Bloomberg Law®

bloombergbna.com



# INSIGHT: SEC Required Recordkeeping in an Evolving Privacy Landscape



By Peter I. Altman, Annie Banks, and Kelly Handschumacher

**Introduction**

An investment professional, Paul Iacovacci, recently filed suit against his former employer, Brevet Capital Management LLC, an SEC-registered investment adviser, for alleged violations of federal and state privacy law violations. *Iacovacci v. Brevet Holdings, LLC*, Case No. 1:18-cv-08048 (S.D.N.Y. filed Sept. 4, 2018). Iacovacci has alleged that after he set up his employer-provided computer at home with remote access via the LogMeIn software, Brevet remotely obtained information stored on his personal external hard drives and in his personal email account. Brevet has denied that any unauthorized access occurred, stating that the SEC requires it to maintain the ability to remotely monitor employees' communications.

The case raises questions about the balance between SEC-registered firms' needs to monitor employee communications—for, among other things, regulatory compliance and the protection of trade secrets—and employees' privacy rights. This article will provide an overview of these issues in the context of SEC regulations, surveying what employers *must* do in order to comply with federal securities laws, what employers *should* do to be mindful of both federal and state privacy laws, and what employers *can* do regarding best practices for finding a balance to both.

**SEC Recordkeeping Requirements** In the first instance, SEC-registered investment advisers (''RIAs'') are required to maintain, and therefore must be able to access, certain records of the business, which may necessarily involve email communications and other electronic data. To be sure, compliance with the ''books and records'' requirement of Rule 204-2 of the Advisers Act is crucial for RIAs. Failure to do so is not only a likely deficiency in an SEC examination, but it also increases the possibility of an investigation by the SEC's Division of Enforcement. *See* Peter Altman et al., *Electronic Communications in SEC Examinations and Investigations*, 1 DER 1-2-18 (2018).

Rule 204-2 requires that an RIA maintain records, which can include communications, regarding a wide variety of matters, including investment recommendations made or proposed to be made on behalf of a client, investment advice given or proposed to be given to a client, buy/sell orders on behalf of a client, receipt and distribution of funds or securities, and the performance of managed accounts or recommended securities. *See* 17 CFR § 275.204-2(a)(7).

Regardless of the medium of communication, if any RIA personnel sends or receives written communications covered by Rule 204-2, the RIA is responsible for maintaining those records. If, for example, an RIA employee makes an investment recommendation to a client on his or her personal Gmail account or sends a trade instruction via Apple's iMessage platform, the RIA is responsible for maintaining records of those communications.

To the extent RIA personnel send and receive communications subject to Rule 204-2 on platforms or devices that are *not* captured by the RIA's systems, the RIA should take immediate steps either to (1) direct employees to send such communications via authorized platforms and devices, or (2) capture those communications made on the non-RIA communication platforms and devices.

Under the first approach, the RIA should implement policies and procedures to prohibit its personnel from using non-RIA communication platforms and devices

for RIA purposes and to monitor that such policies are in fact being followed. For example, an RIA might run searches across its email system for phrases such as ''text me,'' or the names of communication platforms such as ''Wickr'' or ''Gmail,'' to monitor compliance with policies against employee use of non-RIA platforms for work purposes.

Under the second approach, however, privacy issues may arise. RIAs capturing communications made on non-RIA-managed communication platforms and non-RIA-owned equipment should take into account the following issues.

**Privacy Issues** Broadly speaking, various federal and state privacy laws pertain to access to electronic communications. And while this article focuses solely on U.S. law, RIAs in the U.S. may also be subject to overseas privacy laws. For example, an RIA's collection, storage, and disclosure to the government of records subject to Rule 204-2 could fall under the European Union's General Data Protection Regulation if, for example, the RIA's records include the personal data of any of the RIA's employees located in the European Union.

At the federal level, the Computer Fraud and Abuse Act (''CFAA'') prohibits knowingly accessing an employee's device (*e.g.*, computer or smartphone) without authorization. *See* 18 U.S.C. § 1030; *see also United States v. Kramer*, 631 F.3d 900 (8th Cir. 2011) (finding that smartphones fall within the CFAA's definition of ''computer''). The Electronic Communications Privacy Act (''ECPA'') extends privacy protections against phone wiretapping to modern forms of technology by prohibiting the intentional interception of digital and electronic communications such as email and text messages. *See* 18 U.S.C. § 2510. The Stored Communications Act (''SCA'') prohibits intentionally accessing, without authorization, employee communications stored on the internet (*e.g.*, web-based email services like Gmail and Yahoo!). *See* Title II to the ECPA, 18 U.S.C § 2701.

Additionally, state laws provide employees with common law civil rights of action (*e.g.*, trespass to chattels, conversion) and, more recently, statutory causes of action (*e.g.*, computer trespass) for violations of employees' privacy interests. Indeed, all 50 states have enacted laws against computer trespass or unauthorized computer access. *See, e.g.*, Cal. Penal Code § 502.

