BYOD:

BRING YOUR OWN DEVICE

KNOW THE PRIVACY AND SECURITY ISSUES BEFORE INVITING EMPLOYEE-OWNED DEVICES TO THE PARTY

BY HENRY Z. HORBACZEWSKI
AND RONALD I. RAETHER

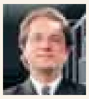
Growing up, some of us may have gone to a summer camp or country club owned and operated by a parent's employer. Employers also had doctors, dentists and heavily subsidized cafeterias onsite. Such benefits were not unusual in corporate America in the 1970s, but are almost nonexistent today. For most of us, gone are the days of company cars. Today, not only do we drive our own cars, but we also use our own cellphones for work. Some companies also ask (or allow) employees to use their own laptops and other electronic resources to interact with company systems.

This trend is driven by recessionary cost pressures, which often result in employers attempting to shift these costs to their employees. However, there is also a significant element of employee preference for selecting and using their own devices. As the economy strengthens, and tech-savvy employees are in increasing demand, employers should expect the pressure to allow employee-owned devices and the related security and privacy issues to increase, not abate. This article will identify the unique security issues presented by employee-owned devices and suggest steps to help mitigate related risks.

Risks of employee-owned devices

While there is an economic incentive to avoid fixed costs (e.g., improving EBITA) and accommodate mission-critical employees, the use of employee-owned devices raises unique data security and privacy issues that are not always adequately considered (if considered at all). What happens with the data and the equipment upon termination? How do you ensure security updates are promptly uploaded? What are the licensing and ownership or access issues? How do you accomplish security scans, and what is the scope? What expectation of privacy is reasonable for the employee to assume? How do you appropriately monitor use to comply with company policies, including its code of conduct? Certain aspects of these issues are not new. For example, many of these issues are present in the context of home-based or traveling employees. Employee-owned devices, however, complicate many of these practices and raise new issues.

HENRY Z. HORBACZEWSKI is general counsel of Reed Elsevier Inc. He can be contacted at *henry@reilaw.com.*



RONALD I. RAETHER, CIPP, is a partner at Faruki Ireland & Cox P.L.L., providing leadership and guidance to companies experiencing unauthorized access to sensitive data, and facilitating a team- based effort of legal, IT and business departments to proactively address these issues. He can be contacted at *rraether@ficlaw.com.*

The security issues are particularly acute for employers in the financial services and related industries who deal with data regulated under the Fair Credit Reporting Act, the Driver's Privacy Protection Act, Gramm–Leach–Bliley Act, and analogous state laws and related administrative regulations. In addition, many employers are subject to the Health Insurance Portability and Accountability Act and must similarly be concerned about the transmittal of data on such devices.

To understand the risks created by employee-owned devices, it is important to understand the general security issues raised by remote access via a laptop, mobile phone, tablet or similar device. Think of information security like a castle and sensitive information as the crown jewels. Until recently, companies have focused their efforts on enhancing the protections of the castle and isolating data to the main keep. Companies improved their system architecture, built hacker-resistant firewalls and intrusion detection programs, and trained employees who guarded the access points. Now, think of each device as an outpost that not only provides access to the castle, but also keeps some part of the crown jewels. The defenses of the castle no longer suffice. Now, every outpost (e.g., laptop) must be as strong as the castle.

This illustration is not unique to employee-owned devices, but applies equally to cloud computing, traveling and home-based employees. The same general security issues presented by these models provide a good starting point for looking at employee-owned devices. Cloud service providers are required to have equivalent security measures. They should be required to properly isolate your company's sensitive data in a manner that provides sufficient segregation from the data of another client. They also should ensure that the servers, which hold such company-sensitive data, are not vulnerable to SQL injection attacks or malicious code. The cloud service provider also must be required to have appropriate processes for ensuring proper disposal/sanitization of the data if your contractual relationship changes.

Likewise, policies require employees to take certain protections, such as system scanning before connecting to the company network, periodic reviews of the equipment by network administrator's metadata cleaning processes, and return of the equipment upon termination. Some companies now go as far as implementing automated applications so that when an outside device tries to connect to the company network, it validates that the antivirus/malware software is up to date, and that there is appropriate firewalling on the device. Each of these points should be addressed when dealing with employee-owned equipment.

