BUSINESS LAW TODAY
The ABA Business Law Section's Online Resource

Going Mobile: Are Your Company's Electronic Communications Policies Ready to Travel?

By Kathleen M. Porter

Computers have dotted office desks for decades, and the Internet and e-mail have been common workplace tools since the mid-1990s. When the Internet and e-mail were first introduced, they dramatically increased the ability to transmit information. They also created the potential for misuse and liability. Employees surfing the Internet during the work day or accessing inappropriate websites affected productivity. In litigation, e-mails produced in discovery were often embarrassing or damaging evidence against a party.

Companies adopted "electronic communications," "Internet access," or "computer use" policies to address these misuse and liability concerns arising from the use of workplace computers and e-mail. These policies communicated to employees the company's rules for proper professional and personal use of the Internet and e-mail on the company's computers and systems, and the risks of misuse. These policies also stated that the company could look at the employees' documents, e-mails, and other content created, transmitted, or stored on the company's equipment. The policies permitted the company to view an employees' Internet browsing and viewing activity on the company's equipment. These statements dispelled any expectation of privacy that an employee might have in his or her use of the company's equipment. They authorized the company to access and monitor the employee's activities while using corporate equipment and systems. The policy also warned employees of disciplinary action if the monitoring uncovered non-productivity or misuse.

Existing Policies are Often Inadequate

Electronic communications policies are generally premised on the fact that the company owns the computer equipment and pays for the access, security, and other services. The company has broad control over what it owns and pays for, subject only to the need to give the employee appropriate notice about monitoring and access.

However, today, business is conducted not only with workplace computers, but more often with portable devices. Additionally, employees regularly access personal web-based e-mail, social media and other accounts from their work computers. Many electronic communications policies fail to address these types of equipment and technology.

For example, many policies don't address whether and how employee-owned devices may access the corporate network. Even if remote access is contemplated, the wording may relate only to home computer access. Many policies do not consider the employee's use of his or her computer to access a private web-based e-mail, social network, or other account, or access of the Internet on his or her mobile device.

With mobile devices, a company has far less control than with corporate equipment, making it even more important for the company to have authority to access, monitor employee activity, and take appropriate action to prevent misuse or liability. While it is not as simple as amending an electronic communications policy to add the words "and mobile devices" after every use of the word "computer," with some careful thought and planning, an effective mobility policy can be created.

Case Law on the Right to Monitor

Before discussing the components of a mobility policy, it is helpful to first review how courts have interpreted electronic communications policies generally. Many U.S. courts, including the U.S. Supreme Court, have recognized the validity of computer usage policies in defining the company's authority to monitor its employees use and activity. The Court, in the *City of Ontario v. Quon*, held that a municipality's computer use, Internet, and e-mail policy determined the scope of the employee's privacy rights in text messages he sent and received on his work-issued pager. In this case, the city's policy extended to pagers. When concerns grew that the monthly texting service plan was inadequate, the city reviewed the text messages. The employee was fired when the review revealed the employee had sent and received personal texts with inappropriate content. With a government employer, the question before the Court was whether the city's access and review of the employee's text messages was an

unreasonable search and seizure in violation of the Fourth Amendment. The Court in *Quon* found that the city's computer-use policy dispelled the employee's expectation that his text messages would be private. The Court also found that the city had the right to review whether its text plan was adequate, that it did so in a limited fashion, and as such, the city's search of the text messages was reasonable. Because the search of the text messages was determined to be reasonable, the city's termination of the employee for violating the computer-use policy was upheld.

What the Court in *Quon* did not do was set parameters on an employee's privacy expectations in his or her company's technology equipment and systems, or define the limits of the company's right to access and review the employee's documents and e-mails. Additionally, the Court did not speculate on what its holding might be if the device at issue was employee-owned rather than city-owned, or if the employee rather than the city paid for the text messaging service. However, there have been several state and lower federal court cases which have examined some of these scenarios and offer some guidance, and a few of these cases are summarized below.