Employees' privacy rights are not, however, absolute. Any privacy analysis in this space begins with the question of who owns the communications—the employee or the employer. Courts routinely hold that emails sent and received via an employer-owned domain, and data stored on employer-owned devices, are employer property, such that employees do not have a reasonable expectation of privacy in these emails or data, nor any of the corresponding legal protections. *See, e.g.*, *Muick v. Glenayre Elecs.*, 280 F.3d 741 (7th Cir. 2002); *TBG Insurance Services Corp. v. Superior Ct.*, 96 Cal. App. 4th 443 (Cal. Ct. App. 2002). Employers should be aware, however, that a few states have nonetheless enacted laws requiring employers to give notice prior to monitoring employees' work emails or employer-owned devices. *See, e.g.*, Conn. Gen. Stat. § 31-48d; Del. Code tit. 19, § 7-705.

The line between ''employer-owned device'' and ''personal device'' has become increasingly blurred with the proliferation of BYOD (''Bring Your Own Device'') programs. Employer-owned devices generally include those provided by the employer to the employee to use for work purposes, and maintained under a company account. Conversely, a device that is purchased by an employee, and serviced by an account opened and maintained by the employee, is generally considered a ''personal device.'' Whether or not an employer reimburses an employee for some or all of the device's service fees is not generally controlling, especially given that some states mandate that employers reimburse employees when they are required to use personal devices for work. *See, e.g.*, Cal. Lab. Code § 2802; *Cochran v. Schwan's Home Services*, 228 Cal. App. 4th 1137 (Cal. Ct. App. 2014). Employees have privacy interests in their personal devices (including in the non-work-related communications and data stored on them) such that employers' attempts to access information on them may implicate privacy laws. *See Riley v. California*, 134 S. Ct. 2473 (2014) (recognizing privacy interest in data stored on cellphones).

Another gray area exists in the space where personal and work information overlap, such as with Iacovacci's personal email account that was accessed on his work computer. Though there are no bright-line rules, a review of the case law suggests privacy issues in this gray area will turn on whether the employer has prior authorization to access an employee's personal communications (including due to company policies), and whether the employee, versus the employer, was the cause for such information being made available to the employer.

*Personal Email Accounts.* In general, employers may not access an employee's personal email account, regardless of whether on a personal or work device, without authorization. *E.g.*, *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010). What defines ''access'' and ''authorization'' here, however, is not well-settled. For example, an employer may be able to analyze digital trails (''breadcrumbs'' or electronic artifacts) left on a work device and thus company property to view an employee's personal email data without actually accessing that employee's email. *See, e.g.*, *Thygeson v. U.S. Bancorp*, 2004 U.S. Dist. LEXIS 18863 (D. Or. Sept. 15, 2004); *Leventhal v. Knapek*, 266 F.3d 64 (4th Cir. 2000); *McLauren v. Microsoft Corp.*, 1999 Tex. App. LEXIS 4103 (Tex. App. May 28, 1999). On the other hand, using an employee's auto-filled password on a work device to access their personal email is unlikely to be considered proper authorization. *See, e.g.*, *Rene v. G.F. Fischers, Inc.*, 817 F. Supp. 2d 1090 (S.D. Ind. 2011) (accessing employee's personal email by using keystroke-logging software on work computer supported claim for SCA violation).

*Servers and Cloud Storage.* Employers may not typically access employees' personal, non-work-related information stored on personal devices (such as text messages and pictures) without authorization. Further, employers likely also cannot access an employee's cloud-based storage (*e.g.*, Dropbox or Google Drive) without the employee's authorization even if an employee has saved company data to the cloud. *See* Julie Totten, *Balancing Workplace Technology and Privacy in the 21st Century* at 48, Am. Bar Ass'n (Mar. 22, 2017).

But if an employee's personal, non-work related information is processed through an employer's servers or cloud storage (*e.g.*, when an employee backs up their personal device's text messages or pictures to their

work computer or cloud), the employee may have relinquished their privacy rights to such information. Federal laws such as the SCA that require the employer's act to be intentional can relieve an employer of liability where information is made available to the employer because of the *employee's* acts, as opposed to proactive steps by the employer to extract such information. *See, e.g., Sunbelt Rentals, Inc. v. Victor*, 43 F. Supp. 3d 1026 (N.D. Cal. 2014) (no liability under the Wiretap Act and SCA where employer gained access to employee's text messages because employee synced work device to cloud service); *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748 (N.D. Ohio 2013) (granting employer's motion to dismiss employee's claims under the ECPA when employer accessed employee's personal emails that had already been opened on employee's work-issued phone, but denying motion as to personal email *not* already opened); *NovelPoster v. Javitch Canfield Group*, No. 13-cv-5186, 2014 WL 3845148 (N.D. Cal. Aug. 14, 2014) (accessing emails already received in an email account's inbox does not constitute interception under the Wiretap Act because the transmission has already occurred).

