With the proliferation of smartphones and tablets in the workplace, employers are struggling with a range of potential legal issues that stem from the blurring of the line between business and personal uses.

Mixed business and personal use of devices can allow businesses to cut costs, drive innovation and boost employee satisfaction. Yet, many of the very features that make portable devices so appealing – data storage, computing power, portability, audio and video recording, location tracking and wireless connectivity – also raise challenges to legal compliance and the protection and balancing of both employee and organizational interests.

Businesses tend to approach shared personal and business use of electronic devices in one of two ways. Under the Corporately Owned, Personally Enabled (COPE) model, employees are permitted to use employer-supplied devices for both work and personal purposes. In a Bring Your Own Device (BYOD) environment, employees are permitted to use their own devices for business purposes, which often include access to corporate networks, email accounts and document sharing platforms.

Whichever approach is undertaken, businesses need to be aware of the legal issues and take steps to minimize the associated risks.

**Liability**
Mixed use devices can challenge an organization’s ability to protect its own commercially-sensitive information, as well as sensitive third party information that it is legally obligated to keep confidential.

**Security**
Ensuring the security of data that may be accessed through or downloaded to an employee device is a prime concern with respect to privacy law compliance, protecting commercial interests, and other legal obligations of confidentiality. Where there are weak controls (or none at all) on the ability of employees to download and store sensitive information on portable devices, there is a significant risk of unauthorized access or disclosure.

**Confidentiality**
Mixed use devices can challenge an organization’s ability to protect its own commercially-sensitive information, as well as sensitive third party information that it is legally obligated to keep confidential.

**Privacy**
When permitting mixed use of mobile devices, companies must ensure compliance with applicable privacy and data protection laws for both customer and employee data, including ensuring that personal information is used only for the purposes for which it was collected, that individuals are permitted access to information about them and that personal information is protected by appropriate security safeguards.

**Electronic Discovery**
Storage of records and potential evidence on employee-owned devices can raise obvious headaches in a litigation context, where BYOD programs can add significant complexity to the discovery process and put companies at risk of not meeting discovery obligations.

**Employment Issues**
Mixed use mobile devices can also raise significant challenges in the workplace, including potential liability for additional compensation for after-hours work due to expectations of 24/7 availability. Given the portability and audio/video capabilities of many devices, they can also lead to increased employer risks when employees use devices to post discriminatory and harassing material on social media and other platforms. Workplace investigations of misconduct can be hindered by difficulties with employer access to logs and data that are stored on an employee’s own device and significant privacy issues are raised by the monitoring of employee owned devices.

See reverse for tips on managing BYOD and COPE.
Managing BYOD and COPE

There are many effective mitigation strategies that organizations can pursue to protect their interests, while allowing greater employee freedom and flexibility:

- **A range of technical solutions is available**, including Mobile Device Management applications that allow for varying degrees of protection and control over employee devices, including restricting the installation of software/applications, enforcing password protection and remote locking and “wiping” of devices.

- **Perhaps most importantly**, organizations should clearly communicate expectations and policies to employees, and obtain at least their implicit consent. Policies should explain how significant events will be handled, including the loss or theft of a device and termination of employment. In particular, employees should be advised of how BYOD policies might affect their reasonable expectation of privacy and set out the circumstances in which access rights may be restricted or stored data erased.

- **Risk can be further minimized** by training employees to be security savvy and implementing - and rigorously enforcing - clear policies for the acceptable use of mixed used devices, including data preservation and retention requirements. Employees should also be aware of the consequences of non-compliance with BYOD policies.

---

**About Stikeman Elliott’s Communications Group**

Stikeman Elliott’s Communications Group consists of partners and associates drawn from the firm’s domestic and international law offices possessing expertise in telecommunications and broadcasting law and complementary legal disciplines, including competition, corporate and commercial, and copyright. The Group is able to draw upon the particular strengths of each of its members in responding to clients’ needs. This ensures that our clients receive legal services tailored to their specific needs in a timely and cost-effective manner, regardless of the complexity of the issues or the size of the particular transaction.

For more information, please contact your Stikeman Elliott lawyer or David Elder at (613) 566-0532 or delder@stikeman.com. David practises communications, competition and privacy law in the Ottawa office, where he is Chair of the firm’s Communications Group.

**Our Communications law blog**

**www.CanadianCommunicationsLaw.com**

Stikeman Elliott’s online resource in the communications area of law provides information and commentary on important legal and policy developments. Visit today to register for regular updates by email, RSS or Twitter.