New York Law Journal

EMPLOYEES IN THE WORKPLACE

U.S. Employees Need A Federal Data Protection Law

By **Wendi S. Lazar**

The adoption and proliferation of mobile devices that are personal to employees but are used to service the needs of the business, or "Bring your own Device to Work," BYOD, as it is called, is the latest nightmare for employee privacy in the workplace. While the U.S. government has taken a backseat and piecemeal approach to protecting the rights of its citizens when it comes to data privacy and protection, the need for legislation is most wanting in the private workplace. The coupling of companies' dual-use-device mobile strategy with the escalating number of hours Americans spend on mobile devices has blurred the lines between employees' work and their private lives, eroding any semblance of personal privacy. Although federal and state legislation have attempted to protect consumers from loss and theft of their data, employees have been left to fend for themselves.

Unfortunately, with no federal legislation protecting both an employee's privacy and a company's need to protect data, there is an impending legal crisis for both employer and employee. Most employees don't understand the implications of using their own devices at work. Companies have attempted to write new employee technology policies and some, to force employees to sign waivers of liability for lost data when entering BYOD programs.

One problem is that employees often don't read these policies or seek legal advice to help them understand the waivers. Accordingly, when their iPads are wiped clean or their irreplaceable information is lost or destroyed, they are shocked. When their personal data becomes subject to discovery requests by a third party in a lawsuit or if they bring their own lawsuit for discrimination or retaliation, they are outraged to learn that when they signed on to the company's BYOD policy, they gave up other protected rights. Whether these policies or waivers are even legally valid in the context of BYOD remains to be seen, as there is no clear legal precedent.

In addition, most employees have no idea how remote wipe outs or active sync devices work. They often don't know about special software that their employer may use that can track them in real time (deliberately or accidentally)—whether they are on vacation, at a basketball game, in a hotel or on a remote work assignment. If the employee's personal device is lost or stolen, the employer may use the device's GPS in an attempt to locate it. This strategy remains in the gray area between legal monitoring of an employee's whereabouts in an earnest attempt to recover what may be confidential information on one hand, and illegal tracking which may be an invasion of privacy on the other.

With no federal legislation protecting both an employee's privacy and a company's need to protect data, there is an impending legal crisis for both employer and employee.

While BYOD policies were established to save companies money while accommodating both the preferences of employees toward certain devices and their mobility, the BYOD initiatives are further eroding any healthy division between work and private life. While actual working time is increasing for many workers, less time is actually spent in the workplace and it is increasingly more difficult for employees to draw the line between work and non-work time.

Equally disturbing to employers is the fact that their data is being stored, viewed and transmitted on devices they do not own or control, posing risks to their trade secrets and opening them up to potential litigation from employees over personal disclosures, security breaches and property destruction. In addition, wage and hour claims can and will be raised regarding the definition of when an employee is performing work.

Another problem is that families, not just employees, have access to and use these devices. Devices go with them to the beach, into bedrooms and to hospitals. While companies can attempt to reduce some of these risks through the use of Mobile Device Management software (MDM), or by enhancing their technology policies or instituting employee waivers, none of these fixes will provide an equal playing field for the parties or provide a consistent set of rules for maneuvering in this dual use world. Without a broad and meaningful federal policy, this situation will worsen as the technology gets smarter.

Limited Protection of Data

Driven by the pervasive issues with consumer protection of personal data and the proliferation of the Internet and online shopping, Congress and state legislatures have passed some meaningful laws that obligate businesses to provide security and notifications when personal data has been compromised. However, these laws give limited redress to employees whose data has been deleted, transferred or worse, disseminated to third parties without their permission or knowledge. Below is a summary of some of the current legislation and cases.

