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

White Collar 'Goes Dark' With Rise Of Secret Messaging Apps

By **Stewart Bishop**

Law360, New York (September 20, 2017, 7:32 PM EDT) -- White collar suspects' use of email and other electronic communications about their illicit activity has been a boon to prosecutors for decades, but the rise of encrypted messaging apps and other new technology may be a roadblock to Wall Street prosecutors accustomed to a run of successes.

Secret messaging apps like Signal, Telegram, WhatsApp and others not only offer end-to-end encryption, but some even allow for self-destructing messages, a far cry from the pages and pages of emails, chat room records and other electronic communications relied on by prosecutors in everything from insider trading to Libor-rigging cases.

Long a concern of the U.S. government because of their usefulness to terrorist groups like the so-called Islamic State group, the ubiquity of such apps has led to their increased use in the world of white collar crime, experts say. Just last month, a former senior accountant at Celator Pharmaceutical Inc. who copped to insider trading admitted to tipping off his friends via Signal about Celator's forthcoming clinical trial results and its acquisition by Jazz Pharmaceuticals PLC.

Also in August, Manhattan federal prosecutors found that former Bank of America technology consultant Daniel Rivas tried to hide tips he was passing on about mergers and tender offers in part through the use of an unnamed smartphone app to send encrypted messages that would self-destruct. And the U.K.'s Financial Conduct Authority in March slapped a former Jefferies Group Inc. banker with a fine of almost £40,000 ($50,000) after he shared confidential client information over WhatsApp.

Robert Silvers, a former assistant secretary for cyber policy at the U.S. Department of Homeland Security under President Barack Obama and now a partner in Paul Hastings' white collar and cybersecurity and privacy practices, said the problem of "going dark" was a big concern during his time in government, but it usually came up in the context of counterterrorism work.

"I think we're going to look back at the last couple of decades as a golden era for prosecutors when it comes to the availability of evidence because of the rise of email meant that more interchange was recorded than ever before and also more spontaneous interchange, which can be a treasure trove when it comes to making a case, because it shows people's true intentions," Silvers said.

As that kind of spontaneous dialog has migrated from email to messaging apps, you're seeing the availability of that kind of evidence decrease, according to Silvers. While in some instances, you have

people having discussions on such apps just by happenstance, and they happen to be encrypted, in other cases you're going to have individuals who resort to them because of the security features and because they want to conceal the nature of their communications.

"Either way, the evidence won't be there, so I think this is going to become a routine issue that investigators and prosecutors are going to have to deal with," Silvers said.

With traditional emailed communications gradually becoming less and less of a reliable source for white collar prosecutions, the government is likely to rely on sources of evidence and investigative methods, including dusting off some old tricks, according to Marcus Christian, a partner in Mayer Brown LLP's Washington, D.C., office and a white collar and cybersecurity specialist.

"I think what happens is you put more techniques on the table. We've even seen over the last several years [that] wiretaps have been used more commonly in white collar cases. I think historically, people don't think of wiretaps being used like that," said Christian, a former federal prosecutor. "For many people who early on in their careers did economic crime specialties, they never did wire investigations, and I think that is changing."

As some forms of evidence like email become more scarce, investigators are turning to other technological solutions such as data analytical tools.

In the Bank of America case, for example, while some of the men charged had used coded conversations and sent messages on an encrypted, self-destructing smartphone app, their unusual trading was still detected by the Securities and Exchange Commission Market Abuse Unit's Analysis and Detection Center.

Other sources of evidence that prosecutors may turn to include location tracking data from smartphones and other internet connected devices or the so-called internet of things. While it may be that certain conversation streams are being taken off archive emails, there's been a concomitant growth in internet connected devices with listening devices and microphone features which are routinely placed in people's homes and workplaces, which could lead to evidence in criminal proceedings, according to Silver.

"I think you're going to see a reduction in certain types of evidence, but you're going to see an explosion of new digital fingerprints that will help … prosecutors in other kinds of cases make different kinds of cases," Silver said.

Reliance on new forms of technology as well as old school methods of evidence gathering like wiretaps and surveillance methods can create many data points for prosecutors, according to Silver, which may give more support to a prosecutor for coming to the conclusion that a particular series of facts would indicate a crime has been committed, but doesn't come cheap.

"This can make the prosecution much more costly, in terms of money as well as human capital, given that the total resources available to the Department of Justice and other agencies are limited. It seems to almost necessitate that there is going to be a smaller number of cases that you can [investigate] unless you are some able to increase the number of people working on them or their productivity," Silver said.

Jonathan "Jed" Davis, a former federal prosecutor who is now a cybersecurity and white collar partner

at Day Pitney LLP, noted that the government is not without options when it comes to the challenges posed by encrypted apps. An app may be secure, but the device may not be, he said.

While it's no small feat, if law enforcement has a means to take control of a phone and exercise arbitrary control over it, then they can read what's transmitting over the phone because they have control over the keys that people are using to make those messages. And there are various levels of gray, black and overt markets for technology that people use to crack supposedly secure apps, Davis said.

The rise of encrypted messaging apps also raises the question to what extent, if any, the app developers would have to cooperate with law enforcement or provide them with access to the technology in the face of a court order.

"Some of this points to the fact that our statutes are very old, and there has not been a resolution on the part of Congress or any other sort of legislative authority to decide what you do with these new challenges — that's the open question," Davis said.

--Editing by Pamela WIlkinson and Kelly Duncan.