The court of appeals in Georgia, in *Sitton v. Print Direction*, recently upheld the firing of a sales employee working for a competing business in violation of company policy. The employee used his personal laptop at work and connected it to the company's network. While connected, he used his personal web-based e-mail account to engage in the competing business. A suspicious supervisor went into the employee's office, moved the employee's laptop mouse around, and e-mails appeared on the screen showing the competing activity. The court in *Sitton* focused on the trial court's finding that the company's computer usage policy granted the company the authority to inspect the employee's personal computer because he used it for work. The computer usage policy also told employees they should not consider "electronic mail left on or transmitted over the company's systems to be private or confidential." The appellate court concurred with the trial court's finding that the personal e-mail account e-mails were subject to the company's review under the terms of the computer-usage policy, and could be used to show the employee violated the company's noncompete policy.

The court in *Sitton* distinguished the facts from those in *Pure Power Boot Camp v. Warrior Fitnexx Boot Camp,* a case decided in 2008 by a federal district court in New York. In *Pure Power Boot Camp*, the court barred the company from using e-mails and documents obtained from a former employee's three password-protected personal web-based e-mail accounts to show the employee stole the company's confidential information. In this case, the employee's username and password for one of his web-based accounts was stored on the company's computers, and then used by the company to access all three accounts and find the incriminating e-mails. However, the court found that the company lacked authority to use this personal information to access the web-based accounts because there was no company policy informing the employee that company computers would be monitored or that personal web-based e-mail accounts could not be accessed from the company computers. Moreover, while the username and password were stored on the company's computers, there was no evidence that the employee downloaded these particular e-mails onto the network, or even viewed these e-mails using the company's computer systems.

In barring the company's use of these e-mails to prove its case, the court in *Pure Power Boot Camp* reviewed several cases whose holdings all turned on whether the company had a policy informing employees that company computers would be monitored, and whether the policy adequately put employees on notice regarding the lack of privacy in their computer use and their e-mail and documents.

In a recent California federal district court case, *Han v. Futurewei Technologies,* the court resisted a company's initial demands to inspect a former employee's personal computing devices and external storage devices for possible misuse or theft of the company's confidential information because there was no actual evidence of misuse or theft. The court in the case also found no evidence an employment policy had been violated by the employee. Very concerned that the inspection of the devices might expose the former employee's personal and privileged information to the company, the court instead approved a protocol whereby the former employee's expert would inspect the devices and produce a list of documents relevant to the company's discovery request. The court's decision in *Han* was based in part on the lack of an employment policy regarding storing or transferring company files onto personal devices, and in part about a concern over access to privileged information of the employee. While the court left open the possibility of revisiting its decision upon hearing evidence of misuse or theft of the company's confidential information, if the company had a computer use policy such as the one in *Sitton*, the initial outcome may have been different.

In certain limited cases, even having an electronic communications policy may not suffice. In *Stengart v. Loving Care Agency, Inc.*, the company issued a computer usage policy, notifying employees of its right to monitor use of its computers and also asserting ownership over any data on the computers. After the employee sued for discrimination, the company preserved the contents of the employee's company issued laptop and found e-mails to her lawyer sent from her employee web-based personal e-mail account. Based on the company's policy, the trial court found the company's access and use of these e-mails in the litigation to be permissible. However, the New Jersey appellate court disagreed, and reversed the trial court's decision. In doing so, the appellate court critically parsed the terms of the policy, while at the same time underscoring the need for a showing that the employee intended to waive her attorney client privilege. The lack of a signed acknowledgement of the policy by the employee was also a factor in the appellate court's decision.

With these cases, and others like them, we are beginning to see a framework developing regarding a company's right to

monitor mobile devices, employee-owned equipment or data created or stored on an employee supplied service. With this framework, a company can develop a mobility policy that will provide employees with the ability to use mobile devices with the company's network, while safeguarding company confidential information from misuse and theft and insulating itself from liability.

