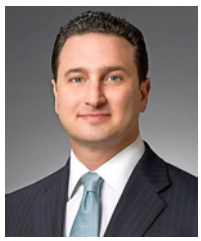
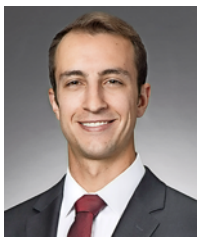
Bloomberg Government

Daily Report for Executives™

ENFORCEMENT

Electronic Communications in SEC Examinations and Investigations





BY PETER I. ALTMAN, KELLY HANDSCHUMACHER, AND BRETT MANISCO

Imagine you are an analyst at a hedge fund. You come into work on a Tuesday morning and send an iMessage from your smartphone to a co-worker complaining about how the hedge fund no longer pays for employees' parking. Next you get a message on Signal from your college friend about his recent thoughts on Bitcoin. Later in the day you come up with an idea for a derivative trade associated with an illiquid stock and want to run it by a contact at a bank in London. Since it is late in London, you decide it will be faster to contact the person on WhatsApp. You have a quick WhatsApp message exchange about your trade idea and the banker says he will come back with a proposed contract the next day.

The next month, the hedge fund you work for receives notice that it will be under examination by the SEC, pursuant to Section 204 of the Investment Advisers Act of 1940, which provides for examinations of investment advisers (''IAs''), including hedge funds. Under the Act, hedge funds such as yours must maintain certain documents as required ''books and records.''

Your hedge fund's chief compliance officer – or ''CCO'' – is concerned that the fund's employees may have been discussing work-related matters on communication platforms that the firm did not keep records of. The firm's policies and procedures require that its employees only send written communications about work matters on company email or Bloomberg chat, for which the firm maintains records. Your CCO thinks the firm's information systems team may be able to access records of certain communications sent through the firm's wifi. He wonders, if those records exist, can the firm be required to produce all of them in the examination? What if those records are of personal communications sent from employees' smartphones while at work? Does the firm have to hand those over as well?

Meanwhile, you start to wonder whether the SEC can access all of your personal communications because you are an employee of the hedge fund. Does it matter that you do not have a designated work smartphone but instead use your own smartphone for both work and personal use? And if the examination were to get referred to the SEC's Division of Enforcement for an investigation, would that change what the SEC is able to collect from you, including via subpoena? Would the SEC be able to access your communications from third

Peter I. Altman is a partner in Akin Gump Strauss Hauer & Feld LLP in Los Angeles. His practice focuses on representing investment management firms, private and public companies, and individuals in white collar and other government enforcement and regulatory matters, securities class action litigation, and internal investigations. Kelly Handschumacher and Brett Manisco are associates in the firm's litigation practice in Los Angeles.

 ISSN 0148-8155

party service providers like WhatsApp or Apple without your knowledge or consent?

Below we set out a summary of the current legal framework relating to the above hypothetical, and offer observations on what you can expect from the SEC given its current approach to electronic communications collection and review.

Which Electronic Communications Must an Investment Adviser Preserve?

Under Rule 204-2(a)(7) of the Advisers Act, an IA (your hedge fund in the hypothetical) must maintain ''records'' of all written communications sent or received by the IA and its personnel regarding a wide variety of matters including investment advice, buy/sell orders, receipt and distribution of funds or securities, and the performance of managed accounts or recommended securities.

Regardless of the medium, if any IA personnel sends or receives written communications covered under Rule 204-2, the IA is responsible for maintaining those records. If, for example, an IA places an order on a platform such as WhatsApp or confirms receipt of funds via Apple's iMessage, the IA is responsible for maintaining records of those communications. In the hypothetical, therefore, the hedge fund is responsible for maintaining a record of your WhatsApp communication with the London banker regarding a derivatives trade.

The importance of maintaining books and records in conformity with Rule 204-2 cannot be overstated. An IA's failure to properly maintain requisite books and records is not only a likely deficiency in an SEC examination, but it also increases the possibility of an investigation by the Division of Enforcement.

But maintaining those records may be a thorny issue. Notably, many communication service providers such as iMessage, Signal, and WhatsApp provide end-to-end encryption and some do not retain the contents of users' communications on their servers once those communications have been accessed by the users or a certain amount of time, such as 30 days, has passed. However, cloud storage providers may save copies of messages sent through encrypted communication platforms that can be unencrypted by the cloud storage provider. For example, iMessages that are normally end-to-end encrypted can be unencrypted by Apple if they are saved on iCloud storage instead of only locally on the user's phone. Still, for some encrypted messaging platforms like Signal, there may not be a practicable way of recordkeeping messages.

Regardless of the various issues associated with storage and accessibility, given that IA personnel could be using alternative communication platforms to discuss work matters, it is crucial for an IA to (1) take steps to ensure that IA-business related communications are not conducted over alternative platforms, or (2) take immediate steps to preserve records of any such communications if they are made.

Under the first approach, it is important for the IA to implement policies and procedures to prohibit its personnel from using alternative communication platforms for IA-business purposes and to monitor that such policies are in fact being followed. As just one example, an IA might implement a policy and procedure of monitoring emails for phrases such as ''text me'' or ''send to my Gmail'' and names of other communication platforms such as ''WhatsApp.''

