COMPUTERS & LAW

Journal for the Australian and New Zealand Societies for Computers and the Law

Editors: Daniel Thompson, David Ng and Isaac Lin

ISSN 08117225

Number: 85

August 2013

Celling Out

Is BYOD a cost saver or a cost creator?

By Jessica Gurevich and Capucine Hague

Jessica Gurevich *is a commercial lawyer in Webb Henderson's Singapore office. Her practice focuses on matters in the telecommunications, media and technology sectors across the Asia Pacific region. Prior to joining Webb Henderson, Jessica was a lawyer in the Intellectual Property and Technology group of Corrs Chambers Westgarth in Sydney. Jessica holds bachelor degrees in Laws (honours) and Commerce (finance), both from the University of Melbourne*

Capucine Hague *recently graduated from the University of Sydney, where she completed a bachelor degree in Laws (honours) and Arts (art history), and studied abroad at the University of Pennsylvania and the National University of Singapore. Capucine will be returning to Webb Henderson as a graduate lawyer in 2014.*

Introduction

BYOD, the latest techno acronym for "Bring Your Own Device", the recent trend in which a company will adopt a policy either allowing or requiring employees to use their own phones, tablets and similar devices for work purposes, sometimes instead of providing a corporate owned device. The policy has attracted significant interest as a method of cutting costs, aiding flexible work arrangements and increasing employee satisfaction.

The merits of allowing or requiring employees to use personal devices for work purposes have been subject to considerable debate. Some of the issues companies should consider when formulating their BYOD policy are set out below. Employers should also take steps to implement a comprehensive policy on personal devices in the workplace - even if the policy prohibits or restricts BYOD to limited functions. Studies have found that around 77% of employees use personal devices for business purposes,[1] however only 53% of organisations officially condone BYOD[2]. Corporations that do not

In this issue

From the editors...

New technology, faster broadband, the proliferation of smart phones and new online services are giving rise to a host of legal challenges considered in this issue.

Jessica Gurevich and Capucine Hague consider the 'Bring Your Own Device' or BYOD phenomenon, a recent trend whereby companies allow or require employees to use their own phones, laptops or similar devices for work purposes. They discuss key factors and legal implications that companies need to consider in formulating a BYOD policy.

Katrina Cavanough, the winner of the 2012 Student Essay Prize, considers the implications of modern technology and ever-increasing broadband speed for copyright protection, and the potential for ISPs to play a gatekeeper role in the fight against piracy of copyright content following the 2012 High Court decision in *Village Roadshow Pty Ltd v iiNet.*

The difficulties facing traditional notions of copyright in the digital age are further explored in the context of online video streaming services in separate articles written by Victor Lei and Jesse Gleeson. These articles highlight the uncertainty surrounding the questions of whether streaming copyright content is an infringement of copyright, and whether the provision of streaming and recording services (for instance, of free-to air television) constitutes copyright infringement.

In her article 'Sub-licences – Underestimated and Overlooked?', Anne Petterd considers recent UK case law that considered a tricking software licensing question, namely, whether a sub-licence can continue to exist once the head licence under which it was given falls away. A recent ruling of the England and Wales High Court suggests that under certain circumstances, a sub-licence may continue on-foot notwithstanding the termination of the head-licence.

Daniel Thompson, David Ng and Isaac Lin

have a comprehensive plan in place risk security breaches and loss of confidential or commercially sensitive information through lack of employee awareness of appropriate measures that they may need to take.

Key recommendations

1. Balance interests – BYOD isn't simply about protecting company information, it's also about respecting employee privacy.
2. Invest time in creating and implementing a comprehensive use and security policy.
3. Make BYOD official – don't just tacitly approve or tolerate employees using their own devices.

Considerations when developing a BYOD policy

Accessible types of data

Employers should consider whether they will restrict the data which their employees have access to on their own devices. There is a significant difference between allowing employees to access company communications (email, voice calls and SMS messages), and facilitating access to software, platforms, resources, documents and raw data. Corporations should consider whether the benefit of allowing employees access to the data in question from their own devices outweighs the associated risks. A clear policy should be adopted regarding the types of data available to employees on their own devices, and may be customised depending on the individual employee. Perhaps more importantly IT infrastructure should be geared to enforcing these restrictions and IT staff will need to understand the company's position on access to information from personal devices so that they can effectively implement those measures.