Mobile Devices

A mobility policy should broadly define what constitutes a mobile device. The definition should include battery, electric, or wireless operated devices that are easily transported and designed or capable of storing, processing, or transmitting data, text or e-mail. This broad definition captures evolving equipment and would include smart phones, portable digital assistants, mini personal computers, tablets, laptops, mini-hard drives, zip, thumb and flash drives. A company could choose to limit the definition to specific manufacturers, mobile networks, devices etc., depending on a company's needs and resources.

The Role of the IT Department

Drafting an employee policy is generally done by the human resources and legal departments. In drafting a mobility policy, the Information Technology Department (IT) should play a considerable role, including establishing the standards for identifying what manufacturers, devices, models, operating platforms, mobile networks, and service plans are acceptable in the workplace and to access the company's network. IT should also define the parameters of its assistance and support to employees with devices. Both the standards and the parameters should be incorporated into the mobility policy.

For example, IT may want to provide initial activation assistance on new devices, or on-going support to existing devices. IT may want to be responsible for identifying relevant security patches and the mechanisms for employees to download them. It may want to send updates on routine issues, or just alerts if there are concerns an employee's device has been compromised. Additionally, IT may want to impose end-of-support life dates to avoid supporting obsolete devices. As part of any employee termination, IT may want to review, and if it is company-owned, retrieve a mobile device. IT may also need to review server logs to determine whether information was downloaded or copied in violation of the company's policy.

IT may elect to outsource some or all of these functions to a third-party mobile device management (MDM) provider, including if there are limited resources or a substantial global workforce or a broad range of mobile devices to be used with the company's network.

Who Owns the Device and Pays for Services?

An initial consideration is whether the devices and the mobile network service will be company- or employee-owned or provided or both. The company should also consider whether to offer a stipend for the mobile device or the service plan, to the extent the device is to be employee-owned. Finally, the company may want to restrict the mobile network plan to certain providers. If employee-owned devices will access the company network, IT should determine what minimum security and other standards an employee-owned device must meet to have access, and define how devices will be authenticated and visible to the network.

Security

A mobility policy should address password and authentication requirements, including requirements to periodically change passwords and for the device to time-out if it is at rest for a designated period of time. The policy should also address whether there are separate or multiple log-in and password requirements to access the device, the company's network, and any personal accounts or network access. If there are log-in requirements, the policy should address whether the employee is required to log into each with each use of the device, access or account, or whether it is permitted to have the company network access open and accessible once the employee inputs the device password. The mobility policy should require the employee to securely store his or her mobile device and not leave it unattended.

With an increase in mobile malware distributed through downloaded applications, companies have a legitimate interest in preventing malware from accessing the company computer systems through devices. Although a company controls its network, its applications and software, it is not as easy to control applications and software on devices which access the corporate network. A company can condition an employee's network access on the employee's agreement to restrict the mobile device's applications and software to only those the company approves and requires.

A company may want mobile devices to have mobile filtering and security software which control the types of sites that can be accessed and applications that can be downloaded. These requirements would be included in the mobility policy. With its authority to monitor the device, the company could also monitor devices for prohibited content and for malware. An MDM provider would have access to these types of tools and could assist a company in implementing them.

Lost or Stolen Devices

Annually, thousands of mobile devices are left in taxis or in pockets of clothes at the drycleaners or otherwise lost, stolen or misplaced. Lost or stolen mobile devices containing confidential or personal information have been the cause of numerous data security breach notifications. Therefore, being able to access and wipe a lost or stolen mobile device to prevent data loss is critically important. Knowing about the loss or theft immediately is equally important and thus, a mobility policy should require employees to immediately report device loss or theft.

Even when mandated to do so, employees often delay reporting, because they believe the device will eventually be found, or they fear disciplinary action for losing the device or they don't want to lose valuable personal photos and contact information when the device is wiped and restored to factory settings. In response, some companies have actually

permitted employees to remotely wipe their device, either directly or through an MDM provider. Other companies penalize employees, by agreeing to reimburse employees for a lost or stolen device only if the mobility policy is followed. Additionally, most mobility policies permit the company to take disciplinary action if the employee fails to report or delays reporting a device loss or theft.

