The risks of implementing 'Bring Your Own Device' in the work place

David Greenspan, Partner, McGuireWoods LLP (Virginia, US) and Andrea Ward, Senior Associate at McGuireWoods London LLP examine the main risks for organisations wishing to implement a 'Bring Your Own Device' scheme, including a focus on practical implications in both the UK and the US, and advice on what provisions to include in an effective BYOD policy

A survey in 2013 found that over 44% of organisations already allow employees to bring their own electronic devices into the workplace for work use – they implement what has come to be known as Bring Your Own Device ("BYOD") - and a further 18% were expected to follow suit by the end of 2013. Of those allowing BYOD, 61% of companies had adopted dedicated BYOD policies for their workforce detailing the general basis on which the devices may be used and, in particular, provisions as to the use and ownership of data held on the devices.

How well these policies are drafted and managed is crucial to the success of BYOD and the organisation's handling of personal data. It is not just the usability of mobile and portable devices that aids the growth of BYOD. The growth of cloud services and the availability of applications and services, such as Dropbox, Hangouts and Google+, all help users to communicate and work remotely. The challenge for businesses is to ensure that they either approve such methods, or adopt useful alternatives which meet the organistion's standards. Otherwise employees will revert to their own preferences which may not be appropriate in the specific business environment.

This article provides a summary of the necessary requirements for employers managing BYOD and employees' rights, in the UK and the US. The concept of BYOD is universal, but companies need to make sure they comply with legal requirements on data protection, privacy and employment laws, all of which can vary considerably in different jurisdictions.

UK Data Protection Act 1998

The UK Data Protection Act 1998 (DPA) contains 8 data protection principles for the management and protection of personal data. The seventh data protection principle provides that "appropriate technical and organisational measures shall be taken against accidental loss or destruction of, or damage to, personal data."

Managing the security of personal data becomes difficult when the data controller has little or no control over the devices on which personal data are processed. Where BYOD is allowed, the company will also need to understand the types of data held, where they are stored, how they are transferred (including whether there are any transfers outside the European Economic Area) and what should happen when the employee leaves the employment.

The DPA also gives employees the right to:

- access their personal data (section 7);
- prevent processing likely to cause damage or distress (section 10);
- prevent processing for purposes of direct marketing (section 11)
- compensation for the data controller's failure to comply with certain requirements (section 13)
- rectification, blocking, erasure and destruction of data (section 14).

These rights must be taken into account when considering whether to adopt BYOD in the workplace, and in the drafting of an effective BYOD policy.

In certain sectors, allowing BYOD seems like an easy decision to make; employees are happier using their own devices and productivity is usually increased.

However, where data are restricted, or governed by regulatory requirements, the take up of BYOD is much less. Professional firms of lawyers or accountants may be more cautious to approve BYOD than, say, media, or recruitment companies, but any business dealing with particularly sensitive, or regulated data needs to have stringent controls in place, and employees working for them may well show resistance to the level and nature of restrictions applied to

(Continued on page 6)

(Continued from page 5)

their personal devices.

US practice on highly sensitive data

It is especially important to appreciate the risks of BYOD when dealing with highly sensitive personal information.

In the United States, for example, the US government has put in place several mechanisms under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), to protect the transmission of Electronic Protected Health Information ("e-PHI") through the HIPAA Security Rules (45 C.F.R. § 160.103).

Organisations which utilise a BYOD system and fall under the umbrella of HIPAA (known as "covered entities") are required to put in place specific mechanisms to protect this e-PHI through their mandates.

Covered entities must perform reasonable and appropriate risk analysis as part of their security management procedures to ensure the confidentiality and integrity of e-PHI. Additionally, covered entities must implement access controls (limiting the flow of e-PHI to only authorised persons), audit controls (to record and examine access to information systems that contain e-PHI), integrity controls (to ensure e-PHI is not altered or destroyed), and transmission security controls (technical security measures that guard against unauthorised access).

While the Security Rule dictates these strict compliance requirements, the US Department of Health and Human Services recognises that covered entities range in size, complexity and capabilities and, in addition to their size and sophistication, takes the following factors into consideration when determining whether a security measure is appropriate:

- the entity's hardware and software infrastructure,
- the costs of the security measures to the entity, and
- the possible likelihood and impact of any potential risks to e-PHI.

Any covered entity utilising BYOD must be vigilant in adhering to the HIPAA Security Rules and privacy protections, and specifically must train employees on compliance requirements to protect against any reasonably anticipated, impermissible uses or disclosures of e-PHI.

