Through their work people seek personal fulfilment, and through participation in a workplace they obtain entry into a social community. Work can be exhausting, boring, and dangerous, but without it many people become socially excluded and lose any sense of personal worth.

These features tend to place employees in a position of subordination or dependence *vis-à-vis* their employers. As a consequence, not all of the standard mechanisms of data protection law provide effective protection to employees. In particular, the consent mechanism may offer limited protection, since employees may in practice feel compelled to give consent to their employers in spite of their personal misgivings about the practices to which they are giving consent.[9]

9 A second possible reason for treating employee personal data specially under data protection law is that the proper functioning of the employer-employee relationship often depends quite heavily on the employer's processing of employees' personal data. In the course of hiring, managing and terminating employees, an employer needs to collect, use and disclose a broad range of personal data about those employees, including for example their names, educational qualifications and prior work experience.[10] Employers may often also need to process

7 Hugh Collins, *Employment Law* (Oxford University Press, 2nd Ed, 2010) at p 3.
8 Hugh Collins, *Employment Law* (Oxford University Press, 2nd Ed, 2010) at pp 3–4.
9 Article 29 Data Protection Working Party, *Opinion 2/2017 on Data Processing at Work* (WP 249, adopted 8 June 2017) at p 23.
10 For common justifications for electronic monitoring by employers, see Kathy Eivazi, "Computer Use Monitoring and Privacy at Work" (2011) 27 *Computer Law & Security Review* 516 at 517–521.

more sensitive personal data about employees, such as information about their criminal background (if any) – such information is typically not required for ordinary transactions. The common need of employers to collect, use and disclose employee personal data must be accommodated by data protection law. This does not necessarily imply the watering down of data protection law in the employment context – rather, what is necessary is for the application of data protection rules to take into account the particular legitimate needs of employers.

10 Relatedly, a third possible reason for treating employee personal data differently is that employers frequently possess large amounts of personal data about their employees, some of which disclosing fairly intimate details about those employees. Much of this information is, of course, voluntarily provided by the employee before the commencement of the employment relationship – at the time when the employee applies for a position with the employer. Subsequently, throughout the course of the employment relationship, the employer has ample opportunity to further gather employee personal data, both by voluntary and involuntary means. One of those means, which this article will now proceed to discuss, is by the use of employee monitoring software.

III. Operation of employee monitoring software

11 In order to gather information about the operation of modern employee monitoring software and their data collection capabilities, a number of different employee monitoring software service providers were studied. These include: ActivTrak, ContentWatch, DeskTime, Ekran System, EmailAnalytics, Hubstaff, iMonitorSoft, InterGuard, Kickidler, SentryPC, SoftActivity, StaffCop, Teramind, Time Doctor, Track.ly, Veriato, VeriClock, Work Examiner and Workpuls.

12 This article proceeds to first discuss the mode of operation of these employee monitoring software, in general terms, before laying out the data collection capabilities of the employee monitoring software.

A. Mode of operation

13 In relation to how employee monitoring software generally operate, two commonalities among the employee monitoring software studied may be identified: first, most employee monitoring software operate in *stealth*, either exclusively or by default. Most employee monitoring software, when deployed by an employer, generally do not

disclose to the monitored employee that he is in fact being monitored.[11] This means that employees may have their personal data collected by employee monitoring software surreptitiously. However, some employee monitoring software do provide the flexibility of running in a more transparent fashion, allowing employees to know when they are being monitored.

14 Second, various employee monitoring software provide cloud-based services. This means that the data collected from employees' workstations or mobile devices is transmitted to the service providers' server for processing and storage. The consequence of the cloud-based operation of employee monitoring software is that the employees' personal data collected by the employee monitoring software will necessarily be disclosed to a third party (namely, the service provider) whose server may be located outside of Singapore; this gives rise to a number of data protection implications which will be discussed later in this article. That said, some service providers, such as Veriato and Teramind, offer on-premise employee monitoring software, which makes it possible for personal data collected by the employee monitoring software to stay within Singapore.[12]

B. Data collection capabilities

15 All employee monitoring software come with one or more data collection functions. These functions enable the gathering of data, which may include personal data, from employees. It should go without saying that the various employee monitoring software available on the market boast varying sets of capabilities. Some products, especially those that are free for use, are basic; other products are more sophisticated. It should be noted that the functions that will be described below are collated from across all the above-mentioned employee monitoring software; these functions are not universally offered by all employee monitoring software.

11 Indeed, this is often presented by service providers as a feature of their employee monitoring software. To give just two examples, SoftActivity claimed to "work invisibly for monitored users": see SoftActivity website <https://www.softactivity.com/get/activity-monitor> (accessed 19 January 2020), while ActivTrak similarly claims that its software "collects data and executes responses to user activity while running unnoticed in the background of tracked computers": see ActivTrak website <https://activtrak.com/product/how-does-it-work> (accessed 19 January 2020).

12 See, *eg*, Teramind, "On-Premise Deployment" <https://www.teramind.co/product/deployment/on-premise> (accessed 14 June 2020).