An MDM provider offers 24/7 coverage to respond to employees' reports of lost or stolen devices. At least one MDM provider has developed the ability to perform a partial remote wipe on the device, in order to minimize the loss of personal photos or other private data. Most importantly, an MDM provider offers expertise, training, technology, and other resources prior to the loss or theft to minimize its occurrence and reduce its effects.

Determining Eligibility for Access

Mobile devices are not typically issued to every employee or contractor. However, some companies allow every employee or contractor network access with his or her mobile device. Companies should be aware of some Fair Labor Standards Act (FLSA) issues if the employee's mobile device has network access and messages are sent to the employee's work e-mail address outside of the workplace, and outside of normal working hours. Workers who are considered non-exempt under FLSA may be considered "working" because they receive or send e-mail outside of the workplace or outside of office hours, triggering possible overtime payments. Calculating the amount of overtime is also difficult, given that messages are sent and received intermittently. Already, numerous FLSA claims have been made based on the receipt of data on mobile devices, including ones by police officers, telecommunications workers and even an employee of a famous talk-show host.

How and When May a Device be Used?

If the device is company-owned, a mobility policy would typically provide that the device is to be used for business needs, for benefit of the company, and not for the convenience of the employee. In many cases, a company may issue a device to an employee (exempt under FLSA) because they want them to be accessible not only during business hours but also, if needed, outside of business hours.

Ironically, many companies express a preference in their mobility policy for the employee to use a landline phone if one is available. One reason for this is that a landline is still considered to be more appropriate if the subject of the call is confidential or sensitive. A landline may also be preferred if there is a concern about the strain on the company's bandwidth. For this reason and for productivity reasons, a company may want to generally restrict the amount of the employee's use of the device in the office.

Privacy––Access, Personal Data

If the device is company-owned, then the statements in the mobility policy regarding the employee's expectation of privacy should be similar to those in existing electronic communications policies. The statements are to the effect that the company is authorized to monitor the device and the activities conducted with the device, personal and professional; and the employee has no expectation of privacy in the device or in her activity while using the device.

This issue is murkier when the employee owns the device and/or pays for the mobile network service or uses it to access web-based personal e-mail or social networking accounts. To address these situations, the mobility policy should grant the company broad authority to access an employee-owned device used for work, as well as an employee's activity on the device, including an employee's web-based personal e-mail or social network account.

The mobility policy should provide that the employee understands that he or she is being permitted to access the company's network with his or her mobile device, on the express condition that the employee agrees the company has the authority to monitor the device and activity, including activity on any web-based personal e-mail or social network account. The best evidence of the employee's consent to the company's right to monitor and access is to have the employee sign an acknowledgement or consent to the mobility policy. Many companies incorporate the mobility policy into the employee handbook or take other steps to have evidence of the employee's acceptance of this policy. Many companies also pay for or subsidize the employee's mobile network service plan, because the service is used partially for work. If the company is subsidizing the cost of the device or the service plan so that the employee has these tools for work, this should be documented.

When the company is monitoring and accessing an employee's device and content, the company should take care to limit access to only what is needed for legitimate business purposes and do so with the advice of legal counsel.

A mobility policy should also address the fact that employees will have personal or private data on their mobile devices. The policy should authorize the company to monitor and access this data for legitimate purposes. The mobility policy should require the employee to back-up her personal data on the mobile device to avoid losing it in the event the device must be wiped.

Evolving Area

It is important to recognize that use of mobile devices for work and other purposes continues to evolve, while the life cycle of particular mobile products and technology is rather short. Any mobility policy adopted by a company today should allow for regular amendments to reflect the introduction of new devices and the retirement of older models, as well as changes in technology. Additionally, the policy should allow a company's IT and HR departments to conduct initial and ongoing training, including issuing periodic updates on security, access, and other relevant issues.

A mobility policy should strive to balance the company's interest in leveraging the benefits of technology to improve productivity with the need to safeguard the company's confidential and personal information and that of its employees and customers.

