

# Employee Use of Personal Devices

## Managing risk by balancing privacy and security

For some time, employers have faced a wide range of risks and obligations related to employee use of email, cell phones, computers, and other devices. Employees can create significant employer liability due to loss or misuse of data by downloading malware, transferring confidential files, surfing for porn, or participating in online gambling. Companies have long handled such issues by using security and monitoring programs on the devices they provide users. The courts have generally held that employees who are clearly informed about and agree to such monitoring do not have an expectation of privacy when using company provided devices.<sup>1</sup> However, this waiver is not absolute and has been limited or given close scrutiny in limited instances when employees were found to have a reasonable expectation of privacy.<sup>2</sup>

### Security and Compliance Concerns

Companies are now increasingly allowing employees to use their own personal mobile devices for work use for a range of reasons, even though doing so creates a number of risks, including:

- Risk to corporate confidential information
- Risk due to multiple unauthorized individuals who may be using the employee-owned devices, exposing the information to breaches that the company will never even learn about until, perhaps, after the data on them has been misused
- Noncompliance with regulatory policies for companies in health, financial, or other sectors subject to specific privacy and security regulations
- Noncompliance with the Federal Trade Commission (FTC) Safeguards Rule covering the wide range of companies significantly engaged in providing almost any kind of financial product or service<sup>3</sup>
- General liability to customers as well as public relations harm due to loss or improper use of personally identifiable information due to lack of security on email, documents, phone calls, and text messages
- Data and network integrity risks due to malware and jailbroken devices
- Human resources issues (for example, surfing porn within the enterprise campus from a personal device)
- Risk of failing to properly comply with obligations to maintain information subject to legal discovery

Discovery, in particular, poses a challenge when employees use personal devices for work-related communications. The failure to preserve, or, if needed, to collect, information that is relevant to a lawsuit that is stored on a personal device may result in a court or regulator taking significant adverse action against a party accused of “spoliation.” In fact, the SEC recently<sup>4</sup> censured, fined, and issued cease and desist orders against a broker-dealer when the company didn’t immediately provide relevant messages from personal devices of one of its contractors.

1. This paper focuses on the United States. In the European Union and in a number of other jurisdictions, employee monitoring may be subject to a range of legal requirements such as consultation with employee work councils, conducting an assessment of the impact on an employee, and other restrictions.

2. See *City of Ontario v. Quon*, No. 08-1332, 560 U.S. \_\_\_\_ (2010). See also *Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300, 990 A.2d 650 (2010).

3. FTC Safeguards Rule, 16 CFR Part 314.

4. In the Matter of vFinance Investments, Inc., <http://www.sec.gov/litigation/admin/2008/34-57088-o.pdf>

Until recently, managing these risks has been difficult for employers due to the inability to practically or technically use the same tools to control these devices that they have used on work computers and other employer-owned devices. But today, the latest versions of consumer devices have the necessary support for employers to assert technical management of these devices. Security and risk management companies have launched enhanced services that are able to provide employers with the needed tools to manage, monitor, and wipe these devices, as required.

These advances raise the question of employee privacy because employees, even if advised that access to the corporate network is subject to security controls, may feel a greater sense of intrusion when actions are taken with regard to a personal device that also stores their private communications and photos. Courts are likely to be more willing to find a basis for potential privacy liability if policies are implemented in a manner that seems over-reaching or unfair to an employee. For example, wiping a device without notice in advance of employee termination could result in loss of personal photos, video, or health records. Media stories are already beginning to appear focused on employees who were surprised to learn that a remote wipe has deleted their personal photos and contacts.<sup>5</sup> Likewise, monitoring web surfing, personal text messages and personal phone calls on an employee's device may be given careful review by courts. Employers should remember that some states, including California, have laws prohibiting employers from taking any job-related action against an employee based on lawful conduct off the job.

