COVID-19: MITIGATING REMOTE WORKING RISKS - MESSAGING AND CHAT APPS

Date: 4 June 2020

U.S. E-Discovery and Investigations, Enforcement and White Collar Alert

By: William D. Semins, Hugh T. McKeegan, Daniel R. Miller

KEY HIGHLIGHTS:

- In response to COVID-19, many businesses expanded remote work practices and use of technology—including video conferencing, enterprise collaboration tools, and ephemeral messaging—in order to maintain operations.
- Coupled with “bring your own device” culture, these tools (in particular, ephemeral messaging) can make data and records retention more difficult and could expose a company to risks including:
  - Sanctions for spoliation of evidence in litigation; and
  - According to Department of Justice's (DOJ) policy, loss of cooperation or remediation credit in an investigation.
- To mitigate such risks, companies that choose to employ these tools should develop policies and procedures governing use to ensure important records and data are preserved. Key components of such a policy include:
  - A thorough understanding of the technology and its functionalities;
  - A thoughtful, advanced business justification statement for the use of ephemeral messaging or other technology with short retention periods;
  - Clear guidelines defining authorized users and permissible subject matter;
  - Specified prohibitions on use where retention is required by law;
  - Suspension of use of ephemeral messaging by employees affected by a litigation hold notice and periodic spot-checks to ensure compliance; and
  - Required training for employees who use the technology.

1. WORKING FROM HOME

With the onset of the COVID-19 pandemic, many companies dramatically expanded remote work practices in response to “stay at home” orders. This rapid shift in operations accelerated adoption of new software solutions, including video conference tools (such as Zoom, Cisco Webex, and Google Meet), enterprise collaboration tools (such as Microsoft Teams, Slack, and Workplace from Facebook), and ephemeral messaging applications (such

as Snapchat, WhatsApp, Telegram, and Signal).[1] Further, lessons learned during the pandemic about a company's ability to continue operations remotely will likely lead many businesses to reevaluate their past practices, needs, and costs (such as physical office space), with some implementing expanded remote work practices even after the current crisis passes. This transition to expanded remote working, paired with the ubiquity of "bring your own device" work culture, in addition to added security risks,[2] may also lead to increased liability or scrutiny, especially as this technology (including ephemeral messaging applications) may be used to facilitate unlawful or inappropriate conduct (such as receiving and trading on insider tips,[3] rate-rigging,[4] employment discrimination,[5] or spoliation of evidence[6]) and the means to cover it up.[7] Indeed, while developers tout ephemeral messages as the functional equivalent of off-the-record phone calls, courts and law enforcement often do not share this view. Instead, they often adopt the position that, like e-mail, ephemeral messages are business records that, depending on content, should be subject to retention and preservation requirements.[8] Thus, it is now more important than ever for companies to implement data retention policies that address ephemeral messaging platforms, their functionalities, their approved uses, and their attendant risks.

2. THE RISKS OF EPHEMERAL MESSAGING APPLICATIONS

Ephemeral messaging applications have a number of legitimate features, among them the promise of enhanced data protection (e.g. encryption) by keeping sensitive communications out of the hands of competitors or hackers. In addition, when used appropriately, ephemeral messaging can offer cost savings. By automatically disposing of messages that contain personal information and which are no longer needed for business or legal purposes, these tools can assist in achieving compliance with data privacy laws (such as the European Union's General Data Protection Regulation, which favors data-minimization with regard to unnecessary personal data). Likewise, eliminating such data can reduce the risks and potential costs associated with data breaches. That said, in choosing to adopt or allow the use of ephemeral messaging applications, a company should also consider certain risk points, such as the ability to conceal misconduct and, less obviously, the potential for litigation sanctions or loss of cooperation or remediation credit stemming from a failure to retain necessary data appropriately.