(1) Location tracking

16 Some employee monitoring software grant employers the ability to track their employees' location using their employees' mobile devices. Employee monitoring software can exploit the Global Positioning System ("GPS") capabilities of employees' smartphones to track their locations. Hubstaff, for example, offers a GPS tracking service, which allows the employer to automatically track the time at which an employee enters and leaves a particular location (such as an office building or a worksite), using geofencing (that is, setting up a virtual perimeter that triggers a response whenever a tracked device crosses that perimeter), allowing the employer to easily "keep track of employee time on the road or on site in real-time".[13] Time Doctor appears to provide a mobile application, installable on employees' mobile devices, to track employees' locations.[14]

(2) Time tracking

17 Most employee monitoring software can track and verify the number of hours worked by employees – this particular function is the focus of some employee monitoring software. Workpuls, for example, automatically tracks when employees clock in and clock out, by reference to the employees' computer activity.[15] VeriClock, on the other hand, appears to rely on manual time tracking, providing multiple avenues by which employees can clock in and out, such as via a mobile application, website or text messaging.[16]

(3) Website and application tracking

18 Most of the employee monitoring software examined in this study offer some form of website and application tracking. For example, one of the features boasted by ActivTrak is its "Live User Activity Data Report", which allows the employer to view, in real time, the computer activities of employees tracked by ActivTrak, including what applications they use and the websites they visit.[17] Work Examiner, a relatively comprehensive employee monitoring software, promises that it "not only collects data about the website address and the date of access, but it also calculates the

13 See Hubstaff, "GPS Tracking" <https://hubstaff.com/features/gps_time_tracking> (accessed 3 February 2020).

14 See Time Doctor, "Features" <https://www.timedoctor.com/#features> (accessed 3 February 2020).

15 See Workpuls, "Employee Monitoring Software" <https://www.workpuls.com/employee-monitoring> (accessed 3 February 2020).

16 See VeriClock website <https://www.vericlock.com>.

17 See ActivTrak, "Real-time User Activity Monitoring" <https://activtrak.com/product/real-time-monitoring> (accessed 3 February 2020).

amount of time that the user spent on the site (including active and idle time)", and it tracks online search requests as well as file downloads.[18]

(4) Communications monitoring

19 Communications monitoring functions are a common feature of employee monitoring software. These include the monitoring of e-mail and instant messaging. E-mail monitoring is perhaps the most common form of communications monitoring. Work Examiner, for example, claims to "capture and save every email message sent or received" via various e-mail services such as Gmail and Outlook, capturing all e-mail information (such as the timestamp, recipient and subject line).[19] EmailAnalytics provides metrics on e-mail account usage (such as the average time taken to respond to an incoming e-mail).[20] Instant messaging monitoring is also frequently offered by employee monitoring software. Work Examiner records instant messages sent through "the most popular [instant messaging] services and protocols", including Facebook, Skype and Google Talk.[21]

(5) Screen capture and webcam capture

20 Some employee monitoring software provide the employer with the ability to view employees' computer screens – this ranges from the taking of static screenshots to the capturing of live feeds from employees' computer screens. For example, InterGuard offers employers three types of screenshot systems: "Alert Word Screenshots" will trigger the capturing of a screenshot upon the typing or viewing of a particular keyword; "Continuous Screenshots" will take screenshots of employees' computer screens at defined intervals; "Smart Camera Screenshots" will take screenshots of selected websites and programs.[22] ActivTrak permits an employer to see what his employees are seeing on their screens in real time, by transmitting screenshots of the employees' screens at five-second intervals.[23] Service providers like Kickidler go further, offering real-

18 See Work Examiner, "Features" <https://www.workexaminer.com/features> (accessed 3 February 2020).
19 See Work Examiner, "Features" <https://www.workexaminer.com/features> (accessed 3 February 2020).
20 See EmailAnalytics website <https://emailanalytics.com>.
21 See Work Examiner, "Features" <https://www.workexaminer.com/features> (accessed 3 February 2020).
22 See InterGuard, "Video Playback and Screenshot Capture" <https://www.interguardsoftware.com/employee-monitoring-screenshots> (accessed 3 February 2020).
23 See ActivTrak, "Real-time User Activity Monitoring" <https://activtrak.com/product/real-time-monitoring> (accessed 3 February 2020).

time video capture of employees' computer screens.[24] Other employee monitoring software allow employers to use webcams in order to monitor their employees. For example, Time Doctor can activate employee-facing webcams to present to the employer "regular camera shots of employees when working".[25]

(6) Keylogging

21 Keystroke logging or "keylogging" is another function offered by several employee monitoring software. This involves the recording of keystrokes made by employees on their computers. Ekran System's keylogging software records actual keystrokes, along with copy, cut and paste operations; particular keywords can be designated to trigger the recording of keystrokes.[26] Teramind's keylogging solution appears to function similarly, albeit with the ability to create "anti-logging rules" to avoid recording keystrokes under certain circumstances, such as where the employee concerned was typing his credit card details.[27]

(7) Remote control

22 Certain employee monitoring software, such as Kickidler's, permit direct intervention by employers, by giving them the ability to control their employees' computers remotely.[28] Remote control is a means by which employers can step in to prevent or halt harmful conduct, but it is also a way for an employer to extract an employee's personal data from his computer.

IV. Application of data protection obligations to employee monitoring software

23 The capabilities of modern employee monitoring software give rise to a number of data protection concerns. These concerns arise mainly because employee monitoring software can enhance an employer's ability to engage in surveillance over his employees, by increasing both the breadth and depth of surveillance. The breadth of surveillance is increased

24 See Kickidler, "Online Screen Monitoring" <https://www.kickidler.com/online-monitoring.html> (accessed 3 February 2020).

25 See Time Doctor, "Features" <https://www.timedoctor.com/#features> (accessed 3 February 2020).

26 See Ekran System, "Employee Keylogger Software" <https://www.ekransystem.com/en/product/employee-keylogging> (accessed 3 February 2020).

27 See Teramind, "Keystroke Monitoring" <https://www.teramind.co/features/keystroke-recorder-logger> (accessed 3 February 2020).

