6 June 2012

"Bring Your Own Device" Brings its Own Challenges

By Susan McLean and Alistair Maughan

The consumerisation of IT is the growing trend for information technology to emerge first in the consumer market and then drive change in the industry generally. One of the most dramatic impacts of this shift is a rise in so-called "bring your own device" strategies in both public and private enterprises.

In the past, the functionality of your work computer and phone tended to be streets ahead of what you used at home. Remember the days when employees would show off their work PDAs, smartphones and laptops as perks of their job? These days, increasing numbers of employees have better access to technology at home than they do at work, with personal devices and apps that are user friendly and convenient in ways that their work equipment and systems are not. Employees also wish to work differently (working remotely, outside regular hours, on the weekend, on vacation, etc. are becoming the norm) and users want their business tools to enable this change. Employees also want to limit their need to carry and manage multiple devices. The answer? Bring your own device to work.

In this Alert, we highlight some of the issues that organisations need to consider when formulating policies and procedures designed to cope with the transition to a bring your own device strategy.

Understandably, IT departments have always been keen to retain absolute control over the office environment and therefore resisted putting any non-company (i.e., non-trusted) devices on the company network. However, IT departments are now under increasing pressure to support – and, indeed, encourage – the use of personal devices for work purposes.

IT departments are embracing the trend on the basis that it can help save costs and change the perception of the IT department as the department of "No". It has also been shown that employees are more satisfied and productive when they have more control over what tools they can use. Therefore, it is said to be good for business too, although some commentators argue that the perceived benefits of "bring your own device" (or "BYOD") have been overplayed.

Either way, this is not a passing fad. The analysts TechMarket View have recently reported that, in the UK alone, the BYOD market will be worth £2 billion to UK software and IT services suppliers over the next five years; with five million employees having adopted BYOD by the end of 2011 and an anticipated rise to around 9.5 million by 2016 – an increase of 80%.

The BYOD trend leads to considerably more complexity for IT departments in terms of how they manage and support end users. Organisations also need to grapple with the potential legal and regulatory issues raised by employees using their personal devices for work purposes. Unhelpfully for organisations in regulated industries – especially financial services – regulatory bodies have been slow to react and provide guidance on how BYOD applies in those sectors.

DATA SECURITY

Data security and the risk of data "leakage" has always been a key concern for organisations. The use of company phones, laptops and other mobile devices increases that risk – because, by their very nature, these devices are more easily lost, stolen and accessed. The risk is further compounded when employees start using their personal devices for business purposes as part of a BYOD strategy.

One of the key challenges in designing a strategy to implement BYOD successfully is how to ensure data security on non-company equipment – primarily as a result of it being harder to keep track of where data may actually be, how data is protected and the difficulty of policing the use of personal devices.

In addition, organisations now need to grapple with the different scenarios raised by their employees' use of corporate data in different applications, such as what happens if an employee puts corporate data into a non-corporate supported location (*e.g.*, an application like Dropbox – which is becoming increasingly popular for both personal and work purposes). These types of third party application may not have been vetted by IT or the company's in-house legal team and their terms and conditions may allow the third party extensive rights in terms of the data stored and/or have wide exclusions of liability for data loss. This is more likely to be the case where the applications were originally developed as consumer tools and not intended to store sensitive corporate data.

It is probably not practical these days to take the policy position that sensitive corporate data cannot be stored on personal devices. Even if an organisation takes this position, how likely is it that an employee will actually comply? Many organisations approach this issue by understanding that users, and the content that they generate and consume, vary in the level of information sensitivity depending on their functional roles and needs. An organisation needs to take a nuanced approach to take account of individual users and the types of data accessed on their devices.

It is not simply a question of analysing how to ensure compliance with existing security policies – it may be that different security policies are required to replace existing security controls that simply do not work in the context of personal devices. Companies must understand that employees tend to value convenience over security and take this into account when formulating security policies – if you make the policies too restrictive, employees will simply ignore them or find a way to circumvent them.

Organisations also need to consider up-front the appropriate corporate response if a security breach occurs in relation to a personal device. Most organisations will wish to deploy remote wipe capability, but they need to consider the HR impacts of such a strategy, as discussed further below.

DATA PROTECTION AND PRIVACY

In addition to data security generally, the data protection and privacy implications of a BYOD strategy are considerable. Most countries have laws specifically dealing with the use and storage of personal data and requiring organisations to protect and ensure against the implications of loss of that data, together with rules regarding the retention and destruction of personal data. Compliance with data protection laws becomes significantly harder if the device on which that data is stored is not owned or controlled by the enterprise itself.

Of course, it is not just a question of compliance with data protection laws (and the legal penalties for failing to comply) – there can also be huge reputational issues if a company is shown to be poor at safeguarding personal data.