Where an IA chooses the second approach of preserving records of communications on alternative platforms such as iMessage, Signal, or WhatsApp, it may need to hire outside companies to capture and store these communications because of complicated end-to-end encryption issues. An IA that permits employees to conduct IA business on alternative media must also consider whether it will adopt a policy of preserving all communications on a given medium or of preserving only those communications that are IA-business related, and if the latter, how the IA will determine which communications must be preserved.

Which Communications Can the SEC Request in an Examination?

The SEC's Office of Compliance Inspections and Examinations (''OCIE'') conducts regular examinations of IAs to improve compliance, prevent fraud, monitor risk and inform policy. While in practice the scope of documents requested in an exam varies based on factors such as the IA's business structure and internal control environment, OCIE takes the position that it has the authority to request all records of IAs, not just those required to be maintained by investment advisers under Rule 204-2. OCIE interprets ''records'' pursuant to the Securities Exchange Act of 1934 § 3(a)(37) definition as ''accounts, correspondence, memorandums, tapes, discs, papers, books, and other documents or transcribed information of any type, whether expressed in ordinary or machine language.'' That, in OCIE's view, includes all non-privileged electronic communications that an IA retains, which can mean any communications that move through an IA's computer servers.

In 2017, OCIE conducted sweep examinations targeting IA policies and procedures around IA personnel's electronic messaging on platforms such as instant messaging, text/SMS messaging, and personal or private messaging whether conducted on the IA's systems or third-party platforms. These sweep examinations indicate that OCIE has a growing interest in communications on alternative platforms. And given that smartphone app usage is now commonplace, OCIE could also begin to request such messages if they are retained by an IA (perhaps in an effort to comply with recordkeeping requirements), regardless of whether the messages are personal or business-related.

There are numerous ways an IA may have broad records of employee communications that could be subject to examination. For example, if an IA maintains data from IA-owned devices, such as smartphones or computers issued to its employees, then that data could be subject to examination as records of the IA. Thus, in the hypothetical, if your smartphone had been issued by the hedge fund, then data of your activities such as messaging friends on WhatsApp or iMessage could be retained by the hedge fund and subject to examination.

Even where employees use their own devices, if an IA saves data regarding its employees' Internet activity on those devices through the IA's wifi, OCIE could potentially deem any such records to be subject to examination. This could include activity ranging from Google searches on a desktop computer at the office to sending messages on a personal smartphone using office wifi.

  DER ISSN 0148-8155

Thus, in the hypothetical, while the hedge fund might not have access to the substance of communications sent through smartphone apps, it could have records of Internet activity on its wifi network.

Which Communications Can the SEC Subpoena in an Investigation?

If your hedge fund's examination gets referred to the SEC's Division of Enforcement for an investigation, the SEC will have greater tools at its disposal to obtain information from your hedge fund and its employees, as well as innumerable third parties. The SEC's broad investigative powers derive from a combination of statutory authority and Supreme Court precedent, which gives the Commission power to subpoena a vast range of materials based on little more than a suspicion that an individual or entity has violated, is violating, or is about to violate securities laws. *See* 15 U.S.C. § 78u; *United States v. Powell*, 379 U.S. 48 (1964).

The Division of Enforcement can exercise nationwide subpoena power as soon as it obtains a formal order of investigation from the Commission, which is granted after internal review by senior officers in the Division. And unlike searches and seizures in criminal investigations, subpoenas in SEC investigations do not require a showing of probable cause or approval from an independent judge. Rather, SEC subpoenas are subject to largely deferential review under the ''legitimate purpose'' standard set forth in *Powell*, 379 U.S. at 57-58 (judicial enforcement of administrative subpoena is contingent on whether: (1) the inquiry is conducted for a legitimate purpose; (2) the inquiry is relevant to that purpose; (3) the information sought is not already within the agency's possession; and (4) the subpoena was issued in accordance with the required administrative procedures). Under this standard, the SEC has the power to issue administrative subpoenas for virtually anything it deems relevant to its investigation.

However, the SEC's ability to subpoena records from entities like Google or WhatsApp (third party electronic communication or remote computing service providers) is somewhat limited by the Stored Communications Act provision under the Electronic Communications Privacy Act of 1986 (''ECPA''). Under ECPA, the SEC can subpoena basic subscriber information from service providers without sending notice to the subscriber. This basic subscriber information includes information such as a user's name, address, session times and durations, length of service, types of services used, telephone number, IP address, other identity information, and means and source of payment for service, including any credit card or bank account number. See 18 U.S.C. § 2703(c)(2). Thus, in the hypothetical, the SEC could obtain subscriber information about you from Apple, Signal, and WhatsApp, without having to send any notice to you that it was obtaining such information. This type of information would confirm that you are the owner of a particular account, such as your WhatsApp account.