28 See Kickidler, "Remote Access" <https://www.kickidler.com/remote-access.html> (accessed 3 February 2020).

because employee monitoring software grants an employer access to a wider range of sources from which an employee's personal data can be extracted. For example, employee monitoring software can collect an employee's personal data from his e-mail account and his mobile devices. Employees may not expect that their personal data be exposed through those new sources, and their reasonable expectations of privacy may be defeated, especially if the employee monitoring software is deployed and operated in a surreptitious manner. The depth of surveillance is also increased by employee monitoring software, as intimate details about employees may be deliberately or inadvertently captured in the course of the operation of these software. For example, employee monitoring software can collect the Internet browsing history[29] and location data[30] of an employee, which can reveal highly private information about that employee to his employer.

24 If data protection concerns are not adequately addressed, this may result in the loss of trust in organisations that process personal data – in this instance, the loss of trust by employees in the processing of personal data by their employers. The Singapore data protection regime, implemented primarily through the enactment of the Personal Data Protection Act 2012[31] ("PDPA"), was implemented as an attempt to maintain trust in the processing of personal data by organisations.[32] The paragraphs that follow provide some background on the PDPA.[33]

25 The PDPA establishes a comprehensive data protection regime in Singapore, setting a baseline level of data protection across all industry sectors. The PDPA imposes a number of data protection obligations on "organisations", defined broadly to include "any individual, company, association or body of persons, corporate or unincorporated".[34] The data protection obligations are imposed in respect of "personal data", which means "data, whether true or not, about an individual who can be identified" either "from that data" or "from that data and other information to which the organisation has or is likely to have access".[35] Enforcement of the PDPA is largely the responsibility of the Personal Data Protection Commission ("PDPC"), who may commence an investigation

29 See para 18 above.
30 See para 16 above.
31 Act 26 of 2012.
32 Benjamin Wong, "Data Privacy Law in Singapore: The Personal Data Protection Act 2012" (2017) 7 *International Data Privacy Law* 287 at 290; *Singapore Parliamentary Debates, Official Report* (15 October 2012) vol 89.
33 See generally Benjamin Wong, "Data Privacy Law in Singapore: The Personal Data Protection Act 2012" (2017) 7 *International Data Privacy Law* 287.
34 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).
35 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).

against an organisation (usually in response to a complaint against that organisation) to determine if it has breached any of the data protection obligations under the PDPA.[36] It is also possible for individuals to enforce the data protection obligations through private action.[37]

26 In the discussion that follows, this article will critically examine how the PDPA applies to the use of employee monitoring software. The focus will be on the data protection obligations, and how these obligations are engaged in the context of employee monitoring software. However, this article does not exhaustively address every data protection obligation that may conceivably apply.

A. Obligations relating to the collection, use and disclosure of personal data

(1) "Consent Obligation"

27 In general, an organisation is required to obtain consent from an individual before collecting, using or disclosing his or her personal data. This is pursuant to the "Consent Obligation" under the PDPA.[38] The Consent Obligation provides that an organisation shall not collect, use or disclose personal data about an individual unless the individual has given consent to the collection, use or disclosure.[39] If an employer deploys employee monitoring software that collects, uses or discloses an employee's personal data, the employer must generally get that employee's consent for that collection, use or disclosure. Consent may be withdrawn by the employee, by the giving of reasonable notice.[40]

28 There is, however, an important exception to the Consent Obligation that may be applicable in the context of the deployment of employee monitoring software. This is the so-called "employment relationship exception" in the PDPA. The employment relationship exception provides that an organisation may collect personal data about an individual without the consent of that individual if "the personal data is collected by the individual's employer and the collection is reasonable for the purpose of managing or terminating an employment relationship between the organisation and the individual".[41] Personal data collected

36 Personal Data Protection Act 2012 (Act 26 of 2012) s 50(1).
37 Personal Data Protection Act 2012 (Act 26 of 2012) s 32.
38 Personal Data Protection Act 2012 (Act 26 of 2012) s 13.
39 Personal Data Protection Act 2012 (Act 26 of 2012) s 13(*a*).
40 Personal Data Protection Act 2012 (Act 26 of 2012) s 16(1).
41 Personal Data Protection Act 2012 (Act 26 of 2012) s 17(1) and Second Schedule, para 1(*o*).

in accordance with the employment relationship exception may also be used and disclosed by the organisation, if it is used or disclosed by the organisation for purposes consistent with the purpose of the collection (that is, managing and terminating an employment relationship between the organisation and the individual).[42]

29 The employment relationship exception is likely to be the most applicable exception to the Consent Obligation, in a situation where an employer wishes to deploy employee monitoring software. The ordinary purpose of an employer's deployment of employee monitoring software is precisely to manage his employees and his employment relationships. Employee monitoring software may also be used for the purpose of terminating an employment relationship. For example, an employer could use employee monitoring software to gather evidence of misconduct by an errant employee to justify the dismissal of that employee. As such, the deployment of employee monitoring software by an employer will usually be for the purposes of managing and terminating an employment relationship.

30 It is, however, important to note that the employment relationship exception will not extend to the collection, use or disclosure of employees' personal data for extraneous or secondary purposes. For example, where an employer has collected substantial quantities of his employees' personal data via employee monitoring software, and wishes to repurpose that collection of personal data for the purposes of business development or operational improvements, such repurposed collection, use or disclosure of the employees' personal data will not be covered by the employment relationship exception. That employer would have to obtain the consent of his employees for the repurposing, or rely upon a different exception to the Consent Obligation.[43]

31 It is also worth highlighting that the employment relationship exception does not grant an employer a *carte blanche* to harvest employees' personal data via employee monitoring software, even if the employer's purpose in doing so is purely to manage his employees. This is because the employment relationship exception is circumscribed by a requirement of reasonableness: the collection of an employee's personal data by an employer must be *reasonable* for the purpose of managing and terminating an employment relationship between the employer

42 Personal Data Protection Act 2012 (Act 26 of 2012) s 17(2) and Third Schedule, para 1(*j*); Personal Data Protection Act 2012 (Act 26 of 2012) s 17(3) and Fourth Schedule, para 1(s).