In the context of litigation, ephemeral messaging can complicate a company's ability to comply with discovery requests, especially if such messaging applications continue to be used to discuss relevant topics after a litigation hold is issued and the company fails to take steps to limit (or even promotes) such use. In that situation, discovery sanctions could be imposed under a theory that the company was willfully blind to,[9] or actively engaged in,[10] the destruction of records and evidence by allowing messages to be deleted wholesale in near real time. Indeed, although severe sanctions require finding an intent to deprive another party of the information in the litigation, courts have indicated a willingness to infer such intent based on a party's use of specific messaging tools and retention practices.[11]

Use of ephemeral messaging could also create similar issues in the context of investigations of corporate misconduct, including situations where a company is seeking to obtain cooperation or remediation credit by self-disclosing and fully responding to and remediating allegations of misconduct, but where key data has been lost. Indeed, the 2019 update to the DOJ's Foreign Corrupt Practices Act Corporate Enforcement Policy (FCPA Policy) requires "[d]isclosure on a timely basis of all facts relevant to the wrongdoing at issue" and "[t]imely preservation, collection, and disclosure of relevant documents and information relating to their provenance" to obtain full cooperation credit.[12] Likewise, the 2019 FCPA Policy ties a company's ability to receive full remediation credit in part to the adequacy of its policies and procedures related to the use of ephemeral messaging applications.[13]

Specifically, the FCPA Policy requires that companies "prohibit[] the improper destruction or deletion of business records, including implementing appropriate guidance and controls on the use of…ephemeral messaging platforms."[14] Although the 2019 policy seems to have softened DOJ's prior stance on ephemeral messaging,[15] prosecutors and regulators appear to expect companies to implement policies and controls to manage use of ephemeral messaging applications.[16] Indeed, DOJ's June 2, 2020 update to its Evaluation of Corporate Compliance Programs places an emphasis on data analytics and whether "compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions."[17] DOJ's assessment of the adequacy and effectiveness of compliance programs going forward will also assess whether "any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments."[18]

Recent comments from senior federal law enforcement officials at a virtual town hall hosted by the American Conference Institute further support this view. Robert Zink, Chief of the DOJ's Fraud Section, commented that DOJ expects companies to undertake some diligence to capture and retain ephemeral communications. Likewise, Daniel Kahn, Senior Deputy Chief of DOJ's Fraud Section, indicated that the COVID-19 crisis is no excuse to not comply with requests for documents and information. If a company cannot comply with such requests, authorities will need to understand the reasoning behind the company's policies and practices that make compliance impossible, including good-faith efforts to overcome obstacles to data preservation and collection.

Thus, the risk of sanctions or potential loss of cooperation or remediation credit underscores the need for a company to have clear policies and procedures for dealing with the use of ephemeral messaging applications and enterprise collaboration tools that incorporate chat functions that approximate ephemeral messaging. In light of the DOJ's June 2, 2020 update to its Evaluation of Corporate Compliance Programs,[19] such policies should, for instance, proscribe certain uses, set commercially reasonable and manageable limits on retention of messages, and provide for periodic testing to ensure that proscribed uses are not occurring. If a company adopts a short retention period for certain platforms (to the extent possible to control) or adopts an ephemeral messaging tool, a thoughtful, advance business justification statement is advisable because it would (1) show how the company weighed the risks when setting its policy and (2) serve as a record that could later be used to explain why the company took this approach.

3. DESIGNING AN EFFECTIVE DATA RETENTION POLICY FOR EPHEMERAL MESSAGING APPLICATIONS

Records management and information governance best practices provide, and court opinion and government agency guidance strongly suggest, that companies should develop policies to manage their data and records in compliance with relevant legally-mandated retention requirements, which are usually based on a record's content, rather than its format. In that regard, ephemeral messages are no different and companies should evaluate the appropriateness of ephemeral messaging in light of these broader records management considerations. Ultimately, where the use of ephemeral messaging is found to be appropriate, the use of such applications—and the mitigation of associated risks—are internal controls issues that should be carefully addressed by legal counsel and compliance departments before any litigation or investigation occurs. An effective data retention policy can help protect a company from liability arising out of litigation or an investigation by retaining and preserving necessary data and providing for the defensible disposal of unnecessary and extraneous data.