Under ECPA, the SEC cannot compel from third party service providers the contents of electronic communications that are 180 days old or less and not considered to be in remote computer storage (*i.e.*, no longer being used for communications purposes). But ECPA permits the SEC to obtain any communication held by a service provider that is greater than 180 days old through an administrative subpoena, provided that the SEC gives notice to the user. 18 U.S.C. § 2703(a)-(b); *see also* 18 U.S.C. § 2705 (allowing delayed notice in certain circumstances). Theoretically the SEC could simply wait the requisite period of time to obtain the contents of any communication from a service provider.

While the statutory 180-day rule may seem arbitrary and inadequate to prevent government abuse of privacy, case law has deterred the SEC from subpoenaing the content of users' communications from third party service providers, regardless of how old the communications are. Notably, in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), the Sixth Circuit held that government agents violated a defendant's Fourth Amendment rights when they compelled his internet service provider (''ISP'') to produce the content of his emails without first obtaining a warrant based on probable cause. Though this decision was made in the criminal context rather than the civil regulatory context, it led the SEC, as a matter of practice, to refrain from seeking the content of emails from ISPs. *See* ''An Uneasy Relationship: The SEC and the Electronic Communications Privacy Act,'' Securities Regulation & Law Report, 49 SRLR 297 (2017). As former SEC Chair Mary Jo White explained in a 2013 letter to Senator Patrick Leahy, Warshak ''greatly impeded the SEC's ability to serve administrative subpoenas on ISPs absent the consent of the subscriber.'' In fact, the SEC's current Enforcement Manual does not anywhere provide that a staff attorney can subpoena anything beyond a user's basic subscriber information from a service provider without the consent of the user. *See* SEC Enforcement Manual, dated November 28, 2017, § 4.6 ''Compliance with the Electronic Communications Privacy Act of 1986.''

Despite this apparent limitation on the SEC's subpoena power, the Commission recently took the position that *Warshak* does not apply to administrative subpoenas. In *SEC v. Yahoo, Inc.*, Case No. 8:15cv1339 (D. Md), argued on June 30, 2017, the SEC sought to use an administrative subpoena to compel Yahoo to produce the content of a user's private emails. In its reply brief, the SEC argued that *Warshak* does not require a government agency to obtain a warrant based on probable cause to compel a service provider to produce the content of emails without its user's consent. Rather, the SEC maintained that *Warshak* simply requires that a government agency notify the user that it has subpoenaed the content of the user's emails from the service provider so that the user has the opportunity to challenge the reasonableness of the subpoena in court. The SEC reasoned that judicial review for reasonableness is the key protection afforded by the Fourth Amendment. Thus, subpoenaing a service provider for the content of a user's email while also providing the user notice and a chance to challenge that subpoena does not violate the Fourth Amendment. The Court did not rule on this argument because the issue became moot when the user subsequently authorized Yahoo to provide the SEC access to his emails. The SEC's position in *Yahoo* may signal a more aggressive stance by the SEC going forward in seeking electronic communications from service providers without users' consent, a shift from its position in the years immediately following *Warshak*.

So where does this leave you as the hypothetical hedge fund analyst? If you choose to challenge an SEC subpoena to you of all your WhatsApp communications

with the London banker in the past year, the SEC might not be able to obtain the contents of your WhatsApp communications (to the extent WhatsApp even maintains that information on its servers) from WhatsApp without your consent. However, as in *Yahoo*, the SEC may take an aggressive stance on demanding the contents of communications, and you may be held in contempt of court if the SEC's subpoena is legitimate and you still refuse to produce the information yourself or consent to a service provider producing the information.

And where does this leave your hypothetical hedge fund? First, the fund may be liable for recordkeeping violations to the extent required communications by its personnel were not properly maintained as adviser records. The SEC's authority to subpoena communications not only from hedge fund personnel but also from third party service providers enhances its ability to detect and enforce incomplete recordkeeping. Second, the hedge fund could be liable for securities law violations by its personnel that are detected by the SEC in subpoenaed communications from alternative platforms. In an investigation, the SEC is well positioned to discover securities violations that a hedge fund did not itself detect because it can access the contents of communications from alternative platforms whether by subpoenaing the information from you as one of its analysts directly, from a service provider with your consent, or, more aggressively and not clearly legally, from a service provider without your consent.

And at that point, liability could expand dramatically. For example, if the SEC subpoenas WhatsApp messages and discovers that you told a friend that your hedge fund was planning to build up its position in a company to ten percent ownership within the next week, then the hedge fund could be liable for your sharing of material nonpublic information and potential front-running harm to its clients. And if your hedge fund did not monitor WhatsApp communications, it likely would learn of this violation for the first time during the investigation.

Conclusion

In sum, the SEC can access a broad array of documents, both in the examination and the investigation setting. And in recent years the SEC has shown a voracious appetite for data. If you are the hypothetical hedge fund employee, you should use firm-approved communication platforms for business and keep your personal communications out of that ecosystem. You must remain cognizant that any firm-related written communications on platforms not generally used for work, such as WhatsApp, iMessages, Gmail, or Facebook, could be accessed by the SEC at some point. In addition, your CCO should ensure the hedge fund is complying with Rule 204-2 by capturing all work-related written communications on any platform through robust policies and procedures and monitoring the effectiveness of those policies and procedures.

  DER ISSN 0148-8155