43 See Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 9 October 2019) at para 5.22.

and the employee. What does reasonableness entail in this context? There does not appear to be substantial guidance with respect to how reasonableness is to be assessed. Presumably, reasonableness would relate to the quantum of personal data collected, such that the collection of an employee's personal data using employee monitoring software should not be excessive in relation to the management and termination of the employment relationship. For example, while an employer may use employee monitoring software to monitor how an employee uses company computer network resources,[44] it may be unreasonable for the employer to engage in a full-blown surveillance of that employee's Internet usage, and the employer may need to confine his monitoring to tracking specific metrics such as data usage.[45] Reasonableness may also relate to the nature of the personal data collected; it may not be reasonable for an employer to collect, without compelling reason, an employee's sensitive personal data, such as information about the employee's medical conditions.

32 Canadian data protection jurisprudence offers some valuable guidance in this regard, due to the close similarities between Canadian and Singaporean data protection law. In the recent decision of *Teck Coal Ltd*,[46] the British Columbia Office of the Information and Privacy Commissioner ("OIPC") had to assess whether the collection and use of recordings from video surveillance cameras was "reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual", pursuant to the equivalent employment relationship exception under the British Columbia Personal Information Protection Act.[47] There, the OIPC affirmed a non-exhaustive list of factors to be considered:[48]

> 1. sensitivity of the employee personal information (*i.e.*, health history or a medical condition is sensitive information, but an employee's name or home address is not);
>
> 2. amount of personal information (*i.e.*, Is the employer collecting, using or disclosing more information than is necessary to achieve its purpose(s)?);
>
> 3. likelihood of effectiveness (*i.e.*, Is there a reasonable likelihood that the collection, use or disclosure of personal information will fulfil the employer's objectives?);

44 See Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 9 October 2019) at para 5.21.

45 There may, admittedly, be exceptional circumstances under which full-blown surveillance could plausibly be regarded as reasonable, for example, where the employee regularly deals with confidential information or trade secrets.

46 Order P20-04 *Teck Coal Ltd* 2020 BCIPC 24.

47 Personal Information Protection Act (SBC 2003, c 63) ss 13 and 16.

48 Order P20-04 *Teck Coal Ltd* 2020 BCIPC 24 at [40].

4. manner of collection and use of the personal information (*i.e.*, Was the employee aware that the information was being collected, or was it covertly collected? In what circumstances and how often does the employer access the information?);

5. less privacy-intrusive alternatives (*i.e.*, Has the employer given reasonable consideration to other methods for achieving its objectives? This factor does not necessarily require the employer to implement the least privacy-intrusive alternative, but the employer must consider the balance between its interest and the right of individuals to protect their personal information); and

6. other relevant factors given the circumstances.

33 Apart from the employment relationship exception, another exception that may be relevant to the deployment of employee monitoring software is the "evaluative purpose exception". The PDPA provides that personal data may be collected, used and disclosed by an organisation, without the consent of the individual, where the collection, use or disclosure is "necessary for evaluative purposes".[49] "Evaluative purpose" means the "purpose of determining the suitability, eligibility or qualifications of the individual to whom the data relates", (a) for employment or for appointment to office; (b) for promotion or continuance in employment or office; and (c) for removal from employment or office, among other things. In the employment context, the evaluative purpose exception overlaps significantly with the employment relationship exception, and the latter largely subsumes the former since the evaluation of an employee is likely to fall within the concept of "managing and terminating an employment relationship".[50] The evaluative purpose exception may be relied upon by an employer using employee monitoring software, in the event that the personal data collected by the employee monitoring software is used to evaluate the work performance of an employee, in order to determine if the employee should be promoted, retained or terminated.

34 The upshot of this analysis is that the Consent Obligation is generally of limited relevance in the context of the deployment of employee monitoring software. The existence of the employment relationship exception and the evaluative purpose exception in the PDPA means that, in general, an employer who wishes to deploy employee monitoring

49 Personal Data Protection Act 2012 (Act 26 of 2012) Second Schedule, para 1(*f*); Third Schedule, para 1(*f*); and Fourth Schedule, para 1(*h*).

50 Note that an important difference between the two exceptions is that the evaluative purpose exception does not require the employer to provide notification to the employee, whereas notification is required if the employer is relying solely on the employment relationship exception: see paras 35–37 below; see also Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 9 October 2019) at para 5.24.

software will not need to obtain the consent of his employees before doing so. Furthermore, even if the employer has extraneous purposes for the personal data collected by the employee monitoring software, it is unlikely that most employees would put their livelihoods at risk by withholding their consent from the employer;[51] this makes it a "simple matter for a well-advised employer to obtain the necessary consent".[52]

(2) "Notification Obligation"

35 Before using employee monitoring software to collect, use or disclose an employee's personal data, the employer must provide the requisite notification in compliance with the "Notification Obligation" under the PDPA. The PDPA provides that an organisation must inform the individual of the purposes for which the organisation is collecting, using or disclosing the individual's personal data, on or before collecting the personal data.[53] Subsequently, if the organisation wishes to use or disclose the individual's personal data for any other purpose of which the individual has not been informed, such additional purposes must also be notified to the individual.[54] While the employer need not provide notification if he is collecting, using or disclosing the employee's personal data without the employee's consent pursuant to one of the exceptional grounds in the Schedules of the PDPA,[55] he must still provide notification if he is relying on the employment relationship exception.[56]

36 What is the nature of the notification that must be provided by the employer? In particular, must the employer provide specific notification of his use of employee monitoring software, or is the employer entitled to keep secret the use of such software? It appears that the Notification Obligation does not strictly require the employer to make the employees aware of any use of employee monitoring software. This is because the Notification Obligation only obliges the employer to state the *purposes* for collecting, using or disclosing employees' personal data, and it does not require notification of the *means* by which the personal data will be collected, used or disclosed. If this is the true position, the practical consequence is that an employer may be able to deploy employee

51 Otto notes that "once a privacy-invasive practice occurs, it is more probable that an employee will withhold his/her privacy claims (even to an extent that is against his/her reasonable interest) rather than object, risking dismissal": Marta Otto, *The Right to Privacy in Employment: A Comparative Analysis* (Hart, 2016) at p 183.