A partial remedy for both employer and employee was offered by Congress when it passed the Electronic Communication Privacy Act (ECPA), 18 U.S.C. §§ 2510 et seq., and two of its subsections, the Stored Communications Act (SCA), 18 U.S.C. §§2701 et seq., and the Wiretap Act, 18 U.S.C. §§2511 et seq.. The SCA prohibits individuals from accessing, without authorization, stored electronic communications, and the Wiretap Act prohibits individuals from accessing, without authorization, electronic information while it is in transit.

Most recently, the U.S. District Court for the Northern District of Ohio confirmed in *Lazette v. Kulmatycki*, No. 12 Civ. 2416, 2013 WL 2455937 (N.D. Ohio June 5, 2013), that employers who intentionally access employees' personal email on a dual use device will be liable under the SCA and may also be liable under state privacy laws. In *Lazette*, a former employee was permitted to use her device for personal email, which she believed she had deleted prior to returning the device to the company. After her employment ended she alleged that her supervisor subsequently accessed 48,000 email messages over months and shared some of her personal information with third parties. While the plaintiff also claimed a violation of the Wiretap Act in this case, the court did not agree that the employer's behavior constituted an "interception" of transmitted electronic communications, such as when employers monitor employees' telephone calls without notice or use spyware on their employees' computers.

In an earlier New York decision, *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 759 F.Supp.2d 417 (S.D.N.Y. 2010), the court confirmed that employers who intentionally access employees' personal email accounts without permission will be liable under the SCA even if the employer's technology policy clearly gives the company blanket authorization to do so. In *Pure Power Boot Camp*, following an employee's separation from employment, the employer

accessed the employee's personal online Hotmail account and other personal email accounts by using the username and password saved on the employer's computer.

However, in *Mintz v. Mark Bartelstein & Associates*, 885 F.Supp.2d 987 (C.D. Cal. 2012) the Central District of California found that an employee had only a limited expectation of privacy in his personal data on a device that he personally owned but also used for work. In an action for misappropriation of trade secrets, the employee moved to quash the employer's subpoena for the data on his phone, including the content of his text messages and their recipients, and the date, time, location, and duration of his phone calls. Because the employer had paid for the phone's service and the employee had signed a data policy acknowledging that he had no expectation of privacy in the phone's data, the court ordered the telephone carrier to produce all the requested data except the content of the employee's communications.

Statutory Protection

Disproportionate to the above protections, several state and federal statutes exist to protect the data of employers. One major source of protection is the Computer Fraud Abuse Act (CFAA), 18 U.S.C. §1030, which imposes civil and criminal penalties upon any person who gains "unauthorized access" to a "protected computer." Because "protected computer" is defined as any computer that affects interstate commerce, the CFAA protects against unauthorized access to any computer. Thus, the law provides employers recourse against employees who gain unauthorized access to any employer data through a company computer.

A circuit split currently exists regarding the scope of the term "unauthorized access" under the CFAA. The Fourth and Ninth Circuits have interpreted the term narrowly to exclude mere misuse of employer information or breach of an employer's computer use policy, interpreting the CFAA to apply only when an employee accesses a computer she has no authority to use. Conversely, the First, Fifth, Seventh, and Eleventh Circuits have adopted a broader interpretation of the term which encompasses any misuse of information that an employee is otherwise authorized to access, including use of computer resources in violation of an employer's computer use policy.

The CFAA's ambiguity in this respect could pose a significant threat to the privacy of employees' data. Specifically, because BYOD has blurred the line between employer and employee ownership of devices, as seen in *Mintz* above, an increasingly broad conception of the scope of "unauthorized access" under the CFAA could expose employees to liability simply for using dual-use devices in violation of employer BYOD or other data policies.

In addition to the CFAA, the Uniform Trade Secrets Act (UTSA), was recently adopted by every state except for New York and North Carolina, the District of Columbia, the Virgin Islands, and Puerto Rico. The UTSA endeavored to standardize varying states' definitions of "trade secrets" and to provide uniform remedies across each state. Under the UTSA, an employer is entitled to injunctive relief, in addition to attorney fees and actual damages, against employees who misappropriate trade secrets by "improper means."

