Legaltech news

Is Gmail's New Ephemeral Messaging Service a Threat to Data Retention?

Despite some potential problems with widespread use of Gmail's "Confidential Mode," the new ephemeral messaging function can be easily managed from an information governance perspective.

By **Rhys Dipshan** | June 22, 2018 at 08:00 AM

At first glance, the launch of Gmail's new **ephemeral** messaging feature known as "Confidential Mode," which is included in a batch of user interface updates to the service, may cause a fair amount of apprehension among e-discovery and information governance managers.

All emails sent using the confidential mode, for instance, are erased after a designated time set by the user. Until they are erased, they are stored directly on **Google's servers** instead of on a proprietary company-owned server. And even if a Gmail user sends an email under confidential mode to a recipient who is using a different email client, the recipient can only access that email via a website link that still connects to Google's servers.

Such a restricted, time-sensitive way of communication can run counter to a company's data retention efforts, or put them in legal risk during pretrial discovery. But apprehension around the tool may be naive. After all, such technology is nothing new, and much of the risk it poses can be vastly limited by how it is used in the first place.

Andy Wilson, CEO of e-discovery company Logikcull, explained that the any risk with Gmail's new updates is "totally dependent on how these businesses enable and police these types of features and functionality."

Confidential model, for example, can be managed at a high level for those using the corporate Gmail applications. “It’s an IT administrative feature” for enterprises, Wilson noted. “The users themselves cannot turn it on” without first being allowed to by a manager with administrative Gmail privileges.

It is also likely that many companies will have a relatively easy time managing such ephemeral messaging functions given that many have used them in the past. “It’s not just Gmail. This technology is not new. There are plugins that have existed for years that allow you to do all the same stuff,” Wilson said.

Indeed, Michael Powell, solutions analyst at ZL Technologies, noted that such tools have been commonly used for years by large corporations, government officials and financial institutions like banks to manage sensitive or confidential information and trade secrets.

Still, for e-discovery attorneys, the use of Gmail’s confidential mode be a red flag. Being unable to produce requested content because it was deleted, after all, can open up a party to **spoliation sanctions** in pretrial discovery.

But Powell has seen courts be “relatively understanding of these [functions] as long as companies have policies that are spelled out,” and have some metadata for the deleted emails, such as information on when they were sent out.

And even if companies weren’t keeping track of their ephemeral emails, Wilson noted that “you can probably get metadata from Google if you really tried hard.” Still, he added that the content of emails in confidential mode are definitely erased from Google’s servers after their expiration as not doing so would violate Google’s terms of service.

However, this isn’t to say Gmail’s confidential mode erasure of emails is foolproof either. Wilson explained that users can “still make a copy of it either by downloading the email itself or taking a screenshot of it.”

To be sure, while nothing new, Gmail’s confidential mode may still present some problem down the road. The feature, for instance, introduces a level of ease to deploying ephemeral messaging that was

lacking in other older tools. “Gmail is going to make it easier for a lot of people to use this,” Powell said. And should more people use self-destructing email, it could pose a growing challenging for e-discovery attorneys and investigators.

Widespread use of such service may also pose cybersecurity challenges as well, especially given that all non-Gmail users will have to open received emails via a hyperlink. “If this does become more common and people are getting used to opening links to view their email that would be a really **potent attack vector** from a cybersecurity point of view,” Powell added.