52 Gordon Anderson, Douglas Brodie & Joellen Riley, *The Common Law Employment Relationship: A Comparative Study* (Edward Elgar, 2017) at p 160.

53 Personal Data Protection Act 2012 (Act 26 of 2012) s 20(1)(*a*).

54 Personal Data Protection Act 2012 (Act 26 of 2012) s 20(1)(*b*).

55 Personal Data Protection Act 2012 (Act 26 of 2012) s 20(3)(*b*).

56 Personal Data Protection Act 2012 (Act 26 of 2012) s 20(4).

monitoring software in an entirely surreptitious manner, since many employee monitoring software are capable of operating in the background, giving the employee no indication that they are being monitored.[57]

37 This may be contrasted with the European position given in *Barbulescu v Romania*.[58] In that case, an employer dismissed an employee on the basis that the employee had misused the employer's internet connection for personal purposes, furnishing as evidence a transcript of the employee's private electronic conversations with third parties. On the facts, the employee had not been given prior notice that his electronic communications were being monitored by the employer. The employee lodged an application with the European Court of Human Rights ("ECtHR"), alleging that the Romanian courts had failed to comply with Art 8 of the European Convention on Human Rights. In finding for the employee, the ECtHR held that "domestic authorities should ensure that the introduction by an employer of measures to monitor correspondence and other communications … is accompanied by adequate and sufficient safeguards against abuse".[59] A relevant factor in this regard was whether the employee had been notified of the "possibility" and "implementation" of monitoring measures, and "for the measures to be deemed compatible with Art 8 of the Convention, the notification should normally be clear about the *nature* of the monitoring and be given in advance" [emphasis added].[60]

(3) "Purpose Limitation Obligation"

38 The "Purpose Limitation Obligation" requires that organisations collect, use or disclose personal data only for purposes "that a reasonable person would consider appropriate in the circumstances".[61] It imposes a normative standard on the purposes for such organisations' collection, use or disclosure of personal data.[62] It is an independent obligation that operates in parallel with the obligations to provide notice and obtain consent; thus the fact that an organisation has complied with the Notification Obligation and Consent Obligation (or has been exempted

57 As noted by Lim, if employers wish to "monitor the activities of their staff at work using close circuit television cameras or video cameras, computer monitoring software and other surveillance devices, they are permitted to do so with just a blanket notification": Hannah Lim YeeFen, "Data Protection in the Employment Setting" in *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Academy Publishing, 2nd Ed, 2018) at p 212.

58 *Barbulescu v Romania* (No 61496/08) [2017] ECHR 742.

59 *Barbulescu v Romania* (No 61496/08) [2017] ECHR 742 at [120].

60 *Barbulescu v Romania* (No 61496/08) [2017] ECHR 742 at [121].

61 Personal Data Protection Act 2012 (Act 26 of 2012) s 18(*a*).

62 Benjamin Wong, "Purpose Limitation Obligation: The Appropriate Purpose Requirement" [2019] PDP Digest 25 at 26.

from compliance with these obligations by virtue of a relevant exception) does not mean that it need not comply with the Purpose Limitation Obligation.[63] The Purpose Limitation Obligation requires, as a threshold requirement, that the organisation has a purpose for its collection, use or disclosure of personal data; if that threshold requirement is met, then the purpose must be assessed as to whether it is appropriate in the circumstances.[64]

39 There are a variety of purposes for an employer to collect, use and disclose employee personal data through employee monitoring software, but in general these purposes can be classified into two categories. The first category of purposes would be those listed in the Second, Third and Fourth Schedules to the PDPA as grounds for the collection, use and disclosure of personal data without consent ("Schedule purposes"). Where the collection, use or disclosure of personal data is for a Schedule purpose, it is arguable that such a purpose is generally appropriate, since "it would have been unlikely for Parliament to have included these purposes as exceptions to the Consent Obligation had it considered these purposes to be generally inappropriate".[65] Thus, if an employer is relying on a Schedule purpose to collect, use or disclose employee personal data through employee monitoring software (such as the purpose of managing and terminating an employment relationship and the purpose of employment evaluation), that purpose will generally not be problematic. However, it must be noted that the fact that an employer is collecting, using or disclosing personal data for a Schedule purpose does not automatically render that employer compliant with the Purpose Limitation Obligation, and it will be necessary to consider the specifics of the employer's purpose in order to determine if it is in fact appropriate.[66]

40 The second category of purposes would be purposes which are not listed in the Schedules to the PDPA ("non-Schedule purposes"). The assumption made of Schedule purposes (that they are generally appropriate) does not apply here. This is of course not to say that non-Schedule purposes should be assumed to be inappropriate: there are perfectly legitimate non-Schedule reasons for employers to collect, use

63 Benjamin Wong, "Purpose Limitation Obligation: The Appropriate Purpose Requirement" [2019] PDP Digest 25 at 26; *Re AIA Singapore Private Limited* [2017] PDP Digest 73 at [18].

