Workforce surveillance monitoring tools and strategies
By Helen de Oliveira Carvalho

The pandemic has substantially impacted the way in which we all work and where we carry out our work.

Consequently, remote working has led to issues arising in connection with:

1. Flexibility around working models and work locations;
2. Employer's requirement for oversight into workforce performance; and
3. Employees right to privacy.

Employer's perspective:

From the employer's perspective, we know that there is an increased requirement to offer employees flexibility around work models. COVID coupled with "The Great Resignation" has undoubtedly escalated the demand for flexibility around work models. The adjustment to new offsite or remote work models, has naturally led to employers wanting to maintain, in some cases increase, oversight into the productivity of the workforce.

Additionally, there is emerging data which suggests that obtaining workforce data can lead to more positive insight for companies. A recent study published by Accenture states that ***"Companies that put in place responsible data strategies could see revenue growth up to 12.5 percent higher than that of companies that fail to adopt responsible data strategies."***[1]

What is interesting about this statement is the indication that what drives the successful collection of workforce data is the ***"responsible"*** adoption of such strategies. We will come back to this point of "responsibility" in our actionable steps checklist below.

Employers are now not only looking to increase oversight into workforce productivity but we are also starting to see evidence that could support the idea that responsible workforce data collection can lead to a direct impact on revenue.

Increased Data Protection rights under the UAE legal framework:

To consider the potential legal implications that an employer's enhanced workforce oversight data strategies could have on the rights of individual employees, we first should start by considering and acknowledging the current legal backdrop and the recently enhanced legal protections offered to individuals under the UAE Federal Decree-Law No. 45 of 2021 Regarding the Protection of Data Protection ("Law").

The Law provides a framework to ensure the protection of data and the privacy of individuals in the UAE. These developments support the long-established constitutional right to privacy under Article 31 of the UAE Constitution and the Law now further recognises the

1 https://newsroom.accenture.com/news/more-responsible-use-of-workforce-data-required-to-strengthen-employee-trust-and-unlock-growth-according-to-accenture-report.htm

Cynthia KL Le Poer Trench (Solicitor, Hong Kong) Principal

Member of Interleges

Office 712, Preatoni Tower,
Cluster L, Jumeirah Lake Towers
PO Box 21832, Dubai, UAE
T + 971 (0) 4 355 3146
F +971 (0) 4 355 3106
E info@trenchlaw.com
W www.trenchlaw.com

protection of personal data as a standalone right. What this Law does is provide individuals with rights over their personal data by providing an integrated governance framework, which runs from federal level and across all industry sectors, for the management of data protection.

It is interesting to note that the UAE Federal Government partnered with major technology companies to draft the Law; this is the first time we have seen the federal law in the UAE drafted in collaboration with the private sector[2]. We will also come back to this point of ***"collaboration"*** in actionable steps checklist below.

The balancing act:

How can companies seek to balance the continuing drive towards increased workforce oversight, through increased workforce data collection through various tools such as CCTV, to activity tracking, time tracking, software and activity loggers, as against the increased data protection rights accessible by individuals who make up the workforce?

From a risk management perspective, can companies safely continue to increase workforce oversight, increase workforce data collection and at the same time manage the risks of increased data breaches and the legal and reputational harm that can follow breaches of data protection rights?

Risk associated with workforce data tools & strategies:

Before we delve into how employers can seek to manage the legal risks of increased workforce surveillance strategies, which we will turn to in the final checklist at the bottom of this article. It is important to consider some of the other impacts that such increased workforce monitoring and surveillance can have on the workforce itself:

a. Acknowledging the inherent imbalance of power between an employer and employee.

Action:

- Prior to implementing workforce surveillance tools and strategies, it is important to acknowledge that (subject to a few exceptions), employers must obtain consent from the employees before implementing any workforce data surveillance tools or strategies.
- To ensure that the right approach is adopted by the employer when seeking such consents, it is advisable to be acutely aware of the inherent power imbalance between employers and employees as this knowing and acknowledgment can positively impact the way in which such strategies are communicated to the workforce.
- With power comes ***responsibility*** and maintaining awareness of the imbalance between employers and employees will help employers to responsibly decide at the outset which workforce monitoring tools and strategies could be deemed as disproportionate, intrusive or unnecessary.

[2] https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws

Cynthia KL Le Poer Trench (Solicitor, Hong Kong) Principal

Office 712, Preatoni Tower,
Cluster L, Jumeirah Lake Towers
PO Box 21832, Dubai, UAE
T + 971 (0) 4 355 3146
F +971 (0) 4 355 3106
E info@trenchlaw.com
W www.trenchlaw.com

Member of Interleges

b. Issues of trust within the workforce.

The implementation of workforce data/surveillance tools can create an environment of mistrust and unease.