As another US-based example, the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) has established a security policy intended to protect personal and official information from falling into the wrong hands. See CJIS Security Policy, Version 5.2, (Aug. 9, 2013). This policy includes the use of information exchange agreements, security awareness training, access controls, audits, and other protection methods to ensure data security.

Moreover, the Payment Card Industry Data Security Standard (PCI-DSS), provides guidance to all entities involved in payment card processing on how to establish baseline technical and operational standards in an effort to protect cardholder data. See PCI-DSS, Requirements and Security Assessment Procedures, Version 3.0 (Nov. 2013). Depending on the nature of the law practice, US employees may be governed by either or both of these policies.

Security risks

Some companies reduce their exposure to risk by choosing not to allow BYOD for employees, save for those who are providing 24/7 support (such as the information technology function), or employees whose job it is to be 'mobile' (such as sales staff, or case workers).

Even in those cases, it is still vital that specific rules on data protection and security are applied. Unfortunately, it is an inevitable reality that people are careless and take short-cuts when using technology, potentially exposing the business and customers to additional risk.

The biggest security risks in connection with BYOD are considered below.

1. Unknown third party access via mobile applications ("apps")

This can happen when employees are using their devices in an open Wi-Fi zone, or when they download and install apps for their personal use. The risk is that unregulated third parties may be able to access company information, personal, and sensitive personal data on the device.

Companies should consider blacklisting certain apps, but as more and more are created each day, they may decide instead to adopt a bring-your-own-application strategy. This would involve using Mobile Application Management (MAM) software to separate company and personal data on the device.

2. Compliance issues

Data mapping is essential for dealing with any compliance issue, as is having a clear BYOD policy and procedures for handling regulatory requests and audits. The steps taken by the company to achieve this should be documented by compliance teams.

3. Lost and stolen devices

Mobile devices are more susceptible to the risk of being lost or stolen than PCs, simply because they are smaller and portable. Basic security measures, such as the 4 digit PIN, may be insufficient protection in these circumstances, so companies should insist upon passwords with a prescribed higher level of security for users of these devices.

4. Employees

Even when they are happily employed, employees can be a source of risk, but following termination of employment managing them becomes much harder. Personally owned devices holding company owned data need to be surrendered, so that the data can be removed, to prevent the employee accessing them post-employment and potentially leaking information to rival organisations.

5. Difficulties tracking data

The best way to manage data on personal devices is to stipulate what information an employee is allowed to access and store on the device. The alternative is to use a content security tool, which includes discovery and monitoring features to protect against data loss, whether on network or mobile devices.

Although managing data in this way may be seen as quite troublesome, companies should try to minimise the risk to the business by engaging their employees and working with their IT departments to choose and test a number of devices, apps and services which work best for the business, whilst remaining within sensibly drawn IT guidelines.

Monitoring employees

Employees should understand that by using their own devices for work, their employer may end up processing more of their personal data and sensitive personal data, as well as personal data belonging to the employee's friends and family. Personal emails, photos, videos and other information will be stored on the employees' own device, all of which should be protected by the data controller.

The employees' access to websites and social media will also fall under the data controller's remit. This is another potential area for concern, both in terms of employee privacy and monitoring, but also in relation to the employer's reputation and relationships with customers.

There are many examples of recent UK Employment Tribunal cases where employees have been dismissed for posting content online in breach of their employer's policies. In investigating such misconduct, employers may be able to access publicly available information from social media sites that have not been made private by the employee. Employees whose personal emails and Facebook accounts have been accessed by their employer have sometimes sought to plead a breach of human rights under the European Convention on Human Rights (ECHR) and the UK Human Rights Act 1998 (HRA). In particular, the rights to respect for private and family life, to home and correspondence (Article 8) and to freedom of expression (Article 10) have been cited. However, these arguments have generally failed where the employee has not taken steps to limit access to his online content, where the employee has forwarded offensive emails on to third parties, or where the employee has posted information which is visible to work colleagues.

For example, in *Crisp v Apple Retail (UK) Ltd ET/1500258/11* an employee dismissed for posting derogatory comments about his employer on Facebook was found to be fairly dismissed, since Apple had made it clear to all employees that protecting its image was a core value. When considering whether the employee's right to privacy had been infringed, the Employment Tribunal determined that there could be no reasonable expectation of privacy, even though his page was limited to 'friends', because he could not control how his comments could be copied and passed on to others.