OWNERSHIP OF DATA AND MATERIALS

There is also the question of who owns the data stored on a personal device. In terms of corporate data stored on an enterprise-provided device, the question of data ownership is pretty straightforward. Similarly, it is generally clear cut that any materials created by an end user using an enterprise-provided device will be owned by the enterprise because they will have been created in the course of the end user's employment.

However, the position is less straightforward when the employee uses a personal device for business purposes. To what extent is there a split in the ownership of data between the employer and the end user, depending on the nature of the data? An enterprise would not expect to own an employee's photos or personal files, but what about an employee's contacts?

Also, when an end user creates materials using a personal device, who owns the intellectual property rights ("IPR") in that material? In some situations, it may be clear whether or not the material was created in the course of the end user's employment, but in others it may not be so clear – for example, if a software developer uses his personal computer to create new code not at the request of the company but as a personal project, should his employer own the copyright in that code? Typically, a company will require that all IPR created by an employee (whether at work or outside work) is owned by the company but in this context it is even more important to ensure that this issue is covered appropriately in the employee's terms of employment.

LICENSING

The licensing implications of a BYOD strategy are often overlooked.

Organisations often forget to check, for example, the scope of their Microsoft licences within the enterprise when employees use personally owned mobile devices or laptops to access a virtual desktop, either from home or the office. Such use may not be permitted within the existing licence terms or may incur additional licence fees (as some licences may be granted on a per device basis, rather than per user basis).

Licensing issues will need to be considered carefully when formulating a BYOD strategy to ensure that the organisation remains compliant.

LEGAL AND REGULATORY COMPLIANCE

A major risk for any enterprise that allows non-standard devices in the workplace is how to ensure and demonstrate regulatory compliance. This is a particular challenge for regulated industries such as healthcare, pharmaceuticals and financial services. But there are other laws, such as the U.S. Sarbanes-Oxley Act (which imposes an onus on public companies to closely monitor financial and accounting activities) where compliance becomes more difficult depending on the more diverse the population of IT devices in use.

In considering regulatory compliance, there are several key issues that should be addressed. These include where the data is stored, what the implications of that storage are and what happens if a device is lost or stolen or when employees leave the company.

INDUSTRY STANDARDS

There is also the question of how to ensure compliance with applicable industry standards (for example ISO 27001, PCI:DSS etc.). Organisations will need to carefully consider how to incorporate non-corporate assets into applicable risk management strategies.

INVESTIGATIONS AND LITIGATION

Employers will clearly have less access to data stored on a personally owned device, but may need or want to obtain access for the purposes of investigations or litigation. Organisations need to ensure that their employees agree to make their personal devices available if the organisation reasonably requires them for investigation purposes or they are subject to a discovery request in the context of litigation affecting the company. (Of course, even if an employee signs a document promising to give access to the device in such circumstances, that doesn't necessarily mean that a court will enforce that agreement.)

INSURANCE

An issue that is sometimes overlooked is that of insurance. Organisations will need to check that their data security/cyber risk insurance covers devices owned by employees to ensure that they are not exposed in the event of a security breach. Any insurance policy which only covers devices owned by or leased to the organisation will need to be revisited.

EMPLOYEE ISSUES

Many of the issues brought up by BYOD involve compliance with HR law, largely because many of the typical corporate policies that exist in the workplace today were developed in a world before BYOD. Some of the issues that will need to be carefully considered when formulating a BYOD strategy are as follows.

- Who should own the device? Ownership will impact how the company approaches some of the risk and liability issues relating to the device.
- Who should be responsible for the cost of personal devices used for work purposes? In some countries, the law requires an employer to provide all of the tools that an employee needs to carry out their job. Could this result in the employer having to reimburse an employee's costs?
- Should the BYOD programme be optional or mandatory? Typically, it is considered best to make it optional for employees to use their personal devices for work purposes, by allowing them to choose to use company-issued devices instead. This helps show that an employee's decision to use a personally owned device (and to agree to the related terms and obligations imposed upon the employee in relation to its use) was voluntary.
- If employees are only allowed to choose from a limited number of devices (which, for example, do not cater to employees with special needs due to disabilities) or the BYOD scheme is only open to certain types of staff (e.g., full-time staff only), the company will need to consider whether there could be a risk of discrimination claims.
- Employers need to consider how responsibility for security is shared. Who is responsible for anti-virus updates, etc.? At a minimum, you would expect an employer to mandate certain appropriate security measures to be enabled by an employee before being able to use their personal device for work purposes. Policies also need to be very clear as to the procedure the employee must follow in the event of a lost or stolen device.
- Employers also need to consider what happens if the device fails. Whose responsibility is it to fix or replace faulty devices?
- The question of data protection and privacy compliance is not just an issue in terms of protecting customer data. It is also a key issue in terms of the personal privacy of employees. It is worth noting in this context that there are some countries where storing business data on a personal device may not even be permitted under applicable privacy laws, so a global BYOD programme may not be appropriate – it is likely to need tailoring to meet regional requirements.

