The Legal Intelligencer

THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2015

PHILADELPHIA, TUESDAY, JUNE 23, 2015 VOL 251 • NO. 119 An ALM Publication

Best Practices for Mobile Device Data Security

BY ABRAHAM J. REIN

AND CAROLYN H. KENDALL

Special to the Legal

In 2014, it became official: There now are more active mobile devices in the world than people, according to data compiled by GSMA Intelligence and the U.S. Census Bureau.

The rise in mobile devices is not confined to personal use; mobile devices increasingly play an integral role in many business operations. We rely on mobile devices to communicate with clients, frequently using them to exchange sensitive data. Health care professionals use mobile technology when interacting with and treating patients. Countless workplaces expect employees to be available on-demand via mobile devices. Mobile devices transmit, receive and store a treasure trove of valuable data, which, if compromised, can be used by bad actors to steal identities, access bank accounts, file false tax returns, misappropriate trade secrets and more. Safeguarding this sensitive data is important to all businesses, both to ensure client confidence and to comply with a complex patchwork of legal obligations. Therefore, businesses, including law firms and attorneys, must be cognizant of the risks involved in using mobile devices and vigilant about following best practices for mobile data security.

ABRAHAM J. REIN *is an associate in Post & Schell's data protection/breach and internal investigations and white-collar defense practice groups in Philadelphia. He counsels corporate enterprises and individuals on the prevention of data security breaches and compliance with related state and federal regulations, and defends them in related investigations and criminal proceedings. Contact him at arein@postschell.com.*

CAROLYN H. KENDALL *is an associate in the firm's data protection/breach and internal investigations and white-collar defense practice groups in Philadelphia. She conducts internal investigations and defends corporations, officers and other individuals facing criminal and civil investigation, as well as counsels them on the prevention of data security breaches, and compliance with related state and federal regulations. Contact her at ckendall@postschell.com.*

MOBILE DATA SECURITY RISKS

Mobile devices, and by extension the data stored on and transmitted by them, are uniquely vulnerable. First, by their very nature, mobile devices are more easily lost or stolen than computers. Second, because they rely on wireless connections, data transmitted by mobile devices is more vulnerable to undetected interception while in transit.

Thefts of mobile devices are on the rise. According to Federal Communications Commission Commissioner Jessica Rosenworcel, one in three robberies includes the theft of a mobile device. Moreover, it is all too easy to lose a mobile device, especially if an employee uses one device for both business and personal use, carrying it virtually everywhere he or she goes. If a mobile device is lost and not properly secured, it is relatively easy for bad actors to gain access to the device and the data stored on it, including emails and their attachments. Depending on whether employees store sensitive information like passwords and access information for other services or sites in their email folders, a thief can find a gold mine of data from just one device.

Additionally, scams to intercept wireless data transmissions are all too common. In one classic scheme—far from the only one—a bad actor will set up a

free public WiFi hotspot, give it an appealing name, and simply pull down all the data that unsuspecting users transmit across it. If that data is unencrypted and includes sensitive information, the trick has been a success.

THE LEGAL LANDSCAPE

Persons and entities that handle or store sensitive data, especially data containing clients' financial, health or other identifying information, are subject to an ever-evolving patchwork of state and federal regulation regarding protecting this data. For example, many states, including Pennsylvania, require these entities to inform customers in the event of a breach. Pennsylvania's Breach of Personal Information Notification Act imposes notification obligations on "any entity that maintains, stores or manages computerized data that includes personal information" in the case of a data breach. Generally, if the personal information was unencrypted, the entity must notify customers if their personal information "was or is reasonably believed to have been accessed and acquired by an unauthorized person." However, if the data was encrypted, then notification is required only if the data was accessed in unencrypted form or if the breach involved the encryption's security.

Currently there is no general federal data breach notification law, although several recently have been proposed. However, the Health Insurance Portability and Accountability Act of 1996 imposes a notification requirement when unsecured protected health information, like individually identifiable health information, "has been, or is reasonably believed ... to have been, accessed, acquired or disclosed." This obligation is imposed not only on health care providers and insurers, but also on their business associates that receive, handle or use protected health information.

Other federal laws also address data security and the protection of personal information. For example, the Federal Trade Commission uses its broad consumer-protection authority to protect consumer privacy and personal data from improper disclosure. The FTC enforces the Gramm-Leach-Bliley Act, which protects nonpublic personal information from unauthorized disclosure by financial institutions. Financial institutions also must comply with the FTC's red flags rule, which obligates them to undertake periodic risk assessments to determine whether they are required to implement a written identity-theft prevention program. Finally, the FTC also brings enforcement actions against individuals and entities that have misused or improperly disclosed consumer data, or failed to take "reasonable" precautions to protect it. According to reported enforcement actions, violators frequently are required to revise or implement comprehensive privacy and data security programs, delete illegally obtained consumer information, and notify consumers whose data has been improperly disclosed.

BEST PRACTICES TO SAFEGUARD

MOBILE DATA

This combination of factors—countless devices storing and transmitting vast and valuable data, vulnerability to infiltration, and a mosaic of regulation—makes mobile device security a crucial area for any business. To protect data stored on mobile devices, consider implementing the following recommendations:

• Physically encrypt mobile devices.

Device encryption and SIM card encryption are available on almost all smartphones and other mobile devices, and prevent bad actors from accessing stored data even if the device is physically dismantled. Physical encryption is stronger than simple password protection because it cannot be defeated with specialized software.

• Strong passwords still are important.

Require mobile devices to be password-protected, and consider requiring alphanumeric passwords or passwords longer than four characters. Discourage employees from using easy-to-guess passwords.

• Have a plan for lost devices.

Install software capable of remotely wiping data from the mobile device if it has been lost or stolen. Also train employees to notify information technology staff immediately in the event of a loss.

• Separate personal from work.

If employees are permitted to bring their own devices to work, ensure that business data is segregated and cannot be downloaded or locally saved onto the personal device. Readily available software can assist with this.

• Maintain control of settings.

Ensure that devices used for work, whether provided by the company or employees' own devices, cannot install applications that can modify key security settings, and ensure that employees cannot modify security configurations without information technology authorization.

• Train employees to minimize risk of physical loss.

Train employees to be mindful of their devices' security, including safeguarding them while traveling.

To protect data transmitted by mobile devices, consider implementing the following recommendations:

• Do not use free public WiFi.

Data transmitted over wireless connections can be seen by the provider. Scammers frequently set up free public hotspots and intercept data transmitted by unsuspecting users.

• Encrypt email.

Many companies encrypt their email, as do major free email providers like Gmail. If not automatically encrypted, encrypt emails containing sensitive financial or protected health information. When exchanging sensitive information with business partners, determine whether they encrypt email.

• Do not text sensitive data.

Texts are the most easily intercepted messages and generally are not encrypted, making their content easily accessible by bad actors.

Othniel Badea contributed to this article. •