Finally, the Economic Espionage Act of 1996 (EEA), 18 U.S.C. §1832, criminalizes the misappropriation of trade secrets with the knowledge that such misappropriation will damage the owner of the trade secret. Violations of the EEA are punishable by substantial fines and up to 10 years in prison.

Thus, a legion of state and federal laws exists to protect employer data against misappropriation, misuse, and unauthorized access by employees. Meanwhile, employees currently have a few meager protections against employers who commit the same actions with their personal data.

Personal Security Breaches

In contrast to the ECPA (SCA and Wiretap Act), there has been federal and state legislation promulgated in an attempt to protect the consumer from information disclosure. To date, except for the Health Insurance Portability and Accountability Act of 1996 (HIPAA) which specifically calls for compliance in the workplace, these laws have not been used in the employment context.

The Gramm-Leach Bliley Act (GLBA), 15 U.S.C. §§6801 et seq., enacted in 1999, protects personal consumer information (including electronic information) received by institutions that extend credit such as banks, car dealerships, and mortgage companies. In addition to some state privacy laws, both statutory and at common law, many states have now enacted and amended laws that require companies that store personal data, such as Social Security numbers, drivers licenses, credit card numbers, etc., to protect this data through security programs.

HIPAA, already well known to employers, was established to provide federal protection for personal health information. Pursuant to HIPAA, health insurers and providers are required to implement technical, physical and administrative safeguards for protected health information (PHI) in electronic form. See 45 C.F.R. §§160 et seq. In the workplace, employers can be seriously fined for unauthorized disclosures under the act. See 42 U.S.C. §1320d-5(a); 45 C.F.R. §160.404(b); 74 Fed. Reg. 56123, 56131 (Oct. 30, 2009) (Office of Civil Rights may impose a fine of up to $50,000 for each violation).

On the state level, after one of the worst security breaches of consumer information in 2007, Massachusetts passed the most stringent data protection law stipulating security requirements for organizations that handle the private data of residents. The law is more formally known as "Standards for The Protection of Personal Information of Residents of the Commonwealth" (or 201 C.M.R. §17.00). Similar legislation exists in Nevada, California and Texas, and most states have imposed a statutory obligation on businesses to safeguard personal information and require that personal information be secured in electronic form and securely destroyed.

While most of these laws could in theory make an employer culpable if an employee's personal information is lost, stolen, hacked or accessed without authorization if stored on a dual use device or in the "cloud," the legislative goals and practical effects of these laws (again, outside of HIPAA) are not directed at protecting employee privacy. Rather, they have been limited to providing security notification in regard to "sensitive" personal information if a consumer's information is hacked, stolen or destroyed.

A legion of state and federal laws exists to protect employer data against misappropriation, misuse, and unauthorized access by employees. Meanwhile, employees currently have a few meager protections against employers who commit the same actions with their personal data.

Conclusion

While certain state and federal laws exist to protect unauthorized access to data or security breaches by businesses, there is no comprehensive protection for the personal data of U.S. employees who have tacitly signed on to these new BYOD policies. Worse, there are numerous state and federal protections of trade secrets and confidential information that go far beyond the reasonable protection of corporate data to create increased civil and criminal liability for employees.

This inequity demonstrates a need for the United States to pass data protection legislation similar to that which has existed in Europe since World War II and, which is becoming more stringent given BYOD policies in many countries. These EU protections, for example, limit a company's ability to access personal information on an employee's device without permission or without "just cause" to track and monitor an employee's whereabouts (without a substantial and reasonable business purpose), or to remotely wipe out an employee's data. Essentially, these laws protect the individual's privacy first and business data only when the individual's data is secure, making employers duty-bound to look after the personal data regardless of the ownership of the device. It is time for the United States to catch up.

WENDI S. LAZAR *is partner and co-chair of the executives and professionals practice group at Outten & Golden.*