Security starts with knowing what data resides where, and who has access to that data. With employee-owned devices, the main unique issue from a security perspective is loss of control. Indeed, many companies prohibit the use of company-owned devices for personal use. Companies also prohibit the use of employee-owned devices to access company systems and networks. An employee (or a third party with access through the employee) using the company computer to play an online game or access Facebook could circumvent the security controls and permit malware to be installed on the device — like what happened in the Koobface attack (*http://en.wikipedia.org/wiki/koobface*) — and ultimately on the company's system.

Using a personal device could result in sensitive data being stored outside of the company's system and thus not subject to scans. The company may have no means to make certain that security updates and patches are uploaded in a timely fashion. Similarly, there are limits on the controls normally in place to make sure the IT department is following policies and processes for maintaining security on company devices. In response to a possible threat, the employee-owned device may not have the proper audit logging in place or be accessible for the forensic analysis. The employee might not even install basic security software on their equipment, and so the data would be extremely vulnerable.

With company-owned devices, the company is able to manage security controls on the device. The company can set up the device with certain security settings and put in place periodic reviews to ensure that those settings are not changed. With employee-owned devices, such measures could be put in place, but raise issues about device integrity and utilization, employee privacy, and whether the company can restrict the permitted uses of the device for personal use. For example, most devices now have a locator feature and a "poison pill." The company may want the ability to locate the device should it go missing and then delete, kill or render the device useless, using a "poison pill." Sometimes, however, the pill cannot differentiate between company data and the employee's personal data.

Privacy challenges of employee-owned devices

On issues of privacy in the case *City of Ontario v. Quon*, the starting point for company-owned devices is a clear and detailed policy, which informs employees that they have no expectation of privacy. No. 08-1332, 560 U.S. (2010) ("And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.") The lines of permitted use and company access to data and information stored, accessed or transmitted (whether for business or personal use), should be detailed and complete. Absent such detail, the company risks finding that the employee had a reasonable expectation of privacy as to the personal data stored on the company computer or system. (*Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (2010) *http://lawlibrary.rutgers.edu/courts/supreme/a-16-09.opn.html.)*

Policies regulating employee-owned devices need to start from a different perspective and recognize certain limitations. However, when is came to company-owned devices, personal use was the exception. Many policies were developed around the concept of company-owned equipment. For example, policies would inform employees that:

- the company would monitor their use of employers' electronic resources;
- email transmitted using company equipment could be stored on that equipment even if through a personal, web-based email account;
- the company could review all communications stored on, or transmitted by, company equipment regardless of whether a personal account is used; and
- the user had no expectation of privacy when logging onto Company XYZ's network.

With company equipment, the expectation of privacy is more limited, and the company is given more discretion as to whether its conduct was reasonable.

Employee-owned devices are expected to be used for personal business and to store the employee's personal information. Reciting the above warnings is insufficient. The policies need to be tailored to the reality of the circumstances. Take the above example regarding remotely wiping content from a mobile device, e.g., when an employee fails to return a device upon termination, the company can trigger an application that erases the content of that laptop — the "poison pill." With an employee-owned device, this action likely would delete the employee's personal files. Likewise, when the device is scanned, the employee's personal information will be exposed.

> The intent of any policy is **not to intrude on the privacy of employees,** but rather to maximize the security of company-related data and **protect the reputation of the company.**

The intent of any policy is not to intrude on the privacy of employees, but rather to maximize the security of company-related data and protect the reputation of the company. Initially, the policy should maintain the lack of expectation of privacy to the extent data ends up on company-owned equipment. For example, if I use my personal laptop to send email via the company server (i.e., using my company-supplied email account), then that email will reside on the company's server. The employee should be informed that there is no expectation of privacy under such circumstances. For this policy to be effective, however, the employee should be educated and trained on what acts can result in personal information being left on company-owned equipment. Likewise, the acceptable use policy should clearly extend to employee-owned devices. For example, the access of pornography may not only harm the company's reputation, as any access might be recorded as coming from the company's IP addresses, but also access to such sites may degrade the security of the equipment.

Employers have a delicate line to walk as the proper lines for monitoring employee use of social media sites continue to be drawn. For example, the National Labor Relations Board has issued several recent decisions concerning the scope of what is permitted in social media policies for employees protected by the Wagner Act, as seen here: *www.*

A company might consider **isolating the company-related data** within the employee-owned device. **The ability to effectively control the location of the data** will depend on the functionality of the device.

nlrb.gov/news/administrative-law-judge-rules-chicago-car-dealership-had-overly-broad-employee-policy-discharg. The case concerned whether an employee could be terminated for Facebook postings that mocked the employer. The company's policy provided that: (a) "[a] bad attitude creates a difficult working environment and prevents the dealership from providing quality service to our customers;" and (b) "[e]veryone is expected to be courteous, polite and friendly to our customers, vendors and suppliers, and to their fellow employees [and] [n]o one should be disrespectful or use profanity or any other language which injures the image or reputation of the Dealership." Paragraph (c) prohibited employees from participating in interviews, and (d) required inquiries concerning employees be directed to human resources. Although the NLRB administrative judge found that paragraphs (b), (c) and (d) were unlawful, the judge held that paragraph (a) was permissible. The judge also found that the discharge was legal, as the communications did not concern the conditions of his employment.