64 Benjamin Wong, "Purpose Limitation Obligation: The Appropriate Purpose Requirement" [2019] PDP Digest 25 at 27.

65 Benjamin Wong, "Purpose Limitation Obligation: The Appropriate Purpose Requirement" [2019] PDP Digest 25 at 30–31.

66 Benjamin Wong, "Purpose Limitation Obligation: The Appropriate Purpose Requirement" [2019] PDP Digest 25 at 31; *Re Club the Chambers* [2019] PDP Digest 304 at [11].

and disclose employee personal data via employee monitoring software. These non-Schedule purposes may include, for instance, business analytics to enhance the efficiency of the employer's business processes, and organisational analytics to improve the employer's organisational structure. There are, however, other non-Schedule purposes that may be more questionable. For instance, it is not inconceivable that employee monitoring software may be offered by employee monitoring software providers, not for monetary consideration, but instead in exchange for access to the collected personal data;[67] this raises the rather difficult question of whether the use of employee personal data as "payment" for the usage of employee monitoring software is an appropriate purpose.

41 As a final note on the application of the Purpose Limitation Obligation, it is also relevant to point out that the Office of the Privacy Commissioner of Canada ("OPCC") has identified certain "No-Go Zones", or purposes which would generally be considered to be inappropriate, based on its experience in applying the equivalent of the Purpose Limitation Obligation in the Canadian federal data protection legislation.[68] In its guidelines, the OPCC flagged out "surveillance through audio or video functionality of an individual's own device" as one such No-Go Zone.[69] If a similar position is adopted in Singapore, the implication for the use of employee monitoring software would be that certain functions of employee monitoring software would generally be out of bounds for employers – for example, functions that use webcams to surreptitiously capture video recordings of employees at work.

B. "Protection Obligation"

42 A key data protection obligation imposed on organisations by the PDPA is the "Protection Obligation". This obliges organisations to "protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks".[70]

---

67 Indeed, it is not inconceivable that this is presently the business model of some employee monitoring software providers, following the business model of such successes like Facebook and Google.

68 Personal Information Protection and Electronic Documents Act (SC 2000, c 5) (Canada). See generally Office of the Privacy Commissioner of Canada, *Guidance on Inappropriate Data Practices: Interpretation and Application of subsection 5(3)* (May 2018).

69 Office of the Privacy Commissioner of Canada, *Guidance on Inappropriate Data Practices: Interpretation and Application of Subsection 5(3)* (May 2018).

70 Personal Data Protection Act 2012 (Act 26 of 2012) s 24.

43 At the bare minimum, it may be said that employers will need to have in place documented data protection policies in respect of the use of employee monitoring software.[71] Officers who have access to the employee monitoring software will also need to undergo adequate training on those data protection policies.[72] The past decisions of the PDPC make it clear that without written policies and proper training, employers are unlikely to be regarded as having fulfilled the Protection Obligation.[73]

(1) Internal and external data breaches

44 The use of employee monitoring software gives rise to the risk of two types of data breaches: internal data breaches, caused by parties internal to the organisation of the employer, and external breaches, caused by external third parties. It will be necessary for the employer to address the risk of both types of breaches.

45 It is reasonably foreseeable that internal data breaches may occur when an employer uses employee monitoring software. In particular, there is the distinct possibility that the employee monitoring software, and the personal data collected by the employee monitoring software, can be misused by the employer's officers for improper personal purposes. In order to mitigate this risk, employers may need to implement stringent access controls, limiting the number of officers who are able to access the employee monitoring software and the personal data collected. When officers who have access to the employee monitoring software leave the employment of the employer, care must also be taken to ensure that these officers cease to have access to the software, either through the deactivation of that officer's account or by the changing of passwords granting access to the software.

46 External data breaches are also a possibility that must be attended to by employers. In relation to employee monitoring software, this would likely require the employer to undertake password management and account management to prevent unauthorised third parties from easily accessing the employee monitoring software.[74]

71 See *Re Furnituremart.sg* [2018] PDP Digest 175 at [14].
72 See *Re SME Motor Pte Ltd* [2020] PDP Digest 306 at [10].
73 See, *eg*, *Re PAP Community Foundation* [2020] PDP Digest 180 at [12].
74 See *Re Orchard Turn Developments Pte Ltd* [2018] PDP Digest 223; *Re Singapore Health Services Pte Ltd* [2019] PDP Digest 376.

(2) Service provider as data intermediary

47 Additional responsibilities are incurred by the employer if the service provider of the employee monitoring software is its data intermediary. A data intermediary is an organisation which "processes personal data on behalf of another organisation".[75] A service provider may become a data intermediary of an employer when it offers cloud-based employee monitoring software and thereby processes employee personal data for the employer. In this situation, the employer would be responsible for complying with all the data protection obligations under the PDPA, in respect of personal data processed on its behalf and for its purposes by the service provider, as if the personal data were processed by the employer himself.[76]

48 Where the Protection Obligation is concerned, the employer would have the "primary responsibility" of ensuring that the employee personal data is protected.[77] Fulfilling this primary responsibility may involve imposing contractual arrangements on the service provider to put in place adequate security measures, as well as checking that the service provider is indeed following through with those contractual arrangements.[78] This may not be easy to accomplish, especially where the service provider offers its employee monitoring software on non-negotiable standard contractual terms.

(3) Heightened protection for sensitive personal data

49 The sensitivity of personal data is an important consideration for the application of the Protection Obligation. Where the personal data concerned is sensitive, the Singapore data protection regime adopts a more protective stance and will demand a higher level of protection from organisations.[79] While the PDPA does not expressly define the types of personal data that are to be regarded as sensitive personal data, and does not specify that sensitive personal data should be given special treatment, the PDPC has identified several types of personal data that would "typically be more sensitive in nature" and would merit a greater degree of protection:[80]

---

75 Personal Data Protection Act 2012 (Act 26 of 2012) s 2(1).
76 Personal Data Protection Act 2012 (Act 26 of 2012) s 4(3).
77 *Re Management Corporation Strata Title Plan No 3696* [2018] PDP Digest 215 at [16].
78 *Re The Cellar Door Pte Ltd* [2017] PDP Digest 160 at [15].
79 Benjamin Wong, "Protection of Sensitive Personal Data" [2019] PDP Digest 19 at 19; *Re Aviva Ltd* [2018] PDP Digest 245 at [19].
80 Benjamin Wong, "Protection of Sensitive Personal Data" [2019] PDP Digest 19 at 21; *Re Aviva Ltd* [2018] PDP Digest 245 at [17].