First, a retention policy that addresses effectively ephemeral messaging should be based on a comprehensive understanding of the applications at issue and functionalities. Key points central to this understanding include how and where data is stored, the length of time for which the data is stored, and whether any aspects of the data can be retrieved or reconstructed following deletion. Another vital point to understand is the process by which any data maintained by the tool could be preserved, collected, searched, de-duplicated, reviewed, and produced in the event of a relevant litigation or investigation.

Next, an effective data retention policy for ephemeral messaging applications should consider and address certain key points, such as: (1) data that cannot be transmitted and subject matter that cannot be discussed while using the application, (2) situations in which use of the application must be suspended, (3) the individuals granted rights to use the application, and (4) training to be completed before such use can begin.

As part of their broader records management and information governance policies, companies should identify applicable laws mandating storage of certain types of information for a defined length of time and then explicitly specify that ephemeral messaging applications must not be used for such information.[20] Additionally, companies can potentially avoid losing credit with law enforcement if their records management policies incorporate appropriate, risk-based guidance and controls on the use of ephemeral messaging applications.

Companies must also take care to suspend uses of ephemeral messaging in any context where the communications could serve as evidence that must be preserved. In the context of ephemeral messaging applications, a standard litigation hold notice on its own may not be sufficient, and companies should consider requiring employees affected by the hold to cease using the application altogether, followed by periodic spot-checking and documentation to ensure compliance.

Companies should define with specificity who is permitted—and how they are permitted—to use ephemeral messaging applications, with such determinations based on a risk assessment that considers factors such as job function and need, access to proprietary information and trade secrets, or relevant position or title. Also, it may be appropriate to restrict use of the application to internal communications only among select personnel within the company, rather than permitting ephemeral messaging with individuals outside of the company, due to heightened risks related to corruption, insider trading, price-fixing, or other conspiratorial or cartel offenses.

Finally, training on the relevant data retention policy and ephemeral messaging software is essential. Employees using the software should understand when it is appropriate to use an ephemeral messaging application in light of routine record retention concerns and litigation holds. Information technology staff should also understand the application, who is allowed to install and use the application, how monitoring (if any) may be conducted, and how to suspend the application for litigation holds. Such staff must also stay informed about software updates and changes that can affect how these tools operate, how they maintain data, and how their functionalities and controls work.

4. CONCLUSION

As with the introduction and widespread adoption of new technologies in the past (e.g., e-mail), the growing use of ephemeral messaging tools presents new benefits and risks to business. The use of applications capable of ephemeral messaging is likely to grow in the wake of the COVID-19 pandemic as in-person work practices evolve further toward broader reliance on new digital modes of interaction. Companies should carefully consider how

best to implement and regulate the use of tools like ephemeral messaging—through adequate, risk-based policies and procedures, training, and monitoring—to avoid exposing themselves to undue risk.

FOOTNOTES

[1] *See* Amanda R. Cashman et al., *COVID-19: There's No Place Like Home: What GCs Need You to Remember While Working Remotely,* Mar. 25, 2020.

[2] *See* Tara C. Clancy and Joseph D. McClendon, *COVID-19: System Security With a Remote Workforce*, Mar. 26, 2020.

[3] *See, e.g.,* Jennifer Van Grove, *CNBC's Jim Cramer implies Snapchat is used for insider trading*, CNET, July 13, 2013.

[4] *See* U.S. DEP'T OF JUSTICE, FIVE MAJOR BANKS AGREE TO PARENT-LEVEL GUILTY PLEAS (May 20, 2015). Five banks agreed to pay more than $2.5 billion in criminal fines for manipulating the London Interbank Offered Rate. According to the plea agreement, traders at these banks "used an exclusive electronic chat room and coded language to manipulate benchmark exchange rates." *See also* Ben Protess et al., U.S. Investigates Currency Trades by Major Banks, N.Y. TIMES, Nov. 14, 2013.

[5] *Zubulake v. UBS Warburg, LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004); *Pension Committee of the Univ. of Montreal Pension Plan, et al., v. Banc of America Securities, LLC, et al*., 685 F. Supp. 2d 456 (S.D.N.Y. 2010).

