Navigating Spoliation and Data Retention Issues in the Remote Workplace

BY WILLIAM R. DENNY, ESQUIRE AND CARSON R. BARTLETT, ESQUIRE

William R. Denny has a business and litigation practice, focusing on commercial and corporate transactions, vendor management, mergers and acquisitions, data privacy and security, and information technology. Mr. Denny is a Certified Information Privacy Professional (CIPP/US) and a Certified Information Privacy Manager (CIPM). He can be reached at wdenny@potteranderson.com.

Carson Bartlett practices general litigation at Potter Anderson & Corroon LLP in Wilmington. She can be reached at cbartlett@potteranderson.com.

Since the advent of the COVID-19 pandemic, companies are increasingly opting for the use of digital messaging platforms in the workplace, including instant messaging applications such as Slack and WebEx, and even ephemeral messaging applications such as Signal and Telegram. The accelerated transition to these new and varied forms of communication presents a significant challenge in the context of eDiscovery and data retention.

Further, as more and more employees are packing up their offices in the "Great Resignation," employers must be prepared quickly and effectively to preserve terminated employees' data when it may be relevant to litigation. This article addresses some of these remote workplace challenges and recommends best practices for approaching these issues.

Retention in the Remote Workplace

The use of messaging applications in the workplace has surged since the beginning of the COVID-19 pandemic, and, when litigation ensues, litigants and their counsel have an obligation to ensure that relevant data is properly retained, even data from more informal collaborative messaging systems like Slack or WebEx. Litigants must be aware of how the programs in use are storing data, how long that data is stored, and how that data can be accessed.

As organizations begin using new platforms, they must familiarize themselves with how these platforms store relevant data. With new messaging platforms come new data organization, file types, and data storage procedures. Litigants must be prepared to access and organize these data with very little notice.

Additionally, litigants must be cognizant of the different data retention timeframes used by various platforms. For example, programs are increasingly instituting auto-deletion settings to minimize storage requirements, so it is possible that data will be deleted without any affirmative action from the user.

Litigants and counsel have a duty to be aware of default auto-deletion settings and understand how they can be disabled or changed as soon as litigation is anticipated. A recent federal court decision, *WeRide Corp. v. Kun Huang*, Case No. 5:18-CV-07233, 2020 WL 1967209 (N.D. Cal. Apr. 24, 2020), underscores the importance of identifying and disabling these auto-deletion settings. In that case, the court found, among other violations, that plaintiff "violat[ed] its

duty to preserve" by setting its email settings to automatically delete emails after 90 days and "*maintaining that setting* despite knowledge that litigation was imminent." *Id.* at *3 (emphasis added).

The duty to preserve requires that litigants and counsel remain abreast of what messaging platforms are in use within their organizations as well as how those platforms store information, for how long, and how promptly to disable any auto-deletion policies. *See, e.g., Doe v. Purdue Univ.*, Case No. 2:17-CV-33-JPK, 2021 WL 2767405 (N.D. Ind. July 2, 2021) (awarding sanctions against plaintiff who failed properly to produce and understand the retention procedure for Snapchat data); *DR Distribs., LLC v. 21 Century Smoking*, Inc., 513 F. Supp. 3d 839, 867-68 (N.D. Ill. 2021) (discussing an attorneys' duty to be reasonably knowledgeable regarding a client's electronically-stored information).

In the remote workplace, auto-deletion is not the only danger to data retention. Litigants also must be proactive about retaining data while it is available and preventing users from destroying or deleting relevant data. Organizations should implement clear data retention policies, outlining when data can and cannot be deleted, as well as proper safeguarding procedures.

Data Retention During the "Great Resignation"

Another eDiscovery challenge in the digital workplace is the increase in employees leaving the workforce altogether, often termed the "Great Resignation." As more employees are turning in their resignations, there is an increased risk that exiting employees' data will be destroyed or lost in the process. For example, employees may delete data on their own, or their workplace accounts may automatically delete data following their termination. To prevent these losses, employers must update their termination procedures to safeguard relevant data that may be on the exiting employees' devices or workplace accounts.

The recent decision *In re Skanska USA Civ. Se. Inc.*, Case No. 3:20-CV-05980, __ F.R.D. __, 2021 WL 5226547 (N.D. Fla. Aug. 23, 2021), is instructive. There, plaintiff agreed to produce text messages from several of its employees' company cell phones. *Id.* at *1. Before those messages could be produced, multiple employees exited the company and deleted data from their mobile phones in the process, either on their own or at the direction of other employees. *Id.* at *1-2. The court ordered an adverse inference and monetary sanctions against plaintiff, specifically faulting its "wholesale failure to take any steps to collect the cell phone data … or, at minimum, to ensure the custodians were aware of and understood the litigation hold." *Id.* at *3. The court also highlighted plaintiff's failure to back up the phone data or "suspend its routine document destruction policies." *Id.* at *5.

Consequently, employers not only must implement clear data retention policies regarding termination of employment, they must ensure that those policies are understood and enforced by the managing employees who are involved in the termination process, not just corporate executives or attorneys.

Implications for Ephemeral Messaging Platforms

As digital communication has increased, so too have the variety of platforms available for use, including platforms that enable ephemeral, or transient, communication, such as Telegram and Signal. These platforms permit users to send and receive messages without leaving any trace of the messages' content. When it comes to eDiscovery, organizations should be cautious about the use of such platforms, which one court has described as "designed to disguise and destroy communications." *Herzig v. Ark. Found. For Med. Care, Inc.*, Case No. 2:18-cv-02101, 2019 WL 2870106, *5 (W.D. Ark. July 3, 2019). The use of such services after a litigation hold is in place has also led courts to sanction litigants in the form of an adverse inference. *FTC v. Noland*, Case No. CV-20-00047-PHC-DWL, 2021 WL 3857413, *14 (D. Ariz. Aug. 30, 2021).

In *FTC v. Noland*, defendants began using the application Signal, with its auto-deletion function enabled, shortly after learning that they were under investigation by the FTC. *Id.* at *1. In subsequent litigation, the FTC sought an adverse inference sanction against the defendants for spoliation of evidence. *Id.* at *5. The court found that defendants' "systematic efforts to conceal and destroy evidence" warranted such a sanction. *Id.* at *1.

While ephemeral messaging may have advantages, the *FTC v. Noland* decision cautions against the use of such messaging platforms when litigation is anticipated or a litigation hold is in place. To avoid exposure to sanctions, organizations should enforce policies that prohibit the use of such messaging platforms for communications relevant to anticipated litigation. Additionally, to the extent the application's settings or other technical processes enable storage of ephemeral data, organizations should become familiar with them. Organizations should also update their data retention policies to reflect the use of ephemeral messaging platforms and require retention of any data generated by these platforms. *See* The Sedona Conference, *Commentary on Ephemeral Messaging*, 22 SEDONA CONF. J. 435, 474-75 (2021).

Conclusion

The remote workplace and the technology it utilizes are constantly evolving, and litigants' eDiscovery practices must keep up. By regularly reevaluating and refining data retention policies and approaching new technologies with caution, litigants can effectively mitigate spoliation and data retention risks.