LEGAL UPDATE

# DREWTECH SERIES CHAPTER 2

**4 June 2019**

# EMPLOYEES, TECHNOLOGY AND A LEGAL HANGOVER – BRING YOUR OWN PROBLEMS?


## SUMMARY

Corporate information governance is changing to take advantage of a hyper-connected world and an explosion in the market for enterprise and consumer devices that significantly improve productivity. This note discusses some possible legal and technological implications of a "Bring Your Own Device" policy which some employers may implement to take advantage of their employees' shifts in attitudes towards technology. It is critical for employers to ensure that information governance policies are properly calibrated with the right legal and technological advice to mitigate risk while at the same time allowing the employer to enjoy the benefits of improved productivity from technology.


## THE WORLD IS IN LOVE WITH TECHNOLOGY

Take a moment to think about how many devices you carry around with you – a smartphone, tablet, laptop, maybe even a smartwatch or a fitness tracker. For most of us, our tech is the last thing we caress (figuratively?) before we go to bed and the first thing we embrace (figuratively?) when we wake up.

Because we love our tech, we spend countless hours personalizing our devices. We all have our favourite hardware and apps. We grow accustomed to the face of the tech that we use. We become so accustomed to our tech that we want to use it ALL the time – even when at work.

"Employee: Dear employer, I want to use my smartphone, not yours".

"Employer: You mean you will spend your money on your tech and use it to do my work? That's great!"

And so, the Bring Your Own Device ("**BYOD**") programme was born. It found favour with employers because there were obvious cost savings. It also found favour with employees who didn't have to learn a new tech platform or deal with multiple (and sometimes clunky) devices. They could use whatever device they wanted so long as there were no compatibility issues.

It was (and is) a beautiful idea. It works for everyone. What could go wrong?

## PRIVACY, PRIVACY, PRIVACY!..... WHAT PRIVACY?

"Employer: If you are going to use your tech to do my work, I should have the right to access and inspect your tech (obviously)."

"Employee: But what about my right to privacy?"

Do employers infringe upon the Personal Data Protection Act 2012 ("**PDPA**") when they offer such programmes and reserve a right to access and retrieve company data from their employees' tech? Or do employees forgo their "right to privacy" over the contents of their personal devices when they participate in a BYOD programme?

First off, let's clear the air on one common myth: there is no general right to privacy in Singapore. The Singapore courts have not made any explicit pronouncement that there exists a general tort of privacy; neither does the Constitution of Singapore provide for the protection of privacy as a fundamental right; nor is there an omnibus privacy legislation in our statutes. This is very unlike the situation in Europe, where the right to privacy is enshrined in the European Convention on Human Rights, and in parts of the Commonwealth which

have been steadily recognising privacy as a standalone common law right. The enactment of the PDPA does not change this general position.

However, this does not mean an employer can demand access to an employee's mobile phone to flip through his WhatsApp conversations without repercussions. Singapore's approach to the protection of an individual's privacy is achieved by a framework of common law and statutory torts which seek to protect aspects of an individual's privacy. An action in defamation, trespass, nuisance, negligence or breach of confidence may all indirectly protect one's privacy in certain circumstances. In the employment context, an employee could even claim that there is an implied term in one's employment contract that the employer owes a duty of trust and confidence not to, for instance, conduct extensive on-premises surveillance of one's employees.

The PDPA was introduced as one of Singapore's most extensive pieces of legislation on personal data. It seeks to hold organisations accountable for the proper and respectful handling of one's personal data, defined as data from which an individual can be identified from, or data that, together with other information to which an organisation has or is likely to have access, an individual can be identified. The PDPA imposes a standard of conduct that permits reasonable use, processing and disclosure while preventing misuse or abuse of personal data. However, the scope of its protection is limited to one's informational privacy, and the Personal Data Protection Commission has cautioned that it should not be distorted to address privacy issues beyond its intended scope.

## WHAT'S MINE IS MINE, WHAT'S YOURS IS MINE TOO?

There is much to be celebrated in the mutual benefits which a BYOD programme brings to the workplace: employers enjoy the cost savings of not having to purchase and replace equipment for their employees, and employees experience the freedom of working on their personal device without having to worry about multiple devices for work and personal use.

