Published on *The National Law Review* https://natlawreview.com

Employers Beware: Judge Greenlights Employee's Privacy Lawsuit Over Dropbox Access

Article By:

Cynthia J. Larose

Jennifer R. Budoff

Many employers maintain policies limiting their employees' expectation of privacy in the workplace, including policies that eliminate any expectation of privacy when using company-issued electronic devices. While employers may think that having such a policy would protect them from invasion of privacy claims under the Fourth Amendment or state law, a recent federal court decision may cause employers to think otherwise. This post examines this decision and provides best practices for avoiding issues with employees' privacy interests.

On March 19, 2019, Judge Kim R. Gibson from the Western District of Pennsylvania partially denied a public employer's motion to dismiss, permitting the Plaintiff Elizabeth Frankhouser's claim for Fourth Amendment violations, as well as her state law claim for invasion of privacy, among others, to move forward.

The Facts

Plaintiff was the Executive Director of Defendant Clearfield County Career and Technology Center ("CCCTC"), an educational facility and, importantly for purposes of this case, a public employer. Plaintiff's position required extensive work on her work computer and Defendant Franklin Walk, CCCTC's Internet Technology Administrator, was responsible for resolving any work-related computer problems, including reloading and re-synching applications on the computer, such as Dropbox.

For those readers unfamiliar with the application, Dropbox is an application that enables users to store files on the "cloud" and access those files using a login on any internet-connected device. Importantly, synching a Dropbox account with a device does not save files on the hard drive of that device, rather it provides an access point for files stored remotely in the Dropbox cloud.

Although Plaintiff's Dropbox account was private, CCCTC authorized its use for work-related matters and thus the account contained both personal and work-related folders, including personal photographs. Among the personal photographs were two photographs of Plaintiff's boyfriend that "could be considered borderline explicit," as well as photographs of Plaintiff at parties.

Plaintiff's Dropbox account was accessible only with her username and password, which were listed on an excel spreadsheet that she used to store various personal and work-related usernames and passwords. Mr. Walk knew of the spreadsheet and used Plaintiff's Dropbox username and password to access her Dropbox account. Mr. Walk then took some of the personal photographs from the account and gave them to Defendant Doug McClelland, CCCTC's Truck Driver Recruiter, who delivered them to Mr. Paladina, CCCTC's Superintendent of Record and Mr. Jefferies, a member of CCCTC's School Board, Joint Operating Committee President and Plaintiff's supervisor.

In August 2017, Mr. Paladina and CCCTC's Superintendent, Michelle Dutrow, accused Plaintiff of storing naked photographs and other inappropriate pictures on her CCCTC-issued computer and cellphone in violation of company policy. Later that month, Mr. Paladina informed Plaintiff that she would be forced to resign.

Not surprisingly, given the circumstances surrounding her termination, Ms. Frankhouser filed a lawsuit alleging Fourth Amendment violations and invasion of privacy claims along with additional federal and state law claims.

The Court's Holding

The Fourth Amendment prohibits unreasonable searches and seizures in situations in which a person has a constitutionally protected reasonable expectation of privacy. To make this determination, a court must consider whether an individual has demonstrated a subjective expectation of privacy in the challenged search. Although often associated with criminal cases, the Fourth Amendment's protections apply when the government acts in its capacity as an employer. Specifically, in the workplace context it has been held that public employees are entitled to a reasonable expectation of privacy in their place of work.

As to her Fourth Amendment claim, Ms. Frankhouser argued that she had a reasonable expectation of privacy in her Dropbox account because she did not view or store the relevant photographs on her CCCTC-issued computer (they were in the "cloud").

Defendants moved to dismiss asserting that: (1) Plaintiff did not have an expectation of privacy in information stored in her Dropbox because she accessed the account frequently at work; and (2) she violated company policy by keeping the photographs in her account. In support of their argument CCCTC referenced their Board Policy Manual which stated in part that "Users [of CCCTC's computer resources] shall have no expectation of privacy in anything they create, store, send, delete, receive, or display on or over the Career Center's Internet, computers or network resources…". While Judge Gibson refused to consider the Board Policy Manual at the motion to dismiss stage, she stated that it would not have changed her ruling even if she did. Judge Gibson reasoned that Plaintiff's allegations do not fall clearly within the boundaries of the policy since she alleges she never housed her personal files on CCCTC's computers or servers, nor did she access any of her personal files through CCCTC's computers or servers.

Ultimately, the Court determined that Ms. Frankhouser did, in fact, have a reasonable expectation of privacy with respect to her personal Dropbox material for the following reasons: (1) it was her own private account, (2) it was password-protected, and (3) Plaintiff never accessed or downloaded the photographs while on CCCTC's system. As such the Court declined to dismiss the Fourth Amendment and invasion of privacy claims.

Notably, the crucial allegation here appears to be that Ms. Frankhouser did not store or view the

personal photographs from her Dropbox account on her work computer. Rather, while at work and on her employer's system, she used the account solely for business-related purposes.

While this case is in the early stages of litigation and the Defendants could ultimately prevail in the end, this decision certainly raises considerations for employers to face.

Takeaways for Employers

- Revisit Workplace Privacy Policies and Practices. As stated at the beginning of this post, it is fairly common place for employers to maintain a policy regarding employees' expectations (or lack thereof) of privacy in the workplace. This policy should include a notice to employees of the employer's right to monitor employees' emails and activities while using their employer's systems. However, such a policy is not failsafe, and caution should be taken in accessing and searching an employee's private or personal accounts. For example, only authorized manager-level employees with a legitimate business need should be able to do so.

- Prohibit Use of Certain Applications. As this decision illustrates, employers should consider prohibiting employees from using applications such as Dropbox for both personal and business-related purposes and/or limiting employees use of these applications on their work computers altogether. In particular, cloud-based applications can cause headaches for employers, particularly where there is a mix of private and business material stored in the cloud.

- Public Employers Take Extra Caution. Public employers should take additional precautions, keeping in mind that their employees have a greater expectation of privacy in the workplace than their private employee counterparts.

As always, it is a good idea to have counsel review any company policy regarding employees' expectations of privacy, and employers should consider consulting counsel if questions arise regarding the legality of a search of employee documents or property.

National Law Review, Volumess IX, Number 87