IPADS, SMART PHONES, AND LAPTOPS, OH MY!!

HOW THE DIGITAL WORLD MAKES US BOTH MORE CONCEALED AND MORE EXPOSED

Julie Proscia and Michael Wong SmithAmundsen

The use of electronics and the digital world within business is almost a necessity these days. Can you even fathom working in your respective business without smart phones, iPads, tablets, laptops, computers and all of the apps, data systems, remote login and technology that go along with them? If not, you are not alone. In fact, the term "nomophobia" was coined during one psychology study to reference the anxiety that an individual feels without access to a mobile phone.

Conscious users regularly download security patches and operating system updates and ensure proper virus protection and malware programs are in place. But, how well do you know the potential liability and exposure you face due to the electronics and technology that your company uses? And, how often do you review your company's data retention and email policies?

The potential liability and exposure that companies face from electronics and technology can be broadly grouped as: (1) data breaches and (2) employment issues.

Data breaches and cyberattacks are the most commonly recognized issues as they often end up being front page news. A data breach can result in the disclosure of confidential business records and/or personal identifying information of employees or customers of the company. While much of the news focus is placed on concerns of third party hacks, note that employees are actually the number one cause of data breach incidents. More than half of companies surveyed in a study by Experian and the Ponemon Institute report a data breach caused by an employee's malicious or negligent act.[1]

Employment issues, while not recognized as commonly as data breaches, are a growing area of liability and exposure for companies. Issues can include the use of technology in hiring, social media, discrimination and harassment claims, wage and hour claims, unemployment issues, state and federal laws limiting access to stored communications, litigation and duty to preserve obligations, and policies conflicting with the National Labor Relations Act (NLRA).

Technology has placed information at our fingertips. This has expanded searches done by employers when reviewing applicants and investigating employees. In doing this review, employers must remember that information posted on websites and social media is not always reliable or true. Additionally, in doing such searches, employers risk learning about an individual's legally protected status that is unlawful to consider when hiring, firing or disciplining an individual.

Furthermore, employers must be aware of state and federal laws impacting background checks, privacy and access to social media accounts. The number of states enacting laws restricting employers' abilities to demand access to applicants or employees' personal social media accounts, usernames and/or passwords have continued to grow with an increased focus on the privacy rights of employees. Additionally, the Electronic Communications Privacy Act (ECPA), 18 U.S.C.A. §2510, and Stored Communications Act (SCA), 18 U.S.C. §§2701-2712, prohibit intentionally access-

ing stored communications without, or in excess of, authorization. For example, viewing an employee's emails on their personal account (e.g. gmail, hotmail, yahoo, etc.) because the employee stored a username and password in a company browser is considered a violation of the ECPA and SCA.

Similarly, these laws place employers in a delicate position when investigating claims of employee harassment, discrimination and misconduct. Discrimination and harassment via text message, email, instant messages, and posts on social media is unlawful conduct that, even when done outside of the workplace, an employer may be liable for allowing, especially if aware of the conduct or if the conduct was done using the employer's electronic device. In fact, the EEOC and courts have started to question whether complaints and comments on social media constitute protected activity. Can employee communications on social media be sufficient to put employers on notice of protected activity? Can monitoring the use of electronic devices or social media use of one employee, but not others, be considered discriminatory or retaliatory? Can an employer's electronic device use or social media presence or policy be considered retaliatory? More and more the EEOC and courts are starting to find that the answers to these questions are "yes." For example, in *Espinoza v. County of Orange*, No. G043067, 2012 WL 420149 (Cal. App. 2012), the California Court of Appeals upheld a $1.6 million verdict against an employer for failing to address harassment by co-workers of the plaintiff via a blog. Additionally, in more and more cases, discriminatory or harassing text messages, emails and social media posts are being used as evidence.

