Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Are Your Slack Communications Primed For E-Discovery?

By **Jessica Brown and Collin James Vierra** (July 7, 2020, 4:34 PM EDT)

Jessica Brown

Collin James Vierra

As COVID-19 continues to force many companies to maintain work-from-home policies, even more workplace conversations are occurring digitally, including in novel platforms like Slack, Facebook Messenger, Google Hangouts, Chanty, Ryver and Microsoft Teams. While these and similar platforms may increase companies' productivity as teams struggle to find new ways to communicate efficiently, companies should ensure they are utilizing these platforms in a way that allows for effective discovery in the event they become subject to litigation or investigation.

In this article, we address how companies using channel-based platforms can manage the use of these platforms and the data to be well-positioned in the event these platforms are subject to discovery. We further provide recommendations regarding review and production of channel-based data.

Basic Introduction to Channel-Based Data

Channel-based platforms are designed to replace the overuse of email within an organization. Within the platform, users may create discrete channels for various projects or user groups. For example, channels could be created for all marketing employees of an organization, for all employees located in a particular company office, or for all employees working on a particular project.

A given user may be a member of numerous channels. The platform manager or channel creators may designate which users are permitted to access which channels. Individuals outside an organization also may be invited to join certain channels via guest accounts.

Within a given channel, users may converse and share files. Instead of being stored separately in each user's email archive, these conversations and files will be stored in a single instance, i.e., in the channel in which they occurred. Thus, for a given channel, every user sees identical content. Companies may decide how long they wish to preserve data in certain channels or when certain channels should be deactivated.

Legal Treatment of Channel-Based Data in E-Discovery

To date, courts have had few occasions to address companies' discovery obligations with respect to

channel-based platforms. In the rare occasions when channel-based data has been the subject of a motion to compel, courts have split as to whether companies should be compelled to produce such data.

For example, in Milbeck v. TrueCar Inc., the U.S. District Court for the Central District of California refused to compel production of Slack data, accepting the defendants' argument that review and production of Slack data would be unduly burdensome, even though the plaintiff provided evidence that information "at the heart of this case" had been exchanged via Slack.[1]

But in Calendar Research LLC v. StubHub Inc., after defendants voluntarily made an initial production of Slack messages, the same court compelled the defendants to supplement their production once the Slack account was upgraded, making additional messages available for production.[2] Importantly, the defendants did not raise burden arguments.[3]

And in West Publishing Corp. v. LegalEase Solutions LLC, the U.S. District Court for the District of Minnesota compelled production of Slack data, but required the party seeking discovery to share the processing and production costs.[4]

As more advanced e-discovery tools and techniques become available for management of channel-based data, and as use of channel-based platforms becomes more widespread within organizations, it is doubtful that companies will be able to withhold such data from discovery in all circumstances.

Thus, companies should assume that they may be compelled to review and produce channel-based data if they become subject to litigation or investigation. And, accordingly, they should take proactive steps to ensure that such data is preserved and can be collected, reviewed and produced in a manner that satisfies their legal obligations, while avoiding overproducing irrelevant or sensitive information.

Management of Channel-Based Data

Even before litigation or an investigation begins, companies can organize their channel-based data to minimize the risks of overpreservation, overdisclosure and privilege waiver. We recommend that companies take the following steps:

First, companies should carefully limit channels only to necessary participants. If a user becomes a custodian in litigation or an investigation, a company may be obligated to preserve and review data from all channels in which that user participated.

Second, companies should take special care to limit third-party access to company channels. If third-party guest users have access to channels in which privileged conversations have occurred, such privilege may be waived.[5]

Third, channels should be descriptively titled, and conversations within channels should be limited to the relevant topic.

We know from how employees use email that limiting discussions by topic will be easier said than done. But doing so not only will make reviewing and investigating such channels easier, it may allow companies to negotiate with opposing counsel or regulators to review only channels with facially relevant titles. Relatedly, companies should liberally create channels for new groups and projects so that there is less temptation for users to converse about multiple topics within a single channel.

Fourth, companies should create designated channels for privileged conversations, and/or clearly designate via keywords or other markers when privileged conversations are occurring in otherwise nonprivileged channels.

Although all channels subject to review and production should be reviewed for privilege during discovery, companies may have an easier time excluding certain channels from review and production if they are facially reserved for privileged conversations. Companies should include descriptors like "ACP" (for attorney-client privilege) or "Legal" in the titles of any privileged channels.

Fifth, companies should put these protocols in writing and ensure that users familiarize themselves with the protocols. Periodic brief training sessions to reinforce the protocols are advisable as well. These efforts will not only increase user compliance, they may support companies' assertions during discovery negotiations that only facially responsive, nonprivileged channels should be collected and reviewed.

Sixth, companies should audit channels, both for the substance of conversations and for user access.

Users should be removed from channels in which their participation is unnecessary, and new channels should be created for conversation topics that appear not to belong in the channel in which they are taking place. Companies should take particular care to search for privileged conversations occurring in nonprivileged channels and for the presence of third-party guest users.

Review and Production of Channel-Based Data

Notwithstanding these recommendations, channel-based platforms pose unique review and production considerations. In particular, channels are likely to persist longer and cover a greater number of topics than a single email thread.

