PUBLICATION

Florida Employee Privacy Alert: No Expectation of Privacy for Contents of Employee's Flash Drive Attached to Work Computer

Authors: Aldo M. Leiva, Jonathan Cromwell Hancock
August 07, 2019

Can an employee bring a claim against an employer if the employer bases an employment-related decision on information obtained from a personal data storage device? On June 26, 2019, the Florida Third District Court of Appeals answered that question by holding that a former police employee had no reasonable expectation of privacy in a personal flash drive that was plugged in to her work computer. The employee had been convicted of official misconduct for falsifying police reports in an effort to get her husband fired from his job. On appeal, the employee argued that the trial court had erred in admitting the evidence obtained from her flash drive because the drive was her personal property, and she otherwise normally kept it in her possession. In rejecting the argument, the appellate court identified several factors that established that the employee had no expectation of privacy in the contents of the flash drive:

1. The employee shared an office with a co-worker who had access to the employee's computer at all times because the employee left a sticky note with her computer password on her desk for that purpose;

2. The work computer contained a login banner that clearly warned users about the police department's computer policy, which included language confirming that the computer was for authorized use only and that ***all*** uses of the computer system were subject to monitoring, recording, copying, or auditing, followed by an acknowledgement of consent to use of the computer under these conditions;

3. The employer had a protocol that anything attached to the work computer, including external media, such as a flash drive, is deemed to be part of the employer's computer system; and

4. The employee had left the flash drive plugged in to her work computer, which was seized along with the computer as part of an internal investigation into the allegations.

Although issued within the context of an official misconduct case, the decision reinforces Florida case law on the subject of limits on employee privacy and emphasizes the key role of employer privacy policies and employee acknowledgements of such policies. In addition to serving as an administrative safeguard to mitigate against such risks as employee theft, misconduct, and violation of any applicable non-competition agreement, clear delineation of such policies are useful in any subsequent litigation involving the employee, where privacy rights may be raised by the employee for various tactical reasons.

The facts of the case also serve as a reminder to employers to think about what their policies and practices allow or prohibit, and to consider instituting proper controls to manage the use of flash drives on workplace computers, as such devices may be used to download employer data, contacts, or trade secrets. From the employment litigation perspective, an early comprehensive litigation hold letter may include specific reference to any flash drives or similar portable media that are connected to employer computer networks at the time the hold letter is issued, with a clear prohibition on removal of any such devices that have been connected to the employer's computer network as of the time of the litigation hold letter. But as the Florida court demonstrated,

an employee's claim to privacy may be rendered unreasonable when clearly communicated policies and related notices undermine the reasonableness of that employee's expectation of privacy. Does this holding apply to an employee's public social media posts or to emails sent and received on a personal email address? These questions and others like them all warrant a closer look at how this information is addressed by an employer, as waiting until there is an issue will likely mean the Company is unprepared to address it.

If you have any questions regarding these issues or any other data privacy or security-breach related issues, please contact the authors of this article or any of the attorneys in Baker Donelson's Data Protection, Privacy and Cybersecurity Group or Labor and Employment Practice Group.