What lawyers need to know about BYOD: Bring Your Own Devices

Speedread
Here's a checklist and guidance to deal with the increasing legal and reputational problems with staff using their own mobiles, iPads, etc.

Checklist

1. Has the IT Department categorised data and associated risk?
   a. what type of data is held;
   b. where data may be stored;
   c. how it is transferred;
   d. potential for data leakage;
   e. blurring of personal and business use;
   f. the device's security capacities;
   g. what to do if the person who owns the device leaves their employment; and
   h. how to deal with the loss, theft, failure and support of a device.
2. What types of devices are used and permitted?
3. Any specific legal issues applicable to the organisation such as legislation or onerous contracts?
4. Any specific reputational concerns?
5. What level of protection is required, based on what is reasonably required for each category of data?
6. What technical solutions are being used and are they adequate for each category of information?
7. Are adequate corporate policies in place taking account of
   (a) employment law; and
   (b) binding buy-in by the employee or contractor?
8. Are there systems to monitor what is happening and are they implement?

The list at (a) to (h) is quoted from the *ICO report, Bring your own device (BYOD) Guidance*, referred to in the article.[1]

November 2013

There's little turning back the tide on organisations allowing their people to access the network and hold data on employee's and contractor's own devices such as mobiles, personal laptops, USB data sticks, and so on. Surveys point to a number of advantages including staff efficiency. But without the rigour usually found in company IT systems, this throws up the risk of unencrypted data going public, with legal and reputational consequences.

BYOD can open up security gaps in best practice internal IT systems. BYOD is a big issue for IT people and IT security specialists so they're likely to understand the lawyers getting involved.

The challenge is usefully set out by Nigel Miller in his October 2013 article in Computers & Law, BYOD:Win-win or Zero-sum Game?, as follows:

> "*The big risk factor for organisations with BYOD schemes is the loss of control over the devices being used. This leaves organisations in the dark in terms of knowing what data are stored on the devices or in the cloud, what data security vulnerabilities there may be and how to secure access themselves. This potential loss of control opens the door to a host of privacy and data security issues.*
>
> *For the employee who has to share control of the device with an organisation looking to protect its data assets, he could be forced to allow the organisation access to his own equipment, often without compensation, and face the risk that the organisation could access his private information, lock him out of the device and wipe his data.*"

What are the legal issues?

There are plenty of contract, tort and statutory reasons why this is legally a problem area – on top of reputational risk. A convenient benchmark for assessing legal obligations[2] for both commercial and for personal data, is what the Privacy Act has to say:[3]

> An agency that holds personal information shall ensure—
>
> (a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—
> (i) loss; and
> (ii) access, use, modification, or disclosure, except with the authority of the agency that holds the information; and
> (iii) other misuse; and
>
> (b) that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.

Essentially, the organisation must ensure the information is protected to a standard that is reasonable in the circumstances, including taking reasonable steps, when third parties including staff and contractors get information, to prevent unauthorised use or disclosure of the information. This is not necessarily about 100% fail-safe security protection. It is about the organisation still being largely responsible for compliance over an employee's and contractor's BYOD device.

What is needed obviously depends on the level of sensitivity of the information. Therefore an organisation may, for example, stop highly sensitive information being used over BYOD, but take a more relaxed approach to other information.

What should the lawyer do?

To the extent BYOD access and data holding is permitted, the lawyer should get reassurance around two main categories, based on an adequate assessment of risk in the context of the organisation's specific circumstances:

1. Are there adequate technical requirements in place? That could include restricting BYOD access to certain information in the network, and mobile device management solutions such as encryption, monitoring corporate policy implementation, configuring settings and remote wiping and locking of lost or stolen devices.

2. Are there adequate policies in place, accepted by staff and contractors? That would include:

   (a) Material educating staff and contractors on the risks and how to manage BYOD devices (this can overlap with policies and material on related risks such as cloud computing and WiFi);
   (b) Staff/contractor obligations and acceptable use;

(c) The extent of the organisation's right to access and monitor the device and its use (clearly defined to meet, for example, employment law requirements);

(d) The consequences if there are breaches.

We've briefly summarised the approach in the checklist with this article.

Some more detail

A useful source is the material produced by the UK equivalent of the Privacy Commissioner, such as its report, *Bring your own device (BYOD) Guidance*.[4]

Summarising some of that office's key points:

- *"Be clear with staff about which types of personal data may be processed on personal devices and which may not.*
- *Use a strong password to secure your devices.*
- *Enable encryption to store data on the device securely.*
- *Ensure that access to the device is locked or data automatically deleted if an incorrect password is input too many times.*
- *Use public cloud-based sharing and public backup services, which you have not fully assessed, with extreme caution, if at all.*
- *Register devices with a remote locate and wipe facility to maintain confidentiality of the data in the event of a loss or theft."*

1. http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/byod

2. Assuming no additional obligations such as specific statutory issues for the organisation or high contractual obligations.

3. Privacy Act 1993, s 6 (Principle 5).

4. http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/byod

Wigley+Company
PO Box 10842
Level6/23 Waring Taylor St, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com