> … NRIC/Passport numbers; personal data of a financial nature such as bank account details, Central Depository account details, securities holdings, transaction and payment summaries; names of the policyholder's dependents or beneficiaries, the sum insured under the insurance policy, the premium amount and type of coverage; an individual's personal history involving drug use and infidelity; sensitive medical conditions; and personal data of minors.

50 When employers use employee monitoring software, there is a high likelihood that sensitive personal data will be collected, used and disclosed, due to the indiscriminate data collection done by employee monitoring software. For example, employee monitoring software that record the contents of conversations held over instant messaging platforms such as Facebook Messenger may capture discussions about the employee's sensitive medical conditions. If screenshots of an employee's computer screen are regularly taken, those screenshots may capture the employee's financial information if the employee happens to be engaging in online banking at the time the screenshots are taken. The risk of capturing sensitive personal data may be elevated in the context of remote working, especially if the software is installed on the employee's personal computing device and monitors the employee in her own home. It is thus likely that employers who use employee monitoring software will have to provide the higher level of security demanded by the PDPA in respect of sensitive personal data, unless they manage to avoid collecting sensitive personal data when using employee monitoring software.

C. "Transfer Limitation Obligation"

51 Some employee monitoring software transmit personal data across borders. These include employee monitoring software that are cloud-based, since such software would inevitably transmit personal data to the service providers' servers for hosting and processing, and these servers are likely to be located outside of Singapore. The cross-border transfer of personal data potentially engages the "Transfer Limitation Obligation" under the PDPA, which provides that organisations cannot "transfer any personal data to a country or territory outside Singapore" except in accordance with the requirements prescribed by the PDPA.[81] This would require the employer to take appropriate steps to ensure that the recipient of the personal data (in this case, the service provider) is bound by "legally enforceable obligations … to provide the transferred personal data a standard of protection that is at least comparable" to that conferred by the PDPA.[82]

81 Personal Data Protection Act 2012 (Act 26 of 2012) s 26(1).
82 Personal Data Protection Regulations 2014 (S 362/2014) reg 9(1)(*b*).

52 There are several recognised ways by which the service provider may be regarded as being bound by legally enforceable obligations to provide an equivalent level of protection to personal data. If the personal data is transferred to an overseas location with data protection laws that are comparable to the PDPA, those foreign data protection laws can qualify as legally enforceable obligations for this purpose.[83] If, however, the personal data is not transferred to a location where there are comparable data protection laws, then it may be necessary to make the transfer of the personal data subject to contractual obligations that require the service provider to provide a standard of protection to the transferred personal data that is at least comparable to the protection under the PDPA.[84] In the event that it is not feasible for the employer to ensure that the service provider is bound by the requisite legally enforceable obligations, one alternative is for the employer to obtain the consent of his employees for the transfer of their personal data out of Singapore.[85]

V. Recommendations

A. Good practices

53 It is clear that excessive surveillance of employees using employee monitoring software can result in significant backlash and negative publicity.[86] There is therefore a business case to be made for the responsible deployment of employee monitoring software, even if doing so involves the adoption of standards of practice that go beyond the requirements of the PDPA. Three good practices may be suggested.

(1) Being transparent to employees

54 The Notification Obligation under the PDPA probably does not, strictly speaking, require that employers notify employees that they are being monitored by means of employee monitoring software. There may, however, still be good reason for employers to be transparent to employees about the operation of employee monitoring software. This is because there are situations where the employer may be nonetheless

83 Personal Data Protection Regulations 2014 (S 362/2014) reg 10(1)(*a*); Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 9 October 2019) at para 8.5.

84 Personal Data Protection Regulations 2014 (S 362/2014) regs 10(1)(*b*) and 10(2); Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (revised 9 October 2019) at para 8.5.

85 Personal Data Protection Regulations 2014 (S 362/2014) reg 9(3)(*a*).

86 For a recent example, see Kalyeena Makortorff, "Barclays Using 'Big Brother' Tactics to Spy on Staff, Says TUC" *The Guardian* (20 February 2020).

compelled by the PDPA to reveal his use of employee monitoring software. For instance, if an employee requests access to his personal data that is in the possession or under the control of the employer – as the employee is generally entitled to do pursuant to the "Access and Correction Obligation" under the PDPA – the employer would be obliged to provide the employee with that personal data, as well as information about how the personal data was used or disclosed by the employer within a year of the date of the request.[87] This would likely reveal the fact that the employer has been collecting the employee's personal data using employee monitoring software of some kind. It is perhaps preferable, as a matter of employer–employee relations, for the employer to simply be upfront about his deployment of employee monitoring software, rather than risk being discovered by his employees to have engaged in surreptitious surveillance using employee monitoring software.

(2) Giving individual employees control

55 As mentioned above, the Consent Obligation under the PDPA has limited applicability in the context of employee monitoring software, and this means that employees have little control over how their employers use employee monitoring software. That being said, it seems sensible to give employees some control over when and where they are monitored. Doing so exhibits respect for the individual autonomy of the employees, transforming the employee monitoring software from a tool for employee surveillance to a tool for employee accountability – a means by which employees can report their progress at work and account for the time that they spend at work.

