SCANNING THE SCANNERS – WHAT EMPLOYERS NEED TO KNOW ABOUT THE PRIVACY ACT

23 October 2019 | Global Insights
Legal Briefings

As technology evolves with unprecedented speed, the law can struggle to keep pace. Nowhere is this more apparent than in the area of employment relations and specifically the topic of employee monitoring, where companies and organisations are discovering the truth of the old adage: just because you can do something, it doesn't mean you should...

With security top of mind, both in the physical realm and in the expanding space that is the digital world, it has become increasingly important that organisations have measures in place to ensure the safety of both their staff and their businesses.

One of the ways to do this is implementing fool-proof systems to monitor staff – when they are accessing company premises or carrying out other tasks on behalf of their place of employment. Fleet management and job allocation are just two of the areas where it is advantageous for organisations to know the exact location of their employees at any given moment. But advanced technological processes that facilitate this could be problematic for those who implement them.

Kaman Tsoi, Special Counsel at Herbert Smith Freehills, points to a notable recent test case brought before the Fair Work Commission (FWC) in Australia that involved a company installing fingerprint scanning as its access control system, only to fall foul of the *Privacy Act* when one employee refused to comply. "Because of the way the *Privacy Act* works, fingerprints are treated as biometric information, which is a type of sensitive information, and as such gets a higher level of protection under the *Privacy Act*. In most cases you need consent to collect sensitive information," explains Kaman.

Prior to this case, Australian employers have traditionally relied on an employee records exemption that other countries, such as Germany, Sweden or Singapore, don't have. It's one of two major exemptions relatively peculiar to Australia, the other being a small business exemption, which generally applies to companies with an annual turnover of under $3 million. Both exemptions were brought in at the time of the privacy legislation as a concession to employers and small businesses concerned about compliance costs.

On close examination of the employee records exemption wording, however, it was noted that it exempts conduct relating to personal information that is 'held' in an employee record.

According to the FWC, this means that for any information that is not yet held in such a record, any attached obligations still apply. The obligations in the original *Privacy Act* deal with different stages of the handling of personal information, such as what needs to happen during the actual collection process, and what happens after; i.e. how companies are legally required to store the information and, also, how they are allowed to use and disclose it.

With the fingerprint case, the employee claimed that as his fingerprint hadn't yet been collected and put into his employee record, the employee records exemption didn't apply. "Historically, his employers would have claimed that the exemption applied to all of their conduct, not just the conduct post the actual creation of the record," says Kaman. The FWC, however, found in the worker's favour and he was awarded compensation.

As a result of this case, employers, who have been used to relying on the employee records exemption, need to amend their practices and ensure that they provide employees with details of what they intend to do with any personal information that they collect, and ensure that any sensitive information is collected lawfully, which may require consent.

THE IMPACT OF GDPR

In Europe the recent implementation of the GDPR (General Data Protection Regulation) has had similar ramifications, says Christine Young, Partner at Herbert Smith Freehills. "The GDPR applies to monitoring employees as much as it does any other data subject," says Christine. But she agrees that advancements in technology mean that the law is still playing catch-up with what employers are now physically capable of doing. "I'm aware of some organisations where they don't just have CCTV, but they also have pressure pads under desks to work out how often someone is at their desk."

As in Australia, though, UK employers need to have a lawful basis for accessing or retaining any personal data.

The caveat to this is that European authorities have concluded that an employment relationship is not one of equal bargaining power. "Therefore, an employee can never genuinely be considered to give consent freely in an employment context, which I think is going to be a real problem for organisations in the future if they're collecting more and more of this data," says Christine.

“There are two sides to the legality,” she adds. “One is legally can you do it? And the second is about what you tell people you’re doing with the data. Because with the GDPR, you have to consider both."

“You have to be transparent because there’s a lot of case law in Europe about the use of covert monitoring of staff, which is usually considered to be inappropriate.”

Christine points to one case in which CCTV footage from an educational lecture theatre was put in place following a case of theft. The lecturer complained that this use was a breach of their privacy and the court agreed it was an inappropriate processing of their personal data and upheld the lecturer’s complaint.

In another example, staff at the John Lewis department store complained that the company was ‘spying’ on them when mystery shoppers were fitted with hidden cameras, in an initiative aimed at improving customer service. A worker, writing in the store’s *Gazette* magazine, said the filming was a “gross invasion of privacy”.

As the technology advances further the likelihood of similar cases increases. Whereas it used to be the domain of sci-fi and spy movies, we’re now starting to hear about facial recognition technology being used in workplaces, and not necessarily sensitive environments such as government or military locations. The probability of some workers baulking at being subjected to this technology is high. And not just workers. Christine relates a recent situation at King’s Cross Station in London, when an organisation that owns some of the land there erected facial recognition cameras. “They were able to collect data on the public, because it’s a public station,” she says. “And there was a huge backlash on that which had very significant reputational issues.”

LOCATION TRACKING

Employee monitoring also enters a grey area when organisations use technology to track the physical whereabouts of their staff; for example, in aforementioned instances such as fleet management or job allocation. In Australia, the *Privacy Act* is the national law that applies to the handling of personal information, but it doesn’t have specific provisions for location tracking or surveillance. Compounding the tricky nature of this is that all of the laws around surveillance are actually state laws and the legislation may differ from state to state. While most cover devices such as video surveillance like CCTV and audio recording devices, not all jurisdictions cover location tracking, such as GPS.

In the UK, it is again a case of ‘just because you can it doesn’t mean you should’. “In theory, what you should do as an employer is turn off the GPS when the person’s not working,” says Christine. “There are obviously technological difficulties with that, but you certainly shouldn’t be actively monitoring.”

SOCIALLY ACCEPTABLE

While employers are looking to monitor the physical location of their staff, conduct has become an equally important focus. “Employees’ use of social media, for example, can be of concern to organisations sensitive about brand or reputation issues,” notes Kaman. Monitoring email and internet usage is significant, but in the mobile device era, employees’ phones can also contain GPS tracking, which again falls into an area in which the legislation is unclear.

Employers have always held data about their staff, but what has changed is the quantity. And the power and consolidation of these databases means that all of that data can be searched, interrogated and manipulated in a whole lot of new and more powerful ways.

But in this brave new world, cases like the fingerprinting scanning one and overuse of CCTV show that both employees and employers may perhaps want to put the brakes on a little.

“It’s a very live issue at the moment,” says Christine. “People are asking questions about ‘what functionality do you have?’, ‘were you actually using it?’, ‘what were you using it for?’ and ‘why didn’t you tell us?’”

This suggests that employers who are looking to take things in that direction need to be very careful, because if the law is saying you can’t actually monitor every employee without this being tailored to only what is absolutely necessary and you need to be prepared for challenge by employees as they become more aware of this monitoring, then is the system really going to achieve what it’s intended to achieve anyway? And with the example of the access entry system, maybe swipe cards, which don’t involve biometric information, are a simpler way to go.

Please click here to view The Data Economy Hub

Please click here to view Disruptive Technology & Innovation Hub

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

KAMAN TSOI

CHRISTINE YOUNG

SPECIAL COUNSEL, MELBOURNE
+61 3 9288 1336
kaman.tsoi@hsf.com

PARTNER, LONDON
+44 20 7466 2845
Christine.Young@hsf.com

LEGAL NOTICE