Action:

- Excellent communication and transparency from the employer to the workforce, around what is being collected, why and how, is key.
- Additionally, without such transparency the validity of the legal consents collected from the employees by the employer may not be valid.
- Involving employees in a consultation phase can create trust among the workforce and fuel an environment of ***collaboration***.

c. Integrity of the monitoring tools.

Failure to understand the technical risks involved with monitoring tools could result in financial, reputational, litigation and in worst case scenarios imprisonment for those who are managing the company.

Action:

- As an employer owing a duty of care to the employees in the workplace, it is vital that the employer runs all monitoring tools through its own integrity filter to align with the provisions of various legislation within the UAE including but not limited to the Cybersecurity Law and more specifically with respect to the anti-discrimination provisions of the new Labour Law. Failure to understand such tools can leave companies exposed. See below article with respect to AI recruitment features on Facebook which were exposed to allegations of gender discrimination: https://www.forbes.com/sites/carriekerpen/2021/09/09/facebook-under-fire-for-alleged-gender-discrimination-in-job-advertisements/?sh=433bf1ab3f72 https://privacyinternational.org/video/4710/pas-story-how-facial-recognition-system-potentially-failed-recognise-driver-colour-and
- To purchase tools responsibly, we would recommend that the procurement team, IT security team, data protection officer, diversity & inclusion team work together to identify if the tools align with the purpose for which the employer is implementing it and the employer's values and the widely known and accepted seven key data privacy principles.
- Ensure that the tools will allow the employer to come good on any employee's individual rights claims which they may have under the applicable Data Protection Law.

Summary:

- It is essential for businesses to ensure that they offer their workforce transparency regarding the usage of workplace surveillance and monitoring tools.
- In the UAE the best approach to implementing any such tools is to obtain written consent from the employees.
- Employers must also be aware that under the Data Protection Law employees do have rights to the data being collected and processed, including but not limited to the right to access and request copies of any personal data relating to the employee.

Cynthia KL Le Poer Trench (Solicitor, Hong Kong) Principal

Member of Interleges

Office 712, Preatoni Tower,
Cluster L, Jumeirah Lake Towers
PO Box 21832, Dubai, UAE
T + 971 (0) 4 355 3146
F +971 (0) 4 355 3106
E info@trenchlaw.com
W www.trenchlaw.com

Below is a checklist of actionable steps which we hope will help your company reach a position of confidence with respect to the tools currently in use at your company and review or obtain the recommended legal consents:

Current state checklist:

Phase 1

Conduct an inventory of the various workplace surveillance tools across the organisation and if your company has more than one site ensure that the inventory covers all the various sites controlled by the company. This is important because it will be the backbone upon which your consents will drafted upon.

In this phase you want to clearly identify the following:

(a) the scope of the data that the surveillance tools are collecting with respect to employees,

(b) the purpose of the surveillance tools being used in each site;

(c) where, how and whom is storing the data being collected via the tools;

(d) identify and remove any CCTVs or other monitoring tools in private areas (such as bathrooms, prayer rooms);

(e) identify if there are accompanying signs with monitoring tools (ie. CCTV monitored area); and

(d) discover how long the data is being stored for and by whom.

Note: personal data should only be stored for the length of time necessary to meet the purpose ***(item b above)*** behind the collection of that data or for the legal retention period prescribed by law. The legal retention period will override the retention period provided under privacy notices

Phase 2

✓ Establish whether the existing consents are valid by considering:

(i) which data protection law applies to your company and its activities and whether your company is subject to any exceptions under any other laws such as the Local Laws Dubai Law No. 24 of 2008 and its amendments on 'Regarding Security Service Providers and Users'.

(ii) whether the company has valid express consent to collect the data identified in Phase 1 above as against the applicable data protection law.

Note: Consents may be found by looking at the existing employment agreements, addenda to the employment agreements and employee-signed company policies.

If the boundaries of the consents have been exceeded or if express consents are not currently in place, we would suggest that the below steps are taken/considered:

(a) obtain valid consents from its employee;

(b) the company and its advisors will need the information collected in steps Phase 1 above in order to draft valid consents; and

(c) consider rolling out a communication campaign aimed at creating transparency between the company and its employees. Such campaigns can be executed through the collaboration of relevant departments. Depending on the structure of the company, relevant departments could be the security team, HR team, in-house legal team, data protection officer and/or the company's facilities management team.

Cynthia KL Le Poer Trench (Solicitor, Hong Kong) Principal

Member of Interleges

Office 712, Preatoni Tower,
Cluster L, Jumeirah Lake Towers
PO Box 21832, Dubai, UAE
T + 971 (0) 4 355 3146
F +971 (0) 4 355 3106
E info@trenchlaw.com
W www.trenchlaw.com