ALSTON & BIRD

WWW.ALSTON.COM

White Collar, Government & Internal Investigations ADVISORY ■

MARCH 26, 2019

DOJ's Revised Ephemeral Messaging Policy Amounts to a Distinction Without a Practical Difference

A company's use of so-called ephemeral messaging platforms—where messages disappear after viewing or can be erased within a time window—sits at the intersection of its compliance interests and its employees' privacy rights. Popular applications such as Snapchat, Telegram, Signal, and Wire grant individuals and teams the ability to communicate confidential or proprietary information in environments where verbal communications might be unwieldy or indiscreet. But ephemeral messages present obvious problems for corporate compliance and self-reporting. A company cannot record and report what it cannot capture. Corporate oversight of employee use of these applications, whether the use occurs over a company network or on mobile devices paid for by an employer, can both be impractical and infringe on individual privacy rights, particularly abroad. Recognition of the ubiquity of ephemeral messaging—and the inherent difficulty in regulating and monitoring its use—has led the U.S. Department of Justice (DOJ) to alter its complete prohibition of ephemeral messaging applications in order to receive full credit under its FCPA Corporate Enforcement Policy.

The initial version of the policy, adopted in 2017, established a presumption in favor of declination of criminal enforcement for companies that (1) voluntarily self-disclose potential violations; (2) fully cooperate with the government's investigation; and (3) timely remedy the identified problems. To qualify for remediation credit, the policy provided that, among other things, a company must implement procedures ensuring "[a]ppropriate retention of business records, including *prohibiting* employees from using software that generates but does not appropriately retain business records or communications." Under the plain language of the policy, companies had little choice: either prohibit use of these popular messaging platforms or lose the benefit of the policy.

As revised, the policy nominally relaxes the DOJ's stance on ephemeral messages—but offers no concrete guidance on instances when use of ephemeral messages would be consistent with a fulsome self-reporting. The March 9, 2019 revision provides that a company may receive full credit for timely remediation if it adopts procedures ensuring "[a]ppropriate retention of business records, and prohibiting the improper

destruction or deletion of business records, *including 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 or otherwise comply with the company's document retention policies or legal obligations*."

So the question is whether this largely semantic change—i.e., an outright prohibition versus the implementation of guidance and controls—should affect a company's compliance plans for document retention and use of ephemeral messages for business purposes. The answer: probably not. The touchstone of the policy remains complete and well-documented self-disclosure. Under the new ephemeral messaging guidance, employee use of ephemeral messaging for business purposes is not an absolute bar to declination. But the spirit of the policy remains that not only should companies counsel their employees to avoid use of ephemeral messaging in the business context, but also that business discussions should fundamentally occur via traditional platforms that archive communications for compliance purposes in accessible and searchable formats.

In sum, while the DOJ's stance on ephemeral messaging has relaxed in recognition of prevailing practicality and privacy concerns (especially internationally), this hardly means that the prevalence of ephemeral messaging platforms to facilitate business communications—particularly following a self-disclosure in which corruption was furthered through the use of such platforms—will go unnoticed or unchecked. Companies are well advised to adopt policies stressing the importance of using permanent messaging platforms for business purposes, specifically including through privacy waivers (where available and enforceable) and through the use of networked applications that store business communications and facilitate their ready retrieval.

You can subscribe to future *White Collar, Government & Internal Investigations* advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information please contact your Alston & Bird attorney or any of the following:

White Collar, Government & Internal Investigations

Edward T. Kang
202.239.3728
edward.kang@alston.com

Meredith Jones Kingsley
404.881.4793
meredith.kingsley@alston.com

William (Mitch) R. Mitchelson
404.881.7661
mitch.mitchelson@alston.com

Jenny Kramer
212.210.9420
jenny.kramer@alston.com

Mark T. Calloway
704.444.1089
mark.calloway@alston.com

Paul N. Monnin
404.881.7394
paul.monnin@alston.com

Brian D. Frey
202.239.3067
brian.frey@alston.com

Jason D. Popp
404.881.4753
jason.popp@alston.com

Michael R. Hoernlein
704.444.1041
michael.hoernlein@alston.com

T.C. Spencer Pryor
404.881.7978
spence.pryor@alston.com

William H. Jordan
404.881.7850
202.756.3494
bill.jordan@alston.com

Thomas G. Walker
704.444.1248
919.862.2212
thomas.walker@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Ave. ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, California, USA, 94303-2282 ■ 650-838-2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333