For example, a company preparing to launch a new product might exchange thousands of emails about that product, with multiple different email threads relating to manufacturing, marketing, distribution and the like. By contrast, in a channel-based platform, all of these communications might occur within a single product-focused channel.

Thus, it would be inappropriate to analogize a channel to a single email thread; rather, a channel is more like an email folder that contains all email threads about a given topic. Consequently, in litigation or investigations, channels are more likely than email threads to contain a mixture of responsive and nonresponsive material.

In light of this reality, we recommend that companies split extended channels into smaller "snippets" of conversation. For example, a snippet might include all messages in a given channel over a 24-hour period.

Snippets may then be loaded into a review database as stand-alone documents and reviewed on that basis. Companies may load these snippets into review batches sequentially so that reviewers can recreate the underlying channel, but select only those snippets from the channel that contain content responsive to the litigation or investigation.

Companies may also consider redacting the nonresponsive portions of otherwise responsive snippets. Courts have not yet addressed the extent of companies' obligations to produce nonresponsive content

in otherwise responsive channels. Those propounding discovery requests will insist that channels should be treated more like emails for discovery purposes. Courts are generally skeptical of companies' ability to redact nonresponsive material in otherwise responsive email threads.[6]

Arguably, however, channels should be treated for discovery purposes like text messages, which, like conversations in channels, are more likely than an email thread to persist for an extended period and touch upon multiple topics. Case law regarding text messages indicates that parties may have the ability to excerpt and produce only responsive information from extended text message conversations.[7]

But overly aggressive responsiveness redactions are likely to be faced with suspicion by courts. Nonresponsive content that provides necessary context to responsive content may need to be produced, for example.[8] Nevertheless, where conversations diverge into topics that do not relate to the responsive content, companies should consider redacting such material.

We further recommend that companies keep track of whether attorneys had access to given channels at various points in time. For example, a request from a nonattorney that appears nonprivileged on its face may actually be privileged if the nonattorney believed an attorney would be reviewing the request. Snippets containing requests for legal advice or incorporating legal advice also should be redacted or withheld.

Lastly, recall that following the foregoing recommendations regarding management of channel-based data will reduce the number of situations in which companies risk being compelled to produce nonresponsive or privileged material contained within otherwise responsive channels.

Conclusion

Channel-based platforms are becoming increasingly popular among major companies, especially in a work-from-home era. To date, companies generally have not been compelled to produce such data for a variety of reasons, including because the burdens of review and production have outweighed the anticipated value of the data. However, companies may be compelled to produce such data in the future, and therefore they should plan accordingly.

For channel-based platforms, this means companies should develop protocols and enforcement mechanisms to limit user participation to necessary channels only, regulate guest access to company channels, make liberal use of descriptively titled channels for new projects or user groups, and segregate privileged conversations as much as possible.

In addition, if compelled to review and produce channel-based data, companies should consider splitting channels into time-limited snippets and redacting nonresponsive as well as privileged material within otherwise responsive snippets. They also should keep track of attorney involvement in various channels.

Because courts have had limited opportunities to discuss discovery obligations with respect to channel-based data, companies also should stay abreast of legal developments in this area.

Jessica Brown is a partner and Collin James Vierra is an associate at Gibson Dunn & Crutcher LLP.

information purposes and is not intended to be and should not be taken as legal advice.

[1] Milbeck v. TrueCar Inc. , 2019 WL 4570017, at *1-3 (C.D. Cal. May 2, 2019).

[2] Calendar Res. LLC v. StubHub Inc., 2019 WL 1581406, at *3-4 (C.D. Cal. Mar. 14, 2019).

[3] Id.

[4] West Pub. Corp. v. LegalEase Sols. LLC , 2019 WL 8014512, at *8 (D. Minn. No. 22, 2019).

[5] See In re: Asia Glob. Crossing, 322 B.R. 247, 257-58 (Bankr. S.D.N.Y. 2005) (setting forth factors as to whether a reasonable expectation of confidentiality in attorney-client communications exists such that the attorney-client privilege is preserved, including whether "third parties have a right of access" to the communications, and collecting cases); id. at 258 ("[T]he question of privilege comes down to whether the intent to communicate in confidence was objectively reasonable.").

[6] See, e.g., Milchior v. Hilite Int'l Inc., 2013 WL 2238754, at *3 (E.D. Mich. May 21, 2013) ("Having produced portions of emails ... [subpoenaed party] must produce the emails without redactions."); U.S. ex rel. Simms v. Austin Radiological Ass'n, 292 F.R.D. 378, 387 (W.D. Tex. 2013) (refusing to permit "selectively applied unilateral redactions" of nonresponsive information in otherwise responsive emails); Anthopologie Inc. v. Forever 21 Inc., 2009 WL 690126, at *5 (S.D.N.Y. Mar. 13, 2009) ("string of e-mail exchanges" in which "redacted portions were not relevant to the case" were compelled to be produced "in unredacted form").

[7] See, e.g., Tingle v. Hebert, 2017 WL 2536584, at *5 (M.D. La. June 8, 2017) (limiting requests for production of all of plaintiff's text messages to only those messages exchanged with designated persons during a discrete time period about a given topic).

[8] See Bartholomew v. Avalon Capital Grp. Inc., 278 F.R.D. 441, 451 ("[I]rrelevant information within a document that contains relevant information may be highly useful to providing context for the relevant information.").