[6] *See, e.g., WeRide v. Kun Huang,* No. 5:18-cv-07233-EJD, 2020 WL 1967209 (N.D. Cal., April 24, 2020) (imposing "terminating sanctions," in part, for employee use of ephemeral messaging *after* litigation began); *Herzig v. Arkansas Foundation for Medical Care, Inc.,* No. 2:18-CV-02101, 2019 WL 2870106 (W.D. Ark., July 3, 2019) (finding plaintiffs' use of ephemeral messaging after litigation began to be "intentional, bad-faith spoliation of evidence" and granting defendant's motion for summary judgment)

[7] To be sure, while cases like *Zubalake* and *Pension Committee.* (involving deleted e-mails and other electronic documents) long predate the broad adoption of ephemeral messaging tools, these cases indicate how ephemeral messaging could be misused to effect spoliation of evidence, which could lead to litigation sanctions and other penalties for failing to adequately preserve communications.

[8] *See, e.g.,* Nate Lankford and Dawn E. Murphy-Johnson, *DOJ refines stance on ephemeral messaging apps*, FCPA BLOG (March 18, 2019, 12:18 p.m.).

[9] *See Brookshire Bros., Ltd. v. Aldridge*, 483 S.W.3d 9, 24 (Tex. 2014) (defining "intentional spoliation" to "include[] the concept of 'willful blindness,' which encompasses the scenario in which a party does not directly destroy evidence…but nonetheless 'allows for its destruction.'").

[10] See WeRide, 2020 WL 1967209 ("terminating sanctions" for apparent willful destruction of evidence, including ongoing use of 90-day automatic e-mail deletion and ephemeral messaging after litigation commenced).

[11] *See, e.g., WeRide*, 2020 WL 1967209; Herzig, 2019 WL 2870106. *See also Alabama Aircraft Industries, Inc*., 319 F.R.D. 730, 746–47 (N.D. Al. 2017) (granting adverse inference where "unexplained, blatantly irresponsible behavior" led to loss of ESI); *Decker v. Target Corp*., No. 1:16-cv-00171-JNP=BCW, 2018 WL 4921534 (D. Utah Oct. 10, 2018) (granting adverse inference where store employees failed to preserve relevant video-surveillance

footage).

[12] *See* FCPA Corporate Enforcement Policy, U.S. DEP'T OF JUSTICE. *See also*, Brian F. Saulnier et al., DOJ Revises Corporate Compliance Guidance Calling Attention to Three Areas Where Most Companies Fall Short: Risk Assessments, Compliance Culture, and Continuous Compliance Program Improvement, May 16, 2019.

[13] *Id*.

[14] *Id*.

[15] The 2017 update to the policy declared that corporations would not receive a "presumption of declination" for government cooperation unless the corporation prohibits "employees from using software that generates but does not appropriately retain business records or communications."

[16] Highlighting the need for attention to when use of ephemeral messaging applications are compliant with legal requirement, the Securities and Exchange Commission has taken the position that there can be no valid business case for the use of ephemeral messaging applications under certain circumstances, such as where, under the Investment Advisors Act of 1940, registered broker-dealers and investment advisors are required to retain certain business communications. *See, e.g.*, Observations from Investment Adviser Examinations Relating to Electronic Messaging, U.S. SECURITIES AND EXCHANGE COMMISSION (SEC).

[17] Evaluation of Corporate Compliance Programs *(Updated June 2020),* U.S. DEP'T OF JUSTICE.

[18] *Id*.

[19] *See id.* Although not addressing ephemeral messaging or chat apps directly, DOJ's evaluation of a corporate compliance program emphasizes taking a dynamic, risk-based approach to the compliance function. Accordingly, companies should seek to apply these principles to their policies and procedures relating to ephemeral messaging and chat apps.

[20] For example, Rule 17a-4 of the Securities and Exchange Act specifies that communications relating to a broker-dealer's business must be retained for three years. *See* SEC Interpretation: Electronic Storage of Broker-Dealer Records, SEC, (May 7, 2003).

KEY CONTACTS

WILLIAM D. SEMINS
PARTNER

PITTSBURGH
+1.412.355.8973
WILLIAM.SEMINS@KLGATES.COM