Companies will also need to consider whether there are additional legal or regulatory restrictions on accessing or using certain sensitive data, for instance medical records, financial details and personal information. Some jurisdictions limit offshore storage of certain information without the corporation specifically retaining a measure of control. In addition to the existing risks a corporation may face from its own usage of cloud based platforms and storage solutions, an employee's personal use of a public cloud based solution on their BYOD device may place the corporation in breach of certain regulatory obligations.

Data does not have to be stored directly on an employee's device. Allowing employees to store copies of data on their own device creates a risk of data leakage, and may also mean that the company does not have access to the most up to date version. Data also becomes vulnerable to loss or destruction if the device storing it is lost or destroyed. It is often preferable to store data and applications on a remote server or cloud storage system which is accessed over a secure internet connection (preferably VPN). However, as noted above, measures should be taken to ensure that only devices which have been vetted have access, for instance by restricting the IP addresses able to access the server.

Licensing

Corporations will inevitably be subject to certain licensing restrictions for certain software and services. Often enterprise-wide software will be licensed on a per device basis. In such circumstances, BYOD activities may inadvertently exceed the number of authorised and

paid up licences. As most sophisticated software vendors will embed usage auditing functionality in their products, a corporation could find itself either in breach of its licensing agreement or required to pay for a number of additional users in accordance with the licensing terms.

Security and storage

All company data should be securely encrypted, and where possible, separated from personal data stored on the device. Devices have varying levels of security, and every potential access device should be assessed before employees are permitted to use it. Allowing employees to access information through entering a password on any device should be discouraged, as the particular access device may not be sufficiently secure.

Some devices are purpose-built to accommodate concurrent personal and business use. For instance Blackberry 10 uses two separate domains so that work data remains encrypted, and the iOS version of the iPhone uses sandboxing to separate the information stored by each app. Sandboxing allows an employee to run personal and work programs concurrently, and only allows administrators access to and control over company data. If a device does not have separating features, two issues may arise. Firstly, it may be difficult to wipe the memory when an employee leaves the company whilst preserving their personal information. Secondly, as discussed below, employee privacy may be breached if company administrators seek to access company information as they will also have access to personal information. A solution may be incorporating minimum device specifications as part of the company's BYOD policy clarifying that only devices with sandboxing or similar functionality may be used as part of the regime.

A further consideration is the back-up system adopted. Many devices automatically back up all the stored information to a cloud storage system, which is linked with the owner of the device. For example android backs up most data to the user's Google Plus/Gmail account by default. The risk that a past employee may continue to access such backed information may be nominally addressed by including in the BYOD policy a requirement that device back-ups of this kind be disabled and alternate, separate and private back-up systems for company and personal data should be provided. However such disabling activities may be undone through simple and recurrent updates. To give such a BYOD policy requirement any effect an organisation may have to consider what additional measure may be implemented to ensure the default back-up systems remain disabled. Nevertheless organisations will need to consider how to temper the employee's personal usage rights over the device against the security measures highlighted here.

Cost

BYOD is frequently justified as a cost-cutting measure, however corporations should assess the true costs of implementing a BYOD policy. These include:

- Contributions to initial purchase or running costs of devices (for instance sharing the cost of phone bills and insurance);
- Increase in IT staff workload – screening devices before approving their use, monitoring data security and compliance with the BYOD policy, ensuring devices are wiped after an employee leaves the company;
- Cost of data-tracking software and additional security platforms and measures;
- Increase in unsupervised billable hours if the employee works from home (including overtime hours);
- Additional licensing costs for additional instances of software usage; and
- Potential liability and litigation cost resulting from disclosed confidential, sensitive or personal information.

In tempering these additional risks and costs against the cost cutting justifications, companies may find that in reality it is cheaper and simpler to provide employees with company devices and restrict personal device usage for business purposes.

Legal implications

Who owns and controls the device?

The employee is legal owner of the device, although the company may have contributed to its purchase price or the on-going costs of use. The company will wish to assert some rights over the device or restrict the employee's rights of use, including removing company information when an employee leaves and monitoring use of the device for unauthorised or illegal use. It has been raised that an employee's telephone number might also be considered a valuable company asset. It is advisable that the rights and obligations of each party are settled in advance through a clear and detailed use policy agreed between the employer and employee.

There are also specific legal issues with regards to ownership and control of the device. For example, in the event legal proceedings are commenced against a company an employee's personal device could be seized as part of the discovery process, interfering with the employee's ownership rights.