But alas, the age-old tension between security and confidentiality once again arises: can an employer tread the fine line between securing its confidential company data on the employee's device without infringing upon its PDPA obligations to avoid the misuse of its employee's personal data?

The short answer is yes, with a properly calibrated BYOD policy, the right advice and the right tech.

The most common forms of BYOD programme management are the Mobile Device Management ("**MDM**") and the Mobile Application Management ("**MAM**") policies. Both of these policies provide the means by which an employer can preserve and protect the corporate data stored in an employee's device:

(a) MDM policies deal with the administration and management of mobile devices, allowing an employer to set its security configurations on an employee's personal device. The employee's BYOD device may be configured such that confidential corporate data are segregated or partitioned from the employee's personal data (a "**Corporate Partition**"). MDM policies may allow an employer to conduct a complete lockdown or wipe of the Corporate Partition of an employee's device if, for instance, the employee's device is lost or stolen.

(b) In contrast, MAM policies avoid the management of mobile devices, but instead offer application-level management of the employee's BYOD devices. Employees are limited to conducting their email and work on specific corporate applications ("**Corporate Applications**"), and the employer's controls over the employee's device are in turn limited to these Corporate Applications (as opposed to the device). The employer may thus disable the access to, for instance, the employee's corporate e-mail application, without having to disable part of or the entire device.

Of course, everything is fine, until it is not. When relationships sour, and an employee's employment is terminated, the employer may need to lockdown or wipe the corporate data stored in the Corporate Partition or the Corporation Application on an employee's BYOD device.

If the employer's BYOD policy is not well calibrated or if the employer's tech infrastructure is dated or not properly configured, there is also the possibility that the employer may need all of the data on the employee's device to be wiped to ensure there is no leakage of confidential corporate data.

It is at this stage that rights and obligations come into focus. Is the employer entitled to access the employee's personal device (whether through pre-determined technological means, or as a (reasonable?) instruction to the employee) to delete confidential corporate data, which may or may not be commingled with employee personal data? The answer may well depend on how well defined the employer's and employee's rights and obligations are in the BYOD policy. It would be prudent for employers to seek appropriate advice from technology lawyers who can bridge the gap between management expectations, legal risk management and technology risk management.

What about possible infringements of the PDPA? The PDPA governs generally the collection, use and disclosure of personal data – the access and deletion of corporate data may not run afoul of these obligations. But grouses from the employee are to be expected – no one likes it when you poke around their personal stuff. To mitigate this, a good BYOD policy would also include an express notice seeking the consent of the employee to allow the employer to access the employee's device in the event that corporate data needs to be preserved or wiped. The employee should thus have no cause for complaint if he or she had consented to these terms before participating in the employer's BYOD programme.

## CONCLUSION

It is attractive for employers and employees to take advantage of technological advancements both in the enterprise and consumer space to improve productivity. However, before taking a ride on the BYOD bandwagon, it would also be prudent to ensure that rights and obligations between the employer and employee are clearly defined so that the interests of the employer are protected and the employee's rights are respected. Seeking legal advice will help to mitigate the risk of such disputes arising, but it is also important for the legal advice to take into account the technological limitations and possibilities of the employer's IT infrastructure so that the advice can be as effective as possible.

---

If you have any questions or comments on this article, please contact:

**Rakesh Kirpalani**
Director, Dispute Resolution / Information Technology
T: +65 6531 2521
E: rakesh.kirpalani@drewnapier.com

---

**Updates in DrewTech Series**

1. Chapter 1: The Importance of An Exit Strategy in Technology Contracts <6 March 2019>
2. Chapter 2: Employees, Technology and A Legal Hangover – Bring Your Own Problems? <4 June 2019>



Drew & Napier LLC
10 Collyer Quay
#10-01 Ocean Financial Centre
Singapore 049315

**www.drewnapier.com**

T : +65 6535 0733
T : +65 9726 0573 (After Hours)
F : +65 6535 4906

LEGAL UPDATE