Will Gmail's New Security Features Complicate eDiscovery?

Tad Simons August 13, 2018

Topics: Artificial Intelligence, Data Analytics, ediscovery, Efficiency, Law Firms, Legal Innovation, Midsize Law Firms Blog Posts, Small Law Firms

Google's recent update of its Gmail platform added security features that will soon make it possible for lawyers to have more secure communications with their clients. But those same features may prove problematic in the future when it comes to eDiscovery — specifically when lawyers ask to see electronic records in a case, and those records no longer exist.

According to Brian Schrader, president and CEO of the New York-based eDiscovery firm BIA, Gmail's new security features, while laudable, may have unforeseen and unintended consequences in the area of eDiscovery. "Some of Gmail's new security features, such as automatic expiration and two-factor authentication, are great from a security standpoint," Schrader says. "But both of those features could make eDiscovery extremely difficult, if not impossible."

For example, Gmail's new "confidential" mode allows users to set an expiration date on emails, which is essentially a self-destruct feature — or to "revoke" an email, even after its been read. In theory, this makes it possible for an individual user to destroy emails they don't want others to see, preventing those communications from being used in future litigation. Likewise, two-factor authentication would prevent anyone without the proper pass-code from reading an email, making it impossible, as a practical matter, to read large volumes of encrypted documents.

"If either of these features is turned on, attorneys responsible for examining documents and deciding what is responsive and relevant for litigation would probably never see them," Schrader says. These days, eDiscovery in corporate litigation often involves millions of emails, and attorneys use various types of machine-intelligence search engines and predictive-coding technologies to identify relevant documents. "If Gmail's new security features are enabled, they would not be indexed or searchable, and would probably show up as an error or exception" — or not show up at all, Schrader explains.

> *"Some of Gmail's new security features, such as automatic expiration and two-factor authentication, are great from a security standpoint. But both of those features could make eDiscovery extremely difficult, if not impossible."*
>
> ***—Brian Schrader, president and CEO of BIA***

This is not an entirely new problem for Schrader's company, BIA, which specializes in large-batch corporate eDiscovery. Microsoft Outlook has had a similar email expiration feature for a while now, though not many people know about it or use it. Still, it has presented challenging issues in eDiscovery, Schrader says, because the data-gathering bots that are used to comb through electronic communications can't read data that isn't there.

There are still plenty of questions about how Gmail's new features will actually impact eDiscovery in practice, because they haven't yet been released to G-Suite users and consumers, only enterprise users in Google's early-adopter program. But whatever happens, Schrader says he doesn't think the issues involving eDiscovery will be resolved anytime soon.

"There is a growing discrepancy between the legal disclosure requirements that come from government investigations and the privacy technologies that are being developed by companies like Google, Apple, and Microsoft," Schrader says. "This is the civil-rights battle of the next decade, and it's not going to be solved easily, because the goals are completely opposite. One side wants to hide everything and keep it as private as possible, and the other side wants the ability to see that information and compel people to disclose it."

In the meantime, things are bound to get more complicated as more communication platforms such as Snapchat and Secret are developed — platforms designed to erase all traces of communication — and as the barrier between enterprise data and individual data dissolves due to the fact that many people use a single smartphone for both business and personal use.

True, the privacy side got a boost from the US Supreme Court's recent decision in *Carpenter vs. the United States*that required the government to obtain a warrant for cellphone-tower location data, but more litigation around these issues is sure to come.