Ephemeral Messaging for Businesses: Balancing the Risks of Keeping and Deleting Data by Default

By Avi Gesser, Daniel F. Forester & Mengyi Xu on May 15, 2019

One way for companies to decrease their cybersecurity risks, as well as their risks from new privacy regulations, is through data minimization—significantly reducing the amount of their data. By deleting old data and collecting less new data, companies will have less sensitive information to protect and process in accordance with their regulatory obligations. But getting rid of old data isn't easy, in part because of the legal limitations on what can be deleted. We have previously written **here** about these challenges, as well as the benefits of data minimization, which include reducing:

- the growth of a company's data over time, and the associated storage costs;
- lost productivity associated with searching large volumes of irrelevant data;
- the cybersecurity and privacy risks of having large volumes of unneeded data, especially considering CCPA and GDPR-type rights of access and erasure;
- internal audit and compliance risks;
- contractual risks (e.g., obligations to clients and customers to delete data once it is no longer needed); and
- the volume of documents that may be unhelpful to the company in potential, but not yet reasonably anticipated, litigation or regulatory inquiries.

As we noted, in light of these benefits and recent legal, regulatory, and technological developments, the current risks of keeping large volumes of old data may cause companies to reevaluate their long-term data management planning. Indeed, various cybersecurity and privacy regulatory regimes, such as GDPR and the NYDFS Cyber Rules, now require companies to have policies for disposing of nonpublic information that is no longer necessary for business operations, unless those documents must be retained for legal reasons.

One challenge to implementing data minimization is the tendency of many employees to keep all of their emails unless they are forced to delete them. To address this challenge, some companies are using tools that automatically delete emails after a certain short period of time—also known as ephemeral messaging. In the past, many businesses have had a similar process for voicemails, such as automatic deletion after 30 days, but ephemeral messaging is relatively new for business emails, which are usually kept forever or a long period of time by default.

In March of 2019, the DOJ **revised the provision on ephemeral messaging** in its FCPA Corporate Enforcement Policy. The original policy stated that a company would only receive full credit for remediation if it "prohibit[ed] employees from using software that generates but does not appropriately retain business records or communications." The revised provision requires that, in order to receive full remediation credit, companies must retain business records, and prohibit the improper destruction or deletion of business records, which includes

implementing “appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company’s ability to appropriately retain business records or communications.”

Although the revised guidance seems to open the door to some use of ephemeral messaging platforms, it provides little in the way of specifics as to what is expected.

Similarly, in December 2018, the **SEC’s Office of Inspections and Examinations issued a Risk Alert** reminding investment advisers of their recordkeeping obligations under Rule 204-2 of the Investment Advisers Act of 1940. The alert was likely issued due to the increased use of ephemeral messaging for business purposes, but provided no clear guidance on when it should and should not be used.

In order to provide some guidance, the Sedona Conference currently has a **working group dedicated to brainstorming best practices surrounding ephemeral data** retention and minimization.

Bearing in mind that any company policy on ephemeral messaging must meet its particular facts and circumstances, we are aware of some companies that have adopted a pragmatic risk-based approach, based on the following principles:

Business Records vs. Disposable Data

Some companies are implementing data management policies that classify data as either “Business Records” or “Disposable Data.” Business Records cover data that must either be kept for a significant period of time (a) for legal or regulatory reasons, or (b) because it has lasting business value. Any document that is not a Business Record is Disposable Data, which is not subject to any legal or regulatory retention requirement and does not have sufficient business importance to be retained for an extended period. These companies require that ephemeral messaging should only be used for communications that involve Disposable Data. They achieve this by classifying communication as either Primary or Secondary.

Primary vs. Secondary Communications

“Primary Communications” are work emails (and their attachments), which are automatically preserved for a long period of time. As a result, Primary Communications are the medium through which employees should communicate information that constitutes Business Records. “Secondary Communications” are communications that go through the company’s network or servers, but are preserved for a short period of time (e.g., 14 days before being automatically deleted). Secondary Communications, which are also referred to as ephemeral messaging services, may include voicemails, texts, instant messages, Slack, Symphony, and other company applications used for communications involving only Disposable Data, such as routine scheduling, other non-substantive business communications, and personal messages.

These companies direct employees not to use Secondary Communications to transmit Business Records, and if that happens, require employees to take affirmative steps to preserve the communication for the same length of time that Primary Communications are preserved (for example, by taking a screenshot and sending the image through the company’s email system). Relatedly, these policies often require employees who find themselves to be passive recipients of Business Records via Secondary Communications to move those messages to a Primary Communication channel.

This approach is consistent with the guidance provided in the SEC’s December 2018 Risk Alert, which provides:

In the event that an employee receives an electronic message using a form of communication prohibited by the firm for business purposes, requiring in firm procedures that the employee move those messages to another electronic system that the adviser determines can be used in compliance with its books and records obligations, and including specific instructions to employees on how to do so.

Some companies also have regular reminders in their Secondary Communication channels that these applications are not to be used for communicating Business Records. They are also combining their policies on ephemeral messaging with policies on the use of personal applications for company business, which we have written on separately **here**.

Again, although companies may find these general principles helpful, businesses must develop messaging policies that are tailored to their own practices and risks. We will continue to monitor developments in the regulation of ephemeral and personal messaging for businesses here and at the **Davis Polk Cyber Portal**, which is available to help clients meet their evolving cybersecurity and privacy obligations.

This article has also been posted at the Compliance & Enforcement **blog** sponsored by **NYU Law's Program on Corporate Compliance and Enforcement**.