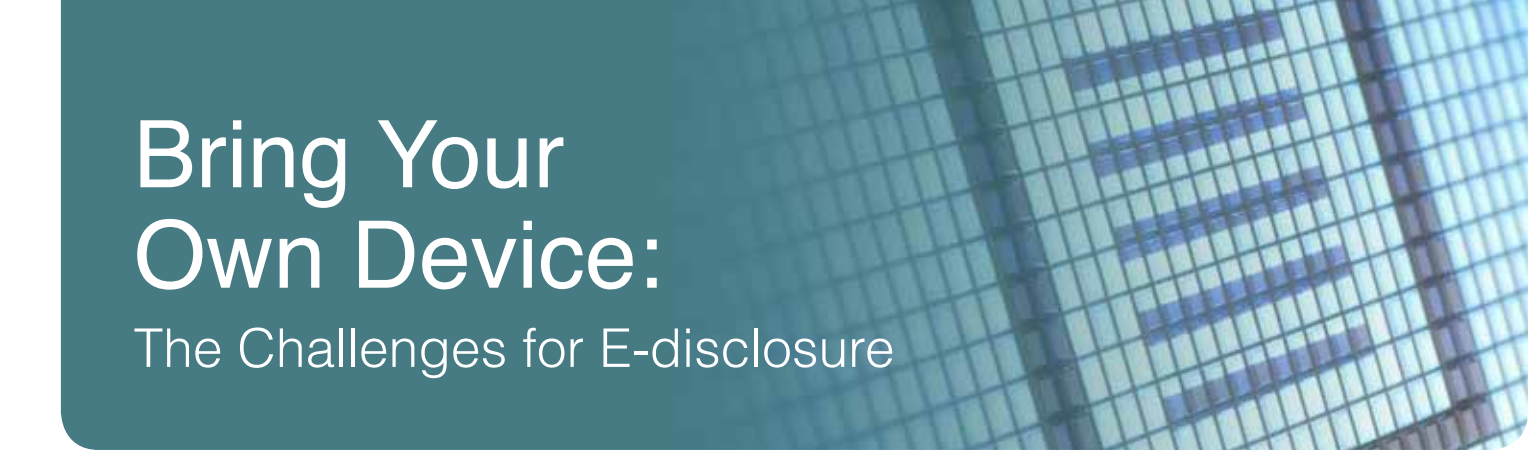
Bring Your Own Device:

The Challenges for E-disclosure



The phrase 'Bring your own device' (BYOD) is arguably the latest technology buzzword, representing a growing trend that has potentially far-reaching ramifications for law firms and chambers. BYOD refers to the practice of allowing employees to bring their own personal mobile devices such as laptops, tablets, and smart phones into work, and to use them to access privileged company information and for other work purposes.

Cost Saving and Convenience

Such is this trend for BYOD that legal organisations need to embrace its benefits. Many believe that permitting employees to bring their own devices to work can aid productivity and morale, and enhance a business's reputation for flexibility. Resisting BYOD now appears to be futile - according to a recent global survey, 80% of all employees will be allowed to connect their own device to corporate networks for work purposes by 2016.

However, the proliferation of BYOD means law firms and other legal organisations must prepare for the risks they present to potential litigation, particularly in the context of e-discovery. The Information Commissioner's Office (ICO) recently published BYOD guidance1 for data controllers, urging them to consider the potential risks of enabling employees to process personal data for which they are responsible on their own devices.

Key Risks

The technical and legal issues around BYOD are particularly complex, due to both their relative infancy and rapid proliferation, and to on-going advances in technology. Critically, law firms need to understand that whilst the legal responsibility for information stored on an employee's personal device rests with the firm, control is transferred to the employee.

This means it is for the employee to take appropriate steps to:

- use a secure password
- install appropriate anti-virus software;
- wipe the device before selling or disposing of it; and
- comply with appropriate obligations placed on employees in relation to BYOD.

Mitigating Risks and Implementing Policies

Organisations adopting BYOD must have processes and procedures in place that can ensure access to mobile devices in case of future investigations/ litigation - or face the prospect of slower, more costly e-disclosure.

Law firms who have not already done so should conduct a risk assessment addressing the types of information likely to be held on BYOD, any specific legal or regulatory obligations and to consider the various technical solutions available. There should be clear emphasis on security guidance for employees (for instance, informing the employer promptly if a device is lost or stolen).

