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

Use Of Personal Cloud-Based Document Accounts Requires New Strategies By Employers

Article By:

V. John Ella

Whether ***Google Docs***, ***Dropbox***, or some other file sharing system, employees, especially millennials and other digital natives, are increasingly likely to set up personal cloud-based document sharing and storage accounts for work purposes, usually with well-meaning intentions, such as convenience and flexibility. Sometimes this is done with explicit company approval, sometimes it is done with tacit awareness by middle management, and often the employer is unaware of this activity.

When an employee quits or is terminated, however, that account, and the business documents it contains, may be locked away in an inaccessible bubble. Worse, the employee could access trade secrets and other information stored in the cloud to unfairly compete. For example, in 2012, the computer gaming company Zynga sued a former employee for uploading trade secrets onto the employee's personal Dropbox account before leaving to work for a competitor. At a minimum, it may take time to recover the information or obtain the user name and password from the former employee. Storage of proprietary information, especially personally identifiable information (PII) on personal cloud accounts also increases the risk of a company data breach if the information is hacked. Finally, allowing business documents to be stored outside of the system can also create headaches when enacting a litigation hold or responding to electronic discovery requests in litigation. What should employers be doing now, to address this trend?

Institute Written Policies Regarding Use of Cloud-Based Storage Accounts

Companies should consider issuing clear policies on the use of personal cloud-based accounts for work purposes, before the litigation storm clouds gather. The most straightforward approach, utilized by many employers, is a strict prohibition on use of personal accounts to store any company-related information. Another option for smaller companies who rely on cloud-based computing or storage for cost reasons or flexibility is to select a secure system controlled by the employer with a requirement that employees record user name and passwords for all accounts with the company, and have them acknowledge that the password and user name are property of the company. (A similar policy is important for company social media accounts like Twitter, Facebook, and LinkedIn) A written policy may merely dissuade use of secret cloud storage accounts and not completely eliminate problems in this area, but a clear directive also allows an employer to show a court that a former employee was violating company protocol and may hasten recovery of documents if the employee is uncooperative in returning the information. More importantly, the lack of a policy addressing cloud-based storage accounts could be used to show that the company failed to take reasonable measures to protect the confidentiality of its trade secrets, which could lead to a loss of legal protection.

Address Recovery of Any Stored Files When an Employee Departs

The task of recovering company property from terminated employees has become greatly complicated by the use of Google Docs, DropBox and similar applications. Employees are also increasingly likely to send documents to their cloud-based email accounts such as Gmail.com for offsite use. HR professionals should ask departing employees the direct question of whether they have ever stored company documents on the cloud. If so, a company representative may need to insist on personally witnessing the former employee delete the items from her account, including the "trash" file. The company may want to first retain a copy of what was sent or stored as evidence if there is a concern about unfair competition or possible litigation. Pursuant to the maxim of "trust but verify", forensic searches of the departing worker's computer are critical if there is any suggestion of competitive intent.

Incorporate Cloud-Based Storage Accounts in Your Litigation Strategy

Litigators need to tailor discovery to address these cloudy issues as well. An employee sued for breach of non-compete may state under oath that he has not "taken" any information or documents from the company, only to have it revealed later that he had been storing customer information on a spread sheet on Google Docs for the past four years while employed, and that he continued to have access to the information after he left. Did he "take" the documents or did he just know where they were parked? Interrogatories should ask about any information stored on the cloud or accessible to the former employee, not just information in the employee's "possession."

One thing is for sure, employers need to get their corporate head out of the clouds, because employee use of personal cloud-based document management is only increasing.

National Law Review, Volume VI, Number 64

new-strategies-employers