August 2010

MAYER·BROWN

Electronic Discovery & Records Management

Tip of the Month

Preserving Data on Custodians' Personal Email and Personal Phones, Devices and PDAs

Scenario

A large manufacturer is served with a class action complaint alleging that the company knowingly produced products that were unsafe in certain circumstances. In-house counsel meets to discuss and identify electronically stored information (ESI) that may be responsive to the complaint and learns that one potentially relevant source of information is employee text messages. While the company issues and supports BlackBerrys, many employees who may be custodians of data relevant to the litigation send work-related messages from their personal, unsupported cell phones, smartphones and PDAs.

Protecting Employee's Reasonable Expectation of Privacy while Meeting Discovery Obligations

If in-house counsel knows, or should know, that employees use personal devices or personal email for work-related communications, a duty to preserve—and potentially collect—that data may arise. Although the Federal Rules of Civil Procedure do not specifically address personal email, text messages or other information stored on personal devices, the 2006 Amendments adopted a broad definition of ESI that encompasses data "stored in any medium" from which it can be obtained and "translated, if necessary" into a "reasonably usable form." As a result, failure to preserve and, if necessary, collect information that is relevant to a lawsuit and that is stored on a personal device or sent through personal email accounts may expose an organization to claims of spoliation.

In fulfilling the obligations set forth in the Federal Rules, both in-house and outside counsel should be aware that the decision to preserve and/or collect data held on a personal device or sent through a personal email account can present issues with respect to employee privacy rights. Communications sent via personal devices or personal accounts, such as text messages, are often highly personal and sensitive in nature. If employees have a reasonable expectation of privacy in their communications sent via personal devices or personal email, either under state or federal statute or company policy, employers should be aware of their employees' rights when collecting such communications for discovery purposes.

Further, the law regarding employees' expectations of privacy in work-related electronic communications sent from personal devices or personal email is unsettled. For example, while

some courts have held that employees have a reasonable expectation of privacy in password-protected personal email accounts, even when accessed through a company-issued laptop, others have found an employer's search of its employee's text messages to be reasonable. The SEC has recently indicated that the recordkeeping requirements of the Securities Exchange Act encompass the personal email accounts of a broker-dealer's employees that were used for business-related activities. As a result, employers should proceed with caution and take steps to avoid any potential conflicts between privacy rights and discovery obligations.

Be Prepared to Respond to Requests for ESI

There are few clear-cut rules for how work-related data stored on a personal device, or work-related communications sent via personal email accounts, should be treated. Taking a proactive stance in considering and responding to the challenges such data presents can prevent conflicts down the road. Some issues that should be considered include:

- *Understand the company culture*. If employees are accustomed to sending and receiving work-related communications via personal devices or personal email, a policy that bans them outright is likely to fall victim to workarounds by resourceful employees. For example, disabling text messaging on company-issued phones or PDAs may simply lead to the less desirable outcome of work discussions occurring on personal phones.
- *Determine what devices to support*. The technology supporting cell phones, smartphones and PDAs is constantly changing, and each new device stores more information than the next. For example, permitting employees to receive company email messages on their iPhones may raise data collection issues, since those devices can store significant amounts of information. Similarly, allowing an employee to direct work related email messages and other such communications to personal hand held devices rather than company-issued devices can create additional challenges for employers in responding to discovery requests.
- *If not currently allowed, consider authorizing the use of work-related text messaging on employer-issued phones or PDAs*. There are numerous benefits for employers to issue and encourage employee use of such employer-issued devices. First, courts are less likely to find that an employee had a reasonable expectation of privacy in a company-issued device, thus minimizing potential privacy related conflicts. Second, messages can be set up to synchronize to the company server. In such instances, the messages stored on the devices themselves may be considered duplicative and unnecessary for production, thus minimizing the burden of collection from individual devices. Finally, uniformly supported devices minimize technological hurdles to collecting text messages, including translating data from multiple formats and maintaining the necessary tools and trained staff to collect from any number of unsupported phones or PDAs. In particularly sensitive matters, where information must be produced in its native format, this advantage becomes particularly salient.
- *Be prepared to explain the burdens and costs associated with preservation and collection*. Open and up-front conversations with opposing counsel about potential sources of relevant information and the burdens associated with collection and production can reduce the risk that an opponent will make a spoliation claim if certain data are not preserved. If both parties face the same challenges with preserving and collecting work-related data stored on a personal device or work-related communications sent via personal email, the parties

may agree to forgo or limit the preservation or collection of such data.

- *Have a written policy and follow it*. Organizations can consider adopting a clear policy about the use of personal devices and personal email accounts that is communicated to all employees. That policy may include the use of periodic audits for compliance. Courts may be more likely to find that a company's response to a discovery request was reasonable if they follow established policies.
- *Provide formal training to employees about the corporate policy*. It is important to educate employees about corporate policies and to make sure that they understand the risks associated with failure to comply. If employees are trained to only use work-issued devices and work email systems for work-related discussions, a court may be more sympathetic to the argument that collecting employees' personal phones is an undue burden.

In our mobile society, the line between personal and work-related communications is increasingly blurring. Organizations should be aware of the potential existence of, and risks associated with, work-related data stored on a personal device or work-related communications sent via personal email, and should take proactive steps to develop policies and strategies for managing those risks before litigation arises.

For inquiries related to this Tip of the Month, please contact Anthony J. Diana at adiana@mayerbrown.com, Kim Leffert at kleffert@mayerbrown.com, or Michael Baltus at mbaltus@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com or Thomas A. Lidbury at tlidbury@mayerbrown.com.

Please visit us at www.mayerbrown.com