> ***"Employees should understand that by using their own devices for work, their employer may end up processing more of their personal data and sensitive personal data, as well as personal data belonging to the employee's friends and family"***

In the United States, an increasing number of states have proposed or passed laws prohibiting employers from accessing employees' or applicants' social media account information.

Many of these laws prohibit employers from requesting or requiring employees or applicants to provide their usernames or passwords for their personal social media accounts or from requiring an employee or applicant to access their personal social media accounts in the presence of the employer. They also prohibit an employer from retaliating against an employee or applicant who resists such an unlawful request. To date, at least twelve states have enacted legislation of this sort, including Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, Oregon, Utah, and Washington.

A right to privacy?

Of course, employees also have statutory employment rights as well as rights under their contracts of employment, but a right to privacy at work is not absolute. Employers should inform employees that they can have no expectation of privacy in the workplace when it comes to their use of company systems and equipment, including IT and telephones.

If employees are permitted to use company owned equipment for personal matters, they must understand and accept that this use should be limited. For example, any personal emails should usually be marked as such.

BYOD obviously complicates this arrangement, since the devices being used belong to the employee. The expectation of privacy will be greater, but employers should maintain their stance on the lack of expectation of privacy, especially if personal data will be held on company equipment or systems. It will be necessary therefore to remind employees that if they send emails on their own devices via the company server, the data will reside on the company server and may be accessible to the employer.

For the company, this is not about intruding on the privacy of its employees, but about maintaining the security of data, protecting customer/

(Continued on page 8)

(Continued from page 7)

client information and guarding against reputational risk.

The company will also need to protect its confidential information and intellectual property. This is often covered by the terms of the employment contract, through the use of restrictive covenants and confidentiality clauses, but when implementing BYOD it is sensible to revisit these terms and ensure they are sufficiently robust.

BYOD policy – practical pointers

When considering a BYOD policy, employers should review their existing data processing requirements and business needs. Practical questions need to be asked, such as:

(a) what is the nature of the data that will be used and/or stored on the device? (is it 'personal data', as defined by the DPA, or 'Personally Identifiable Information' (PII)?;

(b) who has access to the data?;

(c) where does it reside (will it be transferred outside the EEA and, if so, how?);

(d) who will pay for the device (the employee, or the employer)?

Establishing a BYOD policy before introducing BYOD into the work place can benefit both parties. One of the aims of a good policy is to educate employees on the data protection needs of the business and to create an understanding of the limitations the business may impose on BYOD.

The UK data protection authority, the Information Commissioner's Office (ICO), has developed its own guidance on BYOD, focusing of course on the requirements of the DPA and the data protection principles. (The guidance is available at http://www.pdpjournals.com/docs/99001)

The immediate concern with BYOD is the fact that the mobile device used to process the data is owned by the user, rather than the data controller. Having a clear policy and enforcement through the employment contract and other procedures (such as the disciplinary procedure) shapes the reasonable expectations of employees.

The ICO recommends:

- implementing and maintaining an Acceptable Use Policy, to provide guidance and accountability of behaviour;
- considering the need for a separate Social Media Policy;
- being clear about which types of personal data may be processed on personal devices and which may not;
- including all relevant departments (including IT and HR) and the employees in the development of the policy;
- using a strong password to secure devices;
- using encryption to store data on the device securely;
- making sure that users know exactly which data might be automatically or remotely deleted, and under what circumstances; and
- maintaining a clear separation between the personal data processed on behalf of the data controller and that processed for the device owner's own purposes, for example by using different apps for business and personal use.

Having formulated a BYOD policy, this then needs to be properly communicated to employees. This entails rolling it out to staff, providing a copy or link to the policy, and making sure that employees are properly trained on the rationale underlying the policy, as well as its precise content and its application.

Once in place, the policy needs to be kept under review, to ensure it remains relevant in the business environment and takes on board developments in technology and working methods.

It is important that the workforce concerned understands and consents to the terms of the policy, particularly those provisions concerning access to personal data where this is necessary to recover company data, those concerning the employer's right to update security on devices remotely, and terms governing the employer's right to wipe data if the device is lost or stolen.

Further, a policy is only useful if it is actually followed in practice. Compliance management should be tasked with ensuring that the BYOD policy is not only implemented effectively but that there are checks in place to ensure that employees adhere to it.

Andrea Ward,
McGuireWoods London LLP
David Greenspan
McGuireWoods LLP
award@mcguirewoods.com
dgreenspan@mcguirewoods.com