Kathleen M. Porter is an intellectual property and business transactions partner at Robinson & Cole LLP in its Boston office. She is a member of the ABA Business Section's Cyberspace Committee and a certified information privacy professional (CIPP) by the International Association of Privacy Professionals.

Additional Resources

The following article outlines components of a company policy on e-mail and using the Internet.

Business Law Today

Work station or purgatory?
Steps toward a company policy on e-mail and using the Net
By Kathleen M. Porter, David Wilson, and Jacqueline Scheib
Volume 11, Number 6—July/August 2002

TEN CONSIDERATIONS WHEN DRAFTING A MOBILITY POLICY

1. Involve IT in Defining Policy Parameters
• Have IT determine permitted and supported devices, manufacturers, models, operating systems, platforms, mobile networks, etc. • Determine IT assistance for initial activation and on-going support of a device. • Establish the controls and capability for encryption, authentication, virus protection, malware, remote wipe. • Consider using a third party mobile device management tool or provider.
2. Costs and Eligibility
• Determine whether company or employee-devices or a combination. • Decide whether to give allowance or stipend for employee purchase of device or service. • Keep Fair Labor Standards Act (FLSA) in mind when establishing employees/contractors eligible for a device and/or network access.
3. Security
• Establish minimum security standards for devices, access, authentication. • Decide whether to permit open or require separate log-ins to access device, voicemail, e-mail, network, or Internet. • Mandate download/use of certain security or other mobile device management tools. • Permit company to monitor device for illegal content or for malware to protect company against damage if device used to access company network. • Consider adding encryption if available or a device access timeout for when device at rest. • Obligate employee to use reasonable care in handling, safeguarding, and storing device and information and systems accessible on device.
4. Privacy
• For employee-owned device accessing the company network, provide restricted connectivity so that employee is authorized to connect to network only if employee agrees to limit applications, permit access, remote wipe, and audit. • Obtain permission from employee prior to network access for the company to access device, restricted connectivity, monitor activities, and remote wipe. • Develop a plan for handling employee's personal data, including creation, storage, and use.
5. Device Use
• Restrict use to business needs for benefit of company, not convenience of employee; harder to do with employee owned device. • Determine whether want employee to be accessible during non-business hours if needed, and remember the rules regarding nonexempt employees under FLSA. • Place restrictions on employee's use of device while in office to limit productivity issues and pressure on company systems bandwidth.
6. Access to Company Network
• Require registration of device with company in order to access network and make device visible to IT. • Require employees to provide media access control address when available for particular device. • Condition employee's access to personal web-based e-mail account (e.g., Comcast, Verizon, Gmail, Hotmail) or access social network access (e.g. LinkedIn, Twitter, Google+, Facebook) via the company's network on the employee's agreement to allow the company access to employee's account for legitimate business purposes. • Consult legal counsel prior to accessing any employee personal or social network accounts.
7. Applications and Downloads
• Restrict applications and software on device to only those approved by company. • Require HTTPS only, ActiveSync. • Require mobile filtering software to control types of sites accessed and apps downloaded on device. • Determine if network services be available through syncing with a desktop or web application. • Consider how updates/upgrades to the device will be accessed and downloaded.
8. Lost or Stolen Devices; Monitoring
• Require immediate reporting of lost or stolen device or unauthorized access. • Determine disciplinary action; for illegal or unauthorized activity. • Consider disciplinary action if not compliant or if delay reporting. • Provide reimbursement for stolen device only if employee follows policy. • Consider whether to allow employees to remotely wipe directly or via a third party provider (such as Mobile Me). • Understand legal prohibitions on deducting or collecting money for company-owned device if lost, stolen, or destroyed.
9. Use Outside the U.S.
• Comply with U.S. export laws regarding physical or electronic transmission of controlled data outside the United States. • Check device and review policy with employees prior to overseas travel. • Understand that other jurisdictions may have different rules on mobility, e.g., privacy of personal information; required authorization to monitor, access, or remote wipe.
10. Allow for Changing Technology
• Allow for amendments, updates to reflect changing technology, models, and devices. • Allow for IT and HR to issue periodic updates/alerts for security and changes, etc.