



Judge's Ruling May Provide Clues to the Outcome of Employee's 'Dropbox' Privacy Suit





Earlier this year, a judge from the Western District of Pennsylvania acted on behalf of employee privacy rights when she partially denied a public employer's motion to dismiss a suit that accused it of violating the plaintiff's Fourth Amendment rights.

As summarized on Mondaq.com, Elizabeth Frankhouser, an employee of an educational facility, used her personal Dropbox account to store personal and workplace data. Hence, a link to Dropbox was on her workplace screen, though no data contained in the account was on that device because Dropbox data is stored in the cloud. The account was password protected as well.

The employer allowed the use of that Dropbox account for work-related matters, which resulted in Frankhouser adding a mix of workplace content to her personal content, which included photos that "could be considered borderline explicit." An IT administrator was aware of a spreadsheet on the employee's device that included passwords, and he used it to access the Dropbox account. There, he came upon the "borderline" photos and forwarded them to higher authorities in the school district. Soon, the district forced Frankhouser to resign for storing inappropriate content on workplace computers, which violated the employer's policies, according to the Mondaq article.

"Not surprisingly," writes the article's authors, "Ms. Frankhouser filed a lawsuit alleging Fourth Amendment violations and invasion of privacy claims along

with additional federal and state law claims."

The plaintiff claimed she had a reasonable expectation of privacy because she did not view or store the photographs on the workplace computer – Dropbox stores them in the cloud. In response, the defendants called for dismissal because Frankhouser didn't have an expectation of privacy because she often accessed the account at work; and she violated company policy by having the photos in her account.

Judge Kim R. Gibson sided with Frankhouser, citing the content was neither housed on nor accessed via the workplace computer or servers. In declining the request for dismissal, Gibson affirmed that Frankhouser had a reasonable expectation of privacy because the Dropbox account was her own account, was password protected, and was never used to access or download the photos while on the employer's system.

The authors (Ingrid A. Beattie, Cynthia J. Larose, and Jennifer R. Budoff) note that "while this case is in the early stages of litigation . . . this decision certainly raises considerations for employers to face." They suggest that workplace policies (which are rarely failsafe) include a statement that the employer has the right to monitor employees' emails and actions while using their devices; and that employers should prohibit the use of certain applications like Dropbox and anything cloud-based that might mingle personal and private data.