Risks of employee-owned devices can be mitigated

As to the data residing on the employee-owned device, the solution is more complex and requires the consideration of multiple factors. The privacy policy must work in tandem with the security procedures implemented by the company. For example, the privacy policy should permit log-in and periodic scans, and allow company IT personnel to review the sufficiency of the devices security settings, without fear that the employee's rights are being impermissibly invaded. Security requirements also must be communicated to the employee and enforced. These issues include:

- minimum hardware and operating system requirements;
- deployment of antivirus and malware prevention software;
- screensaver configurations and password requirements; and
- encryption of sensitive data.

The content of the policy will vary based on multiple factors, including the technical structure (i.e., architecture) of the overall system. Will the laptop act as only a dumb terminal used to access the company's system through a secured portal, meaning that no company data should ever reside on the laptop? The number of requirements and level of detail will vary depending on the answer. If the policy is properly followed, then no company data should reside on the employee's device. Will the company, however, use tools to further limit or monitor the employee compliance with the "no local storage" policy (e.g., disabling USB ports or monitoring log files for improper conduct)? If so, the policy should permit the company to conduct a forensic study of the employee's device if there is reasonable belief that company data was mishandled.

ACC Extras on…
Employee-Owned Devices

InfoPAK^{SM}

- Workplace Information Risk in the Digital Age: Monitoring Employees, Social Media Challenges, Managing Access to Data and Optimizing Flexibility (Jan. 2011). *www.acc.com/infopaks/info-risk_jan11*

Forms & Policies

- Privacy in the Cloud: A Legal Framework for Moving Personal Data to the Cloud (Oct. 2011). *www.acc.com/forms/privacy-cloud_oct11*
- Electronic Information Systems Policy (April 2011). *www.acc.com/forms/eisp_apr11*

Presentation

- Data Security & Privacy (Nov. 2011). *www.acc.com/data-s&p_nov11*

Article

- Guide to Protecting the Confidentiality of Personally Identifiable Information (April 2010). *www.acc.com/protect-pii_apr10*

ACC has more material on this subject on our website. Visit *www.acc.com*, where you can browse our resources by practice area or search by keyword.

On the other hand, employees will complain that the dumb terminal restrictions inhibit their ability to do their jobs. A company might consider isolating the company-related data within the employee-owned device. The ability to effectively control the location of the data will depend on the functionality of the device. The discipline of the employee to use these controls will be more of an issue in truly limiting the location of the company data. The implementation of such a procedure, along with a policy regarding an employee's violation of the procedure, will improve the company's ability to argue for broader access should there be a need to search the entire device for company-related data.

Another option is to deploy an encrypted external hard drive and require that all company data be stored only on this drive and not on the personal device. This step, in conjunction with the use of a secure encrypted connection, assists in alleviating the data-ownership issue. As the encrypted drive would not be connected, or data decrypted in a manner to be accessible to the malicious code, the risk of contamination by a virus on the employee-owned device is lowered.

Even with this one example, the options and issues are numerous. While many of the high-level issues are the same as in dealing with cloud computing service providers or home-based employees, employee-owned devices require a different approach. Just as moving from a company-owned car to requiring employees to drive their own cars did not absolve the employer if an employee drove recklessly on the job, neither does switching to employee-owned devices absolve the employer of responsibility for how they are used. It is thus important to (1) control the location of sensitive data, (2) decide what, if any, data will be accessible or reside on employee-owned devices, (3) develop technical controls to mitigate risk of allowing such access, and (4) craft employee usage and privacy policies to best protect company assets and properly balance the employee's reasonable expectation of privacy. Before allowing access of employee-owned devices, these issues need to be fully vetted, and the exposure needs to be carefully considered. Without the proper process and procedures implemented to mitigate exposure, the consequences of a breach will quickly overcome any savings or employee goodwill of permitting employee-owned devices.

Have a comment on this article? Visit ACC's blog at www.inhouseaccess.com/articles/acc-docket.