CASE FOCUS

District Court Cuts Litigants No Slack for Failing to Produce Corporate Instant Messaging Data Resulting in Default Judgment

April 26, 2023 Spring 2023 Vol. 67 #2

By John B. Koss

With the rapid emergence of COVID and the resulting rush to accommodate remote work, many corporations swiftly implemented corporate instant messaging applications such as Slack. Slack is a cloud-based instant messaging application that allows users to communicate on a one-to-one basis or in larger groups in dedicated "channels," which are permissioned chat groups that can be commissioned for corporate teams, departments, or parties outside an organization.

While applications like Slack can facilitate remote collaboration and feel familiar to younger workers used to social media messaging, some of their unique features, including the way in which Slack organizes and catalogues individual and group messages as well as programmatic options for identifying, searching, and preserving communications, create strategic risks when such data is implicated in civil discovery. It is crucial that attorneys are mindful of these unique characteristics and understand the preservation and collection pitfalls associated with applications like Slack before advising clients and attempting to collect data to meet discovery obligations.

The importance of this messaging evidence and the litigation risks of failing to properly preserve, review, and produce it were on full display in a recent decision issued by the United States District Court for the District of Massachusetts in the matter of *Red Wolf Energy Trading, LLC v. BIA Capital Management, LLC*, 19-cv-10119-MLW, 2022 WL 4112081 (D. Mass. Sep. 8, 2022). In this case, the Court entered default judgment against the defendants for repeated discovery lapses and misrepresentations associated with the failure to produce responsive Slack communications.

Facts and Procedural History

This remarkable decision arose from a lawsuit brought in January 2019 by an energy trading firm, Red Wolf, against a former employee trader, his new employer, Bia Capital Management ("Bia"), and five of its employees (collectively, the "defendants"). The suit alleged the defendants schemed to create and develop a competing business by misappropriating Red Wolf's trade secrets and taking its software and other assets. The software at issue allowed Red Wolf traders to test the future profitability of a trade model without entering the trade into the energy market.

Red Wolf alleged that from the summer 2017 until December 2018, the former employee used Red Wolf's software to place mock trades to test trading strategies to facilitate Bia Capital Management's entry into the market as a Red Wolf competitor. *Id.* at *4. In October 2019, Red Wolf served its first set of document requests on the defendants. These requests specifically targeted "[a]ll communication with or between the named defendants or anyone working for, with, or on behalf of Bia via Slack […]." *Id.* at *5.

On two occasions, once in April 2021 and again in September 2021, the defendants filed sworn affidavits attesting to compliance with their Federal Rule of Civil Procedure 26 production obligations, including production of all relevant Slack channel communications. Nevertheless, in response to identified discovery deficiencies, continued concern with missing Slack messages, and a Motion to Compel, the Court in March 2022 ordered the defendants to produce all relevant Slack communications. *Id.* at *10. The Court found the defendants' repeated failure to produce the required communications exasperating and, at the hearing on the Motion to Compel, it stated: "[…] I rarely have a discovery dispute. I've spent more time on discovery disputes in this case than I may have certainly in any case in my 37-year career. […]. [T]his is not a game of hide and seek…. I issue an order and you have to disclose [the required documents]." *Id.* at *11.

Despite having previously attested, twice, to compliance with production obligations, in April 2022, the defendants produced additional Slack messages responsive to the original document requests from 2019. A month later, during a May 2022 deposition, one of the individual defendants testified that Slack messages were omitted from earlier productions due to a "mistake" made by a contractor in Kazakhstan he had hired to write a program the defendants used to search and produce Slack messages. *Id.* The deponent further testified he chose not to hire a messaging application expert because of a "limited budget" that would not allow the

defendants to hire a "top tier firm" to search Slack. *Id.* The deponent also claimed he could not find any outside vendors who could do the work. *Id.*

Following the deposition, Red Wolf filed a motion for sanctions in June 2022, requesting a default judgment based on the defendants' repeated failure to produce relevant Slack communications despite the judge's orders to supplement their production and sworn statements that the relevant Slack messages had been produced. Even after filing of the sanctions motion, the defendants identified and produced additional previously unproduced Slack messages in July and August 2022.

In August 2022, the Court ordered the defendants to provide Red Wolf with a copy of the 2019 Slack Archive (the full content of the specific Slack instance) to be searched by Red Wolf's litigation data vendor. This search and analysis identified at least 128 relevant messages from the defendants' Slack account that should have been produced. *Id.* at *15. Most problematically, one of these messages constituted the "proverbial smoking gun" – a communication dated January 22, 2019 (only a few days after Red Wolf originally filed suit) in which two defendants discussed creating a new algorithm to hide the fact that their original algorithm was derived from Red Wolf technology. *Id*.