  - A number of data protection and privacy issues will need to be considered up-front. For example, to what extent should the employer have access to an employee's personal data stored on their device? Can data be appropriately segregated between corporate and personal data? Also, what kind of monitoring and audit access is going to be appropriate in terms of a device which is used for both personal and work reasons? To what extent is monitoring of an employee's personal device even permitted under applicable privacy laws? What about unintentional consequences – for example, that the organisation may, in effect, be able to track an employee's whereabouts, both during and outside work hours (using GPS and WiFi location data)?
  - Another key issue to consider is to what extent should the employer be entitled to remotely wipe, brick or block devices in the event of a security incident? Although it is possible to wipe company data only where it is segregated from other data in an encrypted "sandbox", some remote wiping software will not just wipe the company data, but all data on the device (including, for example, any personal photos and music files).
  - In terms of data protection and privacy, simply including clauses in an employee's contract of employment is unlikely to satisfy the requirements of applicable law. It will be important to bring any conditions that may be considered onerous to the attention of the employees. Particularly in the case of wiping, it is essential that employees are informed in the clearest terms of the potential risks and that employees sign up to appropriate clear, voluntary and express consents/waivers.

- Employers also need to consider to what extent they should restrict anyone except the employee from using the device (e.g., should they prevent an employee's family members from being able to use the device).
- To what extent should the employer control the use of apps? A company may wish to blacklist particularly risky apps. What about apps that may be considered to affect productivity – should an organisation try to block these or restrict their use during working hours?
- To what extent should an employer control the use of a camera on a personal device in the workplace?
- How does an employer deal with the potential consequences of different personnel using different devices, particularly if this makes certain employees more productive than others?
- To what extent can an employer control the use of a personal device by an employee? To what extent is an employer liable if an employee breaches copyright law by carrying out illegal downloads etc. on their device? What about if an employee accesses unlawful or inappropriate material?
- If an employer has existing restrictions in place regarding the use of social media, are these really going to be enforceable on a device used for both work and personal purposes? Employers should also consider to what extent they are able to place restrictions on how employees use their personal device during work hours.
- Another key concern is how to deal with corporate data that is stored on personal devices when an employee leaves the organisation. There is always a risk that a departing employee, particularly when leaving to join a competitor, may be keen to bring corporate data to their new job. If the employee is using company systems, any attempt to do so can usually be identified, but if the information is stored on a personal device this will be more difficult to police.
- What are the implications for work-life balance? Across most of the EU, there is now a 48 hour limit on a working week, but how does that apply when studies show that 66% of people read e-mails 7 days a week and expect to receive a response the same day, and 61% of people continue to check e-mail while on vacation? The likelihood that employees will send and receive e-mails outside of work or office hours is clearly increased where the employee uses a personal device for work purposes (e.g., an employee may decide to leave their work phone at home whilst on vacation, but an employee won't leave a personal phone at home).

- On a related note, in the U.S., organisations need to carefully consider whether the use of a personal device for work purposes could impact an employee's non-exempt status under the Fair Labor Standards Act and the potential consequences. Employees may be considered "working" if they send or receive e-mails outside of work or outside of office hours, triggering the potential for overtime payments. As above, this risk is greater where the employee is using a personal device for work purposes.
- A final key consideration is how to inform, educate and train employees concerning the implications of using their personal devices for work purposes. Employees need to be reminded that all company policies continue to apply to their conduct when using a personal device for work (including policies relating to confidentiality, etc). It is important to get this right as arguably the best defence against data security breaches is well informed employees.

CONCLUSION

Organisations cannot resist the consumerisation trend. It is not a passing trend, but here to stay – and if an enterprise tries to resist it, increasingly tech-savvy employees are likely to find a way to circumvent the restrictions imposed.

The key is to try to take a pragmatic approach and put in place appropriate policies to try to accommodate employees' desire for increased flexibility and mobility, whilst limiting the potential risks created by such an approach. These policies will need to be reviewed regularly and evolve over time to keep up-to-date with changes in technology and applicable law.

BYOD is not just an IT department issue but also a business issue and organisations need to ensure that they do not simply focus on the obvious IT risk and issues such as data leakage, etc., but collaborate with all relevant stakeholders and consider all relevant legal, HR and finance considerations. We all want to work "smarter", but this should not be at the expense of working safely.

Contact:

Susan McLean
+44 20 7920 4045
smclean@mofo.com

Alistair Maughan
+44 20 7920 4066
amaughan@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for eight straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.