Court rulings on e-disclosure issues are relatively recent because of the nature of the technology involved, and it's important to note companies have had to pay costs for failing to comply with their obligations. This means law firms and chambers must pay close attention to e-disclosure requirements to protect their clients' financial interests.

BYOD and Disclosure

The definition of 'documents' to be disclosed under the CPR extends to electronic documents. 'Documents' includes any document held in electronic form, and this is as far-reaching as to include documents stored on portable devices such as memory sticks and mobile phones, servers and back-up systems, as well as documents that have been deleted. It also includes an electronic representation of a paper document[2].

As Elizabeth Wilkinson of Panonne says: *"From a litigator's perspective, the apparent increasing introduction of BYOD policies by businesses will undoubtedly make the process of e-disclosure more difficult, more time consuming and thus more costly. The latter point is of particular concern in the post-Jackson era of the court scrutinising costs budgets and the parameters of each stage in the litigation."*

The convenience to the user and the benefits to a business are tangible, but the e-disclosure implications for litigators are not necessarily so evident. An initial issue is whether a party will readily hand over the relevant device when required. And so, warns Wilkinson, the first headache for litigators and their clients will be *"securing access to the devices in order to retrieve and secure information required for litigation".*

She adds: *"Third party disclosure orders may be required, whereas if the devices are company owned property it is usually a more straightforward request for the return of company property. This all takes time and money."*

If and when a BYOD is handed over, the relevant information stored in it needs to be identified and extracted. However, depending on how many devices need to be obtained and what (and how much) information needs to be

> From a litigator's perspective, the apparent increasing introduction of BYOD policies by businesses will undoubtedly make the process of e-disclosure more difficult, more time consuming and thus more costly. The latter point is of particular concern in the post-Jackson era of the court scrutinising costs budgets and the parameters of each stage in the litigation."

accessed, litigation practitioners may face a herculean task in obtaining/ by-passing passwords and dealing with the different types of file systems and storage methods.

Additionally, data formats and operating systems on smartphones and other devices can differ from those on traditional PCs, which can put an expensive snag in a company's normal e-discovery processes. Skilful techniques are employed by professional litigation support companies such as Legastat to extract evidence from mobile devices that may be highly relevant in the course of litigation.

Reasonable Search

Although electronic discovery is potentially complex, the obligation on a litigant is only to conduct a 'reasonable search' for documents. How the issue of reasonableness is assessed depends on the circumstances of a particular case - for instance, the numbers of documents and devices involved, the nature of the proceedings, and the significance of any document which could be located, and the potential costs implications.

Wilkinson says: *"The remit of e-disclosure experts will have to be expanded to advise on, and then to provide, a solution or solutions, fully costed in advance for the case budget, to the issues arising such as different ways of storing data on such devices and in different formats. The searches for data will have to be particularly careful as company data and the device owner's personal data may be mixed.*

"BYOD policies seem to underline the need to narrow the disclosure exercise as much as possible by careful thought before extensive searches are carried out and masses of data reviewed as supported by Jackson LJ."

How can Legastat help you?

Legastat is at the forefront of helping organisations with their e-disclosure challenges. We have the tools and resources and, critically, the technology to help you with the challenges to litigation presented by BYOD. We are proud to be part of the Government framework for Electronic Disclosure Services and Hard Copy review services for government (RM924). In addition, we have access to expert computer forensic experts who keep pace with the fast-moving developments in the dynamic mobile device market and how mobile devices work.

Whether your requirements relate to small e-disclosure projects or large-scale electronic evidence involving multiple mobile and other devices, we have the technological strength to work on your behalf within the CPR and within budgetary restraints.

[1]http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/~/media/documents/library/Data_Protection/Practical_application/ico_bring_your_own_device_byod_guidance.ashx

[2]http://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31/pd_part31b

About us

Legastat are experts in reprographics and specialist litigation support for the legal sector.

Located in the heart of legal London we've been trusted to deliver a professional and efficient service since 1953.

Top law firms, corporations, government agencies, small law firms and sole practitioners rely on us to meet their litigation support and disclosure obligations on time, accurately and cost-efficiently.

At Legastat we put our customers' needs, quality and confidentiality at the heart of everything we do.

We are proud to be part of the government framework for Electronic Disclosure Services and Hard Copy review services for government (RM924).

Contact

Carey Street office
57 Carey Street,
London, WC2A 2JB

Telephone
0800 064 0204

Email
info@legastat.co.uk