Strategies for data leakage

Data leakage is one of the main problems associated with BYOD. Corporations are frequently required to notify customers if their data is leaked. In order to fulfil this obligation it is necessary to track data. One risk mitigation strategy could be to employ Data Loss Prevention Software, which gives companies the ability to tag their data so admin is alerted when it flows into an unauthorised channel.

In the event of a breach of security companies should have an established policy in place to ensure that all requisite steps are taken. In particular, there may be other

bodies that must be notified when data is lost. Some of these notifications are subject to formal regulation, for instance the requirement to contact bank branches with in a certain period of time when credit card information is compromised.

BYOD usage inherently increases the existing risks information disclosure from employees generally accessing and using such information in the course of their employment. Whether it is personal data, commercially sensitive company information or otherwise confidential information, companies will need to reconsider their general processes and procedures around creating employee awareness around appropriate usage of such information and the existing security measures to address the additional risk imposed by BYOD activities.

Employers may choose to have their employees sign new terms and conditions or revise existing terms on usage. However, it should be noted that these terms and conditions cannot absolve the company of responsibility if the employee misuses company data via their device.

Use and social media policies may also need to be reformulated to take into account the use of devices for personal purposes, for instance prohibiting the employee from using the device to store illegal material or material which infringes copyright.

Employee privacy

As explained above, companies using a BYOD policy may still need to monitor employee device use. This is a different situation from when an employee puts personal information on a company device. It is to be expected that the employee will have personal information stored on their personal device, but personal devices are also expected to be private. In a number of jurisdictions,[3] employees have a legal right to privacy which must be balanced against the employer's risk mitigation imperatives to monitor their usage.

If a company has a policy of wiping devices when an employee leaves, care should be taken to leave personal information intact. In addition, the company should respect employee privacy and not access employee information when configuring or monitoring access to the device.

Intellectual property

Two issues related to ownership and transfer of title to intellectual property may also arise out of a BYOD policy. The first is whether a piece of intellectual property was created in the course of employment or outside of it. For example, a journalist employed by a newspaper who also writes a freelance blog may use the same laptop for both. If the journalist writes a blog post on a topic he had researched at work, it may be difficult to determine whether the final product is considered to have been created in his own time. The separation of formal and personal work through use of separate devices creates more certainty as to the context in which a work is created. For patents the requirement of creating an invention in the course of employment is coupled by a requirement that the employer's time and materials be used. It is uncertain what the outcome of a claim for assignment of a patent would be if the inventor had been using their personal device to create it.

Licensing

In addition to the cost issues highlighted above, where a device is used for both personal and work purposes, it is important to clarify that the manner in which installed software may be used under its licence. For example, an employee may not be permitted to use a personally-licensed version of Microsoft Office for work purposes. Licences may also not cover the situation where content is copied to or from a remote storage location, or an application is used remotely. Companies may need to consider additional licensing of such software and services to cover BYOD devices.

Client information

Finally, corporations should bear in mind that client information does not necessarily belong to the company. When providing information the client consents to its use within the company premises, but this consent may not cover use of information in all the places where an employee using their own device is able to access it. It may be necessary to obtain separate consent where information is to be accessible from an employee's personal device.

Conclusion

Despite the issues raised in this article, employers should not be deterred from allowing employees to use their own devices. BYOD has been linked to increases in productivity, employee satisfaction and business efficiency. The key is to ensure that an effective usage policy that comprehensively addresses the potential risks and costs introduced by BYOD usage is developed, adopted, implemented and enforced.

---

[1] CherylHarris, Ph.D. Chief Research Officer. Decisive Analytics, LLC, "Mobile Consumerization Trends & Perceptions, IT Executive and CEOSurvey" Final Report prepared for: TREND MICRO, INC. August 2010, http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf.

[2] Jeff Jones, BYOD: Organizations Question Risk vs Benefit, 2 August 2012, http://blogs.technet.com/b/security/archive/2012/08/02/byod-organizations-question-risk-vs-benefit.aspx.

[3] For example the United States Supreme Court has recognised that government employees have a constitutional right to privacy, whereas employees of private entities have not such protections. *O'Connor v. Ortega*, 480 U.S. 709, 716 (U.S. 1987). Employers will also need to be aware of the differing United States' state and federal statutes governing workplace communications and privacy. While the European Community generally protects the right to privacy and regulates the processing of personal data in the EC Data Protection Directive, the Directive is limited to data processing activities by private sector employees and possibly government owned businesses. However it would

not cover government employers. Furthermore member states retain the jurisdiction to legislate on a number of administrative details as well as specific statutory exemptions.