One technical solution offered by some companies is to only monitor or control a sandboxed portion of the personal device. Employees are prevented from downloading files outside of the corporate email and only the segregated portion of the device is monitored. Although more advanced versions of this solution may one day be of value for some employers, today they are unlikely to be acceptable due to critical limitations. Employees may need to transfer information from a file to a Microsoft PowerPoint presentation, but current security tools will not allow such transfer because of how they are designed to keep information in the designated environment. And because they are designed to monitor only a portion of a device, these security programs also cannot detect whether a device has been jailbroken or whether risky apps have been downloaded, creating unacceptable security and confidentiality risks for most employers. Regulated industries, in particular, may be unable to rely on partial monitoring of a device due to the extensive security and customer privacy mandates imposed on them. For example, the Financial Industry Regulatory Authority recently issued new guidance regarding broker-dealer communications with the public via email, instant messaging, and social media websites. These rules obligate these employers to control, monitor, and supervise employee communications.<sup>6</sup>

### Privacy Balance

A far more effective approach for most employers to take is to apply similar technical and policy controls as they do for their employer-owned devices but with a measured application in practice that allows for recognition of the need to balance security with employee privacy in specific instances. Employers should clearly inform employees about the policy and have employees specifically acknowledge the security enhancements that will be applicable. In policy, as in practice, the approach should be tailored to recognize that, for some limited classes of personnel, mitigating measures may provide a fair balance of employer/employee needs. For example, wiping a device in advance of termination is not uncommon for employer-owned devices in order to prevent unauthorized transfer of confidential information by a potentially disgruntled employee. When an employee's personal device is involved, a wiser policy might be to—in instances where a particular category of employee is unlikely to possess confidential information—provide limited notice to enable employees to transfer their personal data such as photos from their device prior to wiping. The company might also specifically advise employees not to keep their one (and only) copy of critical financial or health records on the device subject to wiping policy. Employers might also limit scope in terms of taking action on certain adverse information not directly related to workplace activity that they might gain from monitoring device use, recognizing

5. See National Public Radio, "Wipeout: When Your Company Kills Your iPhone," November 22, 2010.

6. See *FINRA Regulatory Notice 10-06 Social Media Web Sites: Guidance on Blogs and Social Networking Web Sites* (January 2010).

that the information about non-workplace-related use of a personal device would ordinarily not have been available. In highly regulated industries, there may be even less room to exempt certain classes of employees and such nuance may not be feasible.<sup>7</sup> It is also more likely that employees of these regulated industries will be aware of their companies' obligation to oversee work related employee communications and to secure even personal devices. Finally, the affirmative legislative obligations to adopt extensive compliance and security measures imposed on such companies will likely result in courts holding that a properly trained employee will have affirmatively waived any expectation of privacy when using a device that is accessing regulated systems.

### Conclusion

Of primary importance for any employer is communication with employees. An employer should over-communicate with employees about its policy, including regular reminders to back up personal data. When an employee uses a personal device to access a corporate system, that employee should be given additional notice that doing so comes with requirements and limitations. Application of the policy can be nuanced but must be consistent and documented. Managers should be advised not to make individual representations to employees that could undermine the company policy.

In highly regulated industries, or businesses holding customer sensitive data, employers are likely to have greater leeway to require an employee to waive privacy expectations in order to use a personal device to access company systems. Businesses holding less sensitive data or in non-regulated industries may want to apply security programs to help manage risk, but should consider tailoring their actions under the program in a consistent but more nuanced manner that balances security and privacy.

### About the Author

Jules Polonetsky has served as Chief Privacy Officer at AOL and DoubleClick and as the Consumer Affairs Commissioner of New York City. He is currently Director of the Future of Privacy Forum, a think tank dedicated to advancing responsible data practices.

### About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. <http://www.mcafee.com>.

---

7. Even if a company is not subject to sector specific privacy or security regulation, companies should be aware that the FTC has brought a series of actions against companies that failed to implement reasonable security measures or that misled consumers about their privacy and security policies.