56 Furthermore, granting employees control over the operation of the employee monitoring software also has the practical benefit of avoiding the collection of sensitive personal data, since employees are unlikely to trigger the operation of the employee monitoring software in the knowledge that doing so at that time would result in the collection of their sensitive personal data. By avoiding the collection of sensitive personal data, the employer can minimise the regulatory burden imposed by the Protection Obligation under the PDPA.

57 It is notable that some employee monitoring software have been designed to give employees control. For example, the application offered by Hubstaff appears to operate on the basis of task timers, which individual employees may turn on themselves when they begin to work on a particular task; the Hubstaff desktop application only "monitors the employee's computer usage as long as they are tracking time, and never

87 Personal Data Protection Act 2012 (Act 26 of 2012) s 21(1).

when the timer isn't running".[88] This grants employees both knowledge of, and some degree of control over, the monitoring that takes place.

(3) Data minimisation

58 Data minimisation is the principle that "the amount of personal data collected should be limited to what is necessary to achieve the purpose(s) for which the data is gathered and further processed".[89] Data minimisation is not a data protection principle that has been built into the PDPA.[90] However, it may nonetheless be good practice for an employer to minimise the amount of personal data that he collects using employee monitoring software. This is because the minimisation of personal data retained by the employer can constitute a reasonable security measure for the purposes of compliance with the Protection Obligation under the PDPA.[91]

59 Some employee monitoring software come with options for limiting the quantity and quality of data that is collected. For example, employee monitoring software that offer screen capturing capabilities often include the option to blur screenshots, so as to capture the gist of what has appeared on the employee's computer screen without necessarily also capturing the details.[92]

B. Regulatory guidance

60 From a regulatory standpoint, it may be valuable for specific guidance or codes of conduct to be given in relation to the use of employee monitoring software. Such guidance would be timely in the present context of the COVID-19 pandemic, as it has forced employers and employees to adapt to working from home as a matter of default, and this could drive the uptake of employee monitoring software by employers.

88 See Hubstaff, "Employee Monitoring" <https://hubstaff.com/features/employee_monitoring> (accessed 3 February 2020).

89 Lee A Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014) at p 151.

90 This is unlike the data protection legislation of some other jurisdictions like the EU and Hong Kong: see Art 5(c) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1; and Schedule 1 para 1(1)(c) to the Personal Data (Privacy) Ordinance (Cap 486) (Hong Kong).

91 See *Re Bud Cosmetics Pte Ltd* [2019] PDP Digest 351.

92 See, *eg*, DeskTime website <https://desktime.com/features/time-tracking-with-screenshots> (accessed 3 February 2020).

61 Such guidance would not be unprecedented. For example, the UK Information Commissioner's Office ("ICO") has released an extensive code of conduct for employment practices containing, among other matters, a set of good practice recommendations on employee monitoring.[93] In this code, the ICO set out a general approach to monitoring, followed by guidance on specific forms of monitoring, such as the monitoring of electronic communications and video and audio monitoring. More recently, the British Columbia OIPC issued a guidance document for employee privacy rights, containing in particular guidance on employee monitoring software and GPS tracking.[94]

VI. Conclusion

62 As a matter of public policy, there may be some cause for circumspection about the adoption of employee monitoring software. As is apparent from the range of data collection capabilities afforded by modern employee monitoring software, the use of employee monitoring software can be highly invasive to the privacy of employees. The irresponsible use of employee monitoring software can erode public trust in the processing of personal data by organisations in Singapore.

63 The policy problems posed by employee monitoring software do not end even if employees eventually grow to accept or tolerate the invasiveness of these software. In this regard, Shoshanna Zuboff has raised concerns about the normalisation of invasive surveillance technologies through the institution of the employment relationship. As Zuboff puts it, the workplace is the "gold standard of habituation contexts, where invasive technologies are normalized among captive populations of employees".[95] Unlike consumers who in general have the practical freedom to avoid products that engage in surveillance, employees are "captive" in the sense that they usually have little real capacity to reject surveillance by their employers.[96] Captive employees who are subject to surveillance by surveillance technologies in their daily lives in their workplaces may become habituated to living with these surveillance technologies. The consequence of habituation is that these employees

93 United Kingdom, Information Commissioner's Office, *The Employment Practices Code* (2011) at p 65.

94 British Columbia, Office of the Information and Privacy Commissioner, *Employee Privacy Rights* (2017).

95 Shoshanna Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019) at pp 156–157.

96 While it is true that some employees may have sufficient bargaining power to effectively opt out of undergoing surveillance, it is unlikely that the majority of employees will be able to negotiate for privacy in this way.

may come to accept the application of similar surveillance technologies in other aspects of their lives, such as in the context of the home, where such surveillance technologies would previously have been regarded as unacceptably invasive.[97] Habituation to surveillance technologies may pose problems for data protection, as both organisations and individuals have a role to play in the protection of personal data.[98] If individuals are desensitised to privacy incursions through the process of workplace habituation, then it can be expected that they will become less motivated to protect their own privacy interests.

64 The invasiveness of employee monitoring software may be minimised if employers who deploy such software do so in a responsible way. The responsible deployment of employee monitoring software, it is argued, would entail not only compliance with the legal requirements of Singapore data protection legislation, but also the implementation of good practices that are respectful of the informational privacy of individual employees. This article has sought to provide some relevant guidance towards that end.

---

97 Habituation is part of what Zuboff calls the "dispossession cycle", which she claims that "surveillance capitalists" use to normalise the extraction of "behavioural surplus". The "dispossession cycle" comprises four steps, namely (a) incursion; (b) habituation; (c) adaptation; and (d) redirection. See Shoshanna Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019) at pp 137–138.

98 See *Singapore Parliamentary Debates, Official Report* (14 January 2019) vol 94.