3-3-2017

B.Y.O.D. – Bring Your Own Device

Jennifer Hwang
Cardozo Arts & Entertainment Law Journal

B.Y.O.D. – Bring Your Own Device

BY JENNIFER HWANG/ ON MARCH 6, 2017

Traditionally, employers have issued company-owned devices to their employees. This traditional approach has allowed employers to have more control of and access to employees' devices. Currently, employers are generally free to monitor its employees' text messages or online activity for business purposes. Under federal law, an employer is legally able to monitor or intercept its employees' oral, wire, or electronic communications in the ordinary course of business.[1] The law provides employers with an ability to do so under two requirements: 1) the employer must provide the device to its employees to use for company purposes and 2) the device has to be used in the ordinary course of business.

In more recent years, employers have shifted to a more contemporary approach, implementing a Bring Your Own Device (hereinafter "BYOD") program.[2] The BYOD program allows employees to use their personal devices in the workplace for work-related matters. Companies secure their employees' devices by investing in a mobile device management solution to enforce policies and monitor its employees' usage and access.[3] Companies also enforce industry standard security policies, such as implementing a whole-device encryption and have the ability to remotely wipe all data and hard-drive memory once an employee leaves the company.[4] The BYOD policy raises a handful of privacy concerns because it blurs the line between personal and corporate usage, as well as the scope of employee monitoring.[5]

In two recent cases, there has been a split among district courts. In In Re Pradaxa,[6] the court found that the employer had control over its employees' text messages on their personal devices.[7] In this case, the employers alleged failure to preserve various types of evidence, including business related text messages that were on the employees' personal devices.[8] The court held that although it was the employer's responsibility to monitor and preserve text messages on company-issued phones, the employees here were also required to give up any business related text message sent and received from their personal phones.[9]

In another recent case, the court found that the employer did not have control over its employees' text messages on their personal devices.[10] The court held that the employer, Costco, was not required to uncover text message contents from its employees' personal devices because the text messages located on these personal devices were not within Costco's "possession, custody, or control."[11] As a result, the court did not allow the employer to receive the contents from its employees' personal devices.

The United States should follow the European Union's approach for employee monitoring. For example, the European Union implemented a new data protection framework, known as the

General Data Protection Regulation.[12] This regulation empowers data protection regulators to impose administrative fines of 20 million Euro for most violations or 10 million Euro for less serious violations.[13] Article 81 of European Union's General Data Protection Regulation implemented a stricter processing compliance method for the processing of employee data in the European Union.[14] The regulation applies to all European Union residents, regardless of citizenship. As a result, U.S. citizens living or working in European Union are entitled to all of European Union's regulation's protections.

The U.S. not only needs to follow the European Union's approach regarding privacy regulations, but it also needs to implement its own strict and uniform BYOD policy that does not implicate privacy law protections for employees. For instance, employers should be mandated to create a BYOD policy that is flexible and effective, yet one that limits security and privacy risks. Employers should be responsible for creating secure security measures for the BYOD devices and also educating its employees on the risks and benefits of participating in a BYOD program. Companies may do so by conducting extremely informative orientation meetings for new hires. In this orientation, the company could lay out the specific functions and utilities of BYOD devices. It should further stress the harms that come with using the BYOD program and also state that employees have the option of being given a company-issued phone.

New technology tools, such as the BYOD programs have increased the ability for employers to track, observe, and monitor their employees. It is important to try and keep up with this groundbreaking advancement of technology and implement appropriate regulations to protect the privacy interests of employees.

Jennifer Hwang is a second-year law student at Benjamin N. Cardozo School of Law and a Staff Editor of the Cardozo Arts & Entertainment Law Journal. She is interested in privacy law and looks forward to a career in Intellectual Property.

---

[1] 18 U.S.C. § 2510(5)(a) (2010).

[2] Dean Evans, *What is BYOD and Why is it Important?*, TechRadar.Pro, http://www.techradar.com/news/computing/what-is-byod-and-why-is-it-important-1175088 (last visited February 12, 2017).

[3] *Id*.

[4] *Id*.

[5] Mary Shacklett, *10 BYOD Concerns That Go Beyond Security Issues*, TechRepublic, http://www.techrepublic.com/blog/10-things/10-byod-concerns-that-go-beyond-security-issues/ (last visited February 12, 2017).

[6] In Re Pradaxa, No. 3-13-cv-51582-DRH-SCW, 2013 WL 6486921 (S.D. Ill. Dec. 9, 2013).

[7] In Re Pradaxa, 2013 WL 6486921, at *18, *20.

[8] In Re Pradaxa, 2013 WL 6486921, at *1, *16.

[9] In Re Pradaxa, 2013 WL 6486921, at *18.

[10] Cotton v. Costco Wholesale Corp., No. 12-2731-JW, 2013 WL 3819974 (D. Kan. July 24, 2013).

[11] Cotton, 2013 WL 3819974, at *6.

[12] *Reform of EU Data Protection Rules*, Justice, http://ec.europa.eu/justice/data-protection/reform/index_en.htm (last visited February 15, 2017).

[13] Philip Gordon, *Ten Steps for U.S. Multinational Employers Toward Compliance With Europe's New Data Protection Framework – The General Data Protection Regulation*, Littler, https://www.littler.com/publication-press/publication/ten-steps-us-multinational-employers-towards-compliance-europe%E2%80%99s-new (last visited February 15, 2017).

[14] *The European Parliament proposal for the new EU General Data Protection Regulation may severely restrict European epidemiological research*, PMC, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4033829/ (last visited February 15, 2017).