Applications like WhatsApp are reshaping government investigations and should be refocusing how compliance departments handle employee oversight

WHITE COLLAR, REGULATORY DEFENSE, AND INVESTIGATIONS CLIENT UPDATE
Law360
04.2015

In today's high tech world, the ways to communicate are almost limitless. This presents risks for organizations and challenges for compliance professionals charged with monitoring employee communications and with retaining and searching all of this data to meet regulatory requirements.

The latest example of these risks and challenges is occurring with Capital World Markets "CWM" FX in London, where the London police are focusing on the employees' WhatsApp accounts as part of a fraud and money laundering investigation.[i] According to The Times of London, the founder of CWM, its head of global market analysis and risk, and other staff used WhatsApp to discuss CWM business. This development, reported Monday by The Times, is the latest in this highly publicized investigation. News of problems at CWM began to spread on March 25th when London police working with the U.K. Financial Conduct Authority, arrested 13 employees of the London based FX trading company on suspicion of fraud, conspiracy and money laundering.[ii]

Companies spend millions of dollars designing programs to preserve communications and keep pace with ever increasing regulatory requirements, and they invest countless hours creating platforms with the latest technology that allows employees to communicate with customers through secure channels. But all of this time and money is wasted when the communications that are the most problematic in an investigation are sent using on an app downloaded for free to an employees' cell phone.

WhatsApp?

WhatsApp is one of a growing number of third party instant messaging programs that allow individuals to send and receive messages over a cell phone's internet connection without incurring per message fees charged by wireless carriers. These messages are stored for a limited amount of time on the user's device and may not be available from WhatsApp once deleted. Similar messaging apps like Snapchat and Ansa are allow users to send messages that are automatically deleted within seconds of being received. Ansa also claims to use military grade encryption to make sure nobody but the users can access the messages exchanged

APPLICATIONS LIKE WHATSAPP ARE RESHAPING GOVERNMENT INVESTIGATIONS AND SHOULD BE REFOCUSING HOW COMPLIANCE DEPARTMENTS HANDLE EMPLOYEE OVERSIGHT

The appeal of these types of applications is obvious, and they are extremely popular around the world, even if they have not taken off as much in the U.S. It is estimated that only 10% of mobile phone users in the U.S. are WhatsApp users. Internationally, it is a completely different story with usage rates estimated to be as high at 72% in Singapore, 71% in Hong Kong, 70% in Spain, and 69% in India.[iii]

This popularity led Facebook to purchase WhatsApp in February 2014 for $22 billion.[iv] Facebook paid such a high price because WhatsApp is the most popular instant messaging service in the world. It claims to have more than 700 million active users that send more than 30 billion messages daily.[v]

Why is it being used?

The appeal of an essentially free messaging platform is obvious for personal use; the appeal to business users may be less obvious, but it is still very real if for no other reason than its widespread adoption means convenient communication for business users. With such high usage rates in Asia and Europe, WhatsApp allows employees in the U.S. easy access to customers in Asia and Europe when those customers are out of the office. These out-of-office communications are essential because of the time differences in the regions. Applications like WhatsApp may be preferred because they allow clients in Asia and Europe to receive information on their personal devices quickly without forcing these clients to log in to their relatively cumbersome work platforms.

Why is this a problem?

Government entities around the world impose obligations on regulated companies to preserve communications. Companies that are not aware their employees are using these messaging apps or do not have a program to address their use are not in a position to preserve the communications.

Regulators also expect that companies are monitoring what their employees are doing to ensure the employees are not violating company policy or the law. Communication through WhatsApp is likely done without the employer's knowledge; and therefore, the employer has no opportunity to monitor these communications.

What can be done?

The first line of defense against this or any employee conduct that threatens the company is a clearly worded policy prohibiting the unwanted practices. In this case, your company's policy should prohibit the use of any non-approved communication platforms for business use. Employees should also be trained on the policy to make sure they understand the reason for the policy, what the policy prohibits, and the consequences for failing to comply with them.

Another line of defense can be the firm's firewall. Preventing the employee from downloading these applications or accessing websites that allow for similar types of communications is one way to prevent employees from using them on work computers and other devices. It may also allow for a conversation with employees about why they want the app and what company approved program can provide similar functionality.

Compliance can also look for policy violators by adding certain keywords to your company's monitoring program to identify users of the apps and to provide them with additional guidance. These key words should include WhatsApp and its competitors (e.g. imessage, ViBer, WeChat, Skype, Blackberry Messenger, SnapChat, Ansa) as well as more general terms such as "sms." These terms should also be reviewed and updated regularly because new programs are continually developed.

Finally, if you determine that employees are using these messaging programs, quick action is essential. WhatsApp messages can be recovered but the backup may be limited to a week or less.[vi] Messages on other apps like SnapChat may be deleted instantly. Local privacy restrictions may also prevent you from gaining access to these messages and should be consulted before reviewing the messages on an employees' device.

###

Please contact Neil Bloomfield at (704) 331-1084 or neilbloomfield@mvalaw.com with any questions.

---

[i] http://www.thetimes.co.uk/tto/business/industries/banking/article4396546.ece

[ii] http://www.ibtimes.co.uk/chelsea-fc-partner-capital-world-markets-investigated-by-police-over-alleged-fraud-1493530

[iii] http://www.statista.com/statistics/291540/mobile-internet-user-whatsapp/

[iv] http://www.bloomberg.com/news/articles/2014-10-28/facebook-s-22-billion-whatsapp-deal-buys-10-million-in-sales

[v] https://m.facebook.com/story.php?story_fbid=10152994719980011&id=500035010

[vi] https://www.whatsapp.com/faq/android/20887921;