*Prior Authorization & BYOD.* Company policies that are sufficiently broad (extending to personal email accounts and personal devices) and explicit (providing notice of monitoring and accessing) can help establish that employees have authorized their employer to access their personal communications and data.

In *Sitton*, for example, the state appellate court in Georgia in 2011 addressed a situation where an employee used his personal computer for both work and personal purposes, including while on the company's premises and connected to its network. *Sitton v. Print Direction, Inc.*, 312 Ga. App. 365 (2011). After the employer suspected the employee of supporting a competing business, a manager entered the employee's office, accessed the employee's non-work email account that was open on this computer, and printed out emails that supported the employer's suspicions. The appellate court affirmed the dismissal of the employee's claims for computer trespass, theft, and invasion of privacy. The court held that lack of authority was a required element for all claims, and that the employer's policies adequately established the employer's authorization because they explicitly applied to both work and personal devices, and provided notice to employees that such devices could be subject to employer inspection upon suspicion of inappropriate behavior.

Though the company policy in *Sitton* was notably broad, employers exerting control over employees' personal devices as part of a BYOD (''Bring Your Own Device'') program must consider whether their policies sufficiently provide authorization, and whether such controls risk violating federal or state privacy laws. In *Pollard*, for example, a state court in New York in 2014 evaluated a scenario where an employee allowed his employer to set up his work email on his personal iPhone. *Advanstar Commc'ns., Inc. v. Pollard*, 2014 N.Y. Misc. LEXIS 4104 (N.Y. Sup. Ct. Sept. 10, 2014). Part of this set-up included installing a remote wipe function, which the employee claimed he did not authorize. After the employee gave notice of leaving the company, the employer used the remote wipe function to delete all data from the employee's iPhone.

The employee sued, alleging that the employer's remote wipe function violated the SCA's prohibition against intentionally accessing an electronic ''facility'' without authorization and illegally obtaining access to his electronic communications while they were in ''electronic storage.'' The court dismissed the employee's claim. The court cited to and agreed with other court decisions (*e.g.*, *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012)) holding that a cell phone is not a ''facility'' under the SCA, ''nor is the information on a cell phone in the form of emails, text messages, pictures, and the like considered 'in electronic storage.' '' The court further clarified that under the SCA, ''electronic storage'' encompasses only information stored by an Internet provider (including for temporary purposes pending delivery or for purposes of backup protection), not information stored on a personal hard drive or cell phone.

Note, however, that employer controls over employees' personal devices (such as the remote wipe function in *Sitton*) would only be permissible to the extent provided for in the employer's BYOD policies, and would not extend to data held by third-parties, such as web-based email providers and cloud storage providers, due to the CFAA and SCA. *See, e.g., Hoofnagle v. Smyth-Wythe Airport Comm'n*, 2016 WL 3014702 (W.D. Va. May 24, 2016) (personal emails from plaintiff's private Yahoo! web-based email account, residing in Yahoo!'s servers, qualified as ''electronic storage'' under the SCA).

**Conclusion** As noted above, RIAs may need to capture a wide variety of employee data to comply with Rule 204-2 under the Advisers Act. Given the rapid growth of use of technologies such as smartphones, remote computing, and cloud storage, RIAs should take a fresh look at their policies and procedures to ensure they reflect the technology utilized by firm employees and authorize employer access as needed to satisfy books and records obligations. There is no one-size-fits-all solution, and thus RIAs should consider custom policies and procedures that reference, as needed, both employer-owned and personal devices and different mediums of electronic storage and communication. Clear policies and procedures in this area will help answer the difficult questions of whether an employer has ''authorization'' to ''access'' the vast amounts of data that employees generate on a daily basis.

*Peter I. Altman is a partner, and Annie Banks and Kelly Handschumacher are associates at Akin Gump Strauss Hauer & Feld LLP. All are members of the firm's litigation practice in Los Angeles.*

*Peter Altman represents investment management firms, private and public companies and individuals in white collar and other government enforcement and regulatory matters, securities class litigation and internal investigations. He also advises investment advisers on day-to-day risk management issues related to topics including securities trading, compliance with the Investment Advisers Act and the use of big data and alternative forms of electronic communication. He is a former member of the SEC's Division of Enforcement.*

*Annie Banks focuses her practice on commercial litigation. She has defended class actions lawsuits involving claims for violations of federal securities laws, federal data privacy laws, and state privacy laws. She also has represented public and private companies in government enforcement and regulatory matters, securities class action litigation, and internal investigations.*

*Kelly Handschumacher's experience includes consumer class action defense, securities fraud class action defense and other complex commercial litigation. She also has experience representing individuals and investment advisers in government investigations and examinations.*