In addition, Red Wolf filed an affidavit from their discovery vendor who conducted its own search of the Slack Archive in which the vendor disputed the defendants' claim of the difficulty and non-standard nature of Slack collections. The vendor stated that, even in 2019, the defendants could have used "a standard eDiscovery processing tool" to search and produce Slack messages for $10,000. *Id.* The vendor further noted that the defendants' search of its Slack messages by their independent contractor in 2019 was "outside of universally accepted standards and best practices for legally defensible data collection" and "not technologically sound." *Id.* at 16. Finally, the vendor described an "anomaly" in the defendants' production — 87 empty folders in the 2019 Slack Archive — which supported an inference that deletion of channel data occurred after export from Slack but prior to the transfer to Red Wolf. *Id.*

In ruling on the motion for sanctions, the Court found that the serious sanction of a default judgement – along with attorneys' fees and costs associated with the motion to compel – was appropriate given the prejudice suffered by Red Wolf, which was long deprived of documents evidencing the merit of its claims, as well as the fact that the defendants' violations of multiple discovery orders constituted extreme misconduct. *Id.* at 24.

In rendering a default judgment against Defendants, the Court was clear that its decision should "encourage litigants to understand that it is risky business to recklessly or deliberately fail to produce documents, and perilous to disobey court orders to review and, if necessary, supplement prior productions." *Id.* at 25.

Takeaways and Considerations When Dealing with Instant Messaging Applications Like Slack

As with discovery in any case, it is imperative that counsel develop a deep and comprehensive understating of their client's communication systems. This understanding enables counsel to ensure that all systems are addressed in the context of both applying legal holds when and where appropriate and successfully collecting, analyzing, and reviewing data outputs from those systems when called for in discovery.

With regard to instant messaging systems such as Slack (as well as other similar messaging applications such as Microsoft Teams), it is important to keep in mind that these applications store communications and associated data very differently than traditional email or document storage systems and may offer more limited preservation and search capabilities. And, while it can be inferred from the facts of *Red Wolf* that a certain element of deliberate bad faith affected the defendants' conduct and likely compounded the Court's frustration, it is equally likely that a lack of familiarity with these differences also contributed to the defendants' clear production shortcomings.

For this reason, counsel must have a good understanding of how these applications work and what limitations exist as to preservation and collection. In that spirit, some of the central questions and considerations that a practitioner confronting the discovery of Slack or other messaging application data should bear in mind include:

- What does your client's document retention and permissible use policies say with respect to the preservation and use of the instant messaging applications?
- What is the size and reach of the instant messaging application (i.e., is it used by relevant employees, teams, departments, etc.)?
- Are in-house lawyers members of any particular chat channels or communications that may require consideration of privilege?
- What is the subscription package that your client has for its instant messaging application?
- What are the preservation options for the data contained in the instant messaging application based on the client subscription? Different pricing packages come with different features with e-discovery preservation and search functionality often reserved for higher priced packages.
- Have you identified and collected all of the relevant components of the messaging, both person-to-person and in group channels, including any attachments and non-messaging content?
- What will be your approach to processing the data for further analysis and review, especially the application of search terms?
- Will an e-discovery expert or professional be required to assist with defensible collection using an industry-acceptable application and to help you understand options and risks?

- Have you captured everything that is relevant and how can you document that confirmation?
- To the extent any Slack data appears to be missing and/or is going to be withheld from production, do you have a valid basis for that lack of messaging or its withholding from production?

While there is no way to guarantee that zero spoliation allegations will arise from complex discovery from modern sources, practitioners should do what they can to safeguard against such issues by taking the time and care to truly understand sources of relevant data. This should include taking adequate preservation steps as soon as practicable, ensuring that data is properly staged for searching, and that relevant results are identified in full and produced. The foregoing considerations and a full understanding of each will help ensure your reasonable basis at each of these phases and avoid an outcome like the one in *Red Wolf.*

John B. Koss is the Managing Director of Mintz's E-Data Consulting Group. John's practice focuses on counseling clients on information governance, e-discovery readiness, and the utilization of technology to manage large data matters. He speaks and writes frequently on these issues and teaches e-discovery law at Suffolk University Law School.

Related Links

CASE FOCUS

Commonwealth v. Rossetti: Searching for Clarity and Justice in Massachusetts' Sentencing Statutes

CASE FOCUS