Similarly, the use of electronics to track time and allow employees to connect and work remotely has opened the potential for wage and hour claims. Indeed, there have already been a multitude of claims alleging non-exempt/hourly employees reviewing and responding to phone calls, emails and text messages outside of work is compensable work time. These claims have typically been limited by the fact that, generally, non-exempt/hourly employees have not been provided cell phones, tablets, laptops or the ability to remotely log in. However, with the decrease in the cost of technology and the potential increase in the salary basis for exempt employees, it is expected that more hourly employees will be provided these tools and the number of these claims will increase. To limit potential liability and exposure from these types of claims, take notice of the ruling in *Allen, et al. v. City of Chicago*, Case No. 10-C-3183 (N.D. Ill. Dec. 10, 2015) in which officers alleged they were performing compensable work when checking their cell phones and electronic devices while off-duty. The court in Allen found for the employer, noting that although there was a procedure for officers to report off-duty work, the officers did not follow that procedure and there was no proof supervisors knew officers were working on their devices off duty. Following this decision, employers should maintain and enforce policies prohibiting non-exempt/hourly employees from doing work outside of regular working hours without authorization, limit access to technology that such employees may use outside of work, recognize when such employees are doing work outside of regular working hours and provide a method for such workers to report work done outside of regular working hours.

Technology policies that companies should consider incorporating in an employee handbook include: (1) no expectation of privacy policy; (2) workplace monitoring of computer usage; (3) limitation of personal use policy; (4) restrictions or limitations on website and social media posts; (5) mobile phone and camera policy; and (6) file management and record retention policies. These policies should be drafted to ensure employees understand company expectations as well as their right of privacy within the workplace. In drafting these policies, both union and non-union employers must be aware of the NLRA and the National Labor Relations Board's (NLRB) position on technology and social media policies. The NLRB has issued a memorandum addressing technology and social media policies in employee handbooks, including what the NLRB considers to violate the NLRA. The NLRB's interest in recommending limitations on employer's technology policies is focused on making sure companies do not limit employees' Section 7 right to unionize, to join together to advance their interests as employees, and to refrain from such activity.

Additionally, in drafting a file management and record retention policy, companies must understand that they have the opportunity to be incredibly specific to each business and circumstance. Indeed, many businesses are subject to industry-specific record keeping obligations and, even with a single business, various departments have different considerations that need to be taken into account. Rarely, is it appropriate for one company to store and maintain its data in a method that is identical to that of another company.

As technology evolves, employers' policies will also have to evolve to address how technology is used, what is stored and the types of data. For example, with the proliferation of laptops and mobile phones all of the different types of data and information that is stored on them must be considered, including, but not limited to, call logs, contacts, calendar entries, photos, videos, emails (work and personal), text messages, location/GPS data, internet browsing history, and electronic files (including documents, lists, records and other files). In drafting retention policies, it is important to involve multiple individuals to make sure that the policy properly addresses both the business needs and legal obligations of the company.

Often, just as important to crafting a proper and useful policy, is involving the person (or people) with the most knowledge of how data is used and stored within your business. All too often, the problem of a lacking or outdated policy is not discovered until one of two instances occurs: 1) a company is facing the exorbitant expense of responding to electronic discovery requests in the course of litigation; or 2) an employee (or former employee) has misappropriated confidential and proprietary business information. Don't wait until your operating system is infected with one of these viruses. Update your record retention and data policies annually. Finally, implement and provide regular training on the technology policies. A policy is only effective and worthwhile if it is followed and complied with by employees. Implementing training that employees understand and can easily comply with is just as important if not more, than having the right policies in place.

Julie Proscia is a partner with SmithAmundsen in St. Charles, Illinois. She navigates employers of all shapes and sizes, including not-for-profits and municipal employers, through a wide range of labor and employment law issues. jproscia@salawus.com

Michael Wong is a partner with SmithAmundsen in St. Charles, Illinois. He advises and represents clients in labor and employment issues arising under state, federal, and administrative laws. mwong@salawus.com.

[1] Managing Insider Risk Through Training and Culture, Experian,2016, http://www.experian.com/data-breach/2016-ponemon-insider-risk.html?WT.srch=2016_insider_risk_pr