CLIENT ALERT

'You Looked At What?' SCA Traps for Employers Who Access Personal Social Media or Email Accounts

Sep.05.2013

The recent decision in *Ehling v. Monmouth-Ocean Hospital Serv. Corp.* (MONOC), No. 2:11-cv-03305, 2013 WL 4436539 (D.N.J. Aug. 23, 2013) serves as a reminder of the potential dangers to employers that access an employee's or former employee's personal social media or email accounts without their authorization. In *Ehling*, the court found that an employee's posts on her personal Facebook account would have otherwise been protected by the Stored Communications Act (SCA) because she had set her privacy settings on the account to only make her posts available to her Facebook "friends." However, MONOC escaped liability for viewing certain of Ehling's posts – after which it terminated her employment – because MONOC had received unsolicited emails containing screenshots of the posts from one of Ehling's co-workers who was a Facebook "friend" of Ehling. MONOC itself had not accessed Ehling's Facebook account. As such, the court found that the authorized user exception to the SCA applied. The decision highlights the need for employers to understand the reach of the SCA as they contemplate the scope of any investigation of their employees' personal social media or email accounts.

Passed in 1986 as part of the Electronic Communications Privacy Act, the SCA prohibits individuals from accessing without authorization nonpublic, electronic communications that are in electronic storage and that were transmitted originally via an electronic communications service. In practice, the SCA is often read to restrict an individual from accessing the email account of another person – typically by accessing the servers of the third-party email service provider (such as Google, Microsoft, or Yahoo) – without the authorization of that other person. The SCA carries both criminal sanctions and civil penalties, including statutory damages of $1000 for each violation, actual damages, punitive damages, and attorneys' fees and costs.

As the *Ehling* court noted, because the law was passed before the explosion of the internet, email and social media, much of the interpretation of the law has been left to the courts. The decision in *Van Alstyne v. Electronic Scriptorium Ltd.*, 560 F.3d 199 (4th Cir. 2009) is representative of courts' handling of issues arising under the SCA in the employment context. There, the court found the former employer violated the SCA when it accessed the personal AOL email account of a former employee for several years after her termination without her knowledge or authorization.

Similarly, at least one court has found that a former employer could not use, as evidence in litigation, emails obtained from multiple personal email accounts of a former employee which demonstrated the former employee was potentially improperly competing against the former employer prior to terminating his employment. *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008). The court reached that conclusion because the emails were obtained in violation of the SCA. As part of gathering facts for the litigation, the plaintiff former employer examined the company-owned computer used by the founder of the defendant company when he was still employed by the plaintiff. The plaintiff found that the username and password for the founder of the defendant company's Hotmail account was auto-populated via the cookies on the computer. The plaintiff just hit the log in button and was able to then view the founder of the defendant company's Hotmail account. In the course of reviewing that account, the plaintiff discovered the founder of the defendant company's Gmail username and password and accessed that account as well. The plaintiff tried to defend its action by claiming that the plaintiff's

computer use policy made it clear that there was no expectation of privacy, and/or that by leaving his Hotmail login information on the computer, the founder of the defendant company had provided implied consent. The court rejected both of these theories. On the company policy theory, the court said the company policy was limited to use of "company equipment" – meaning "any matter stored in, created on, received from, or sent through the plaintiff's system." The court found this policy did not apply then to emails stored on Microsoft or Google servers. In addition, there was no evidence that the emails accessed were created on, sent through, or received on the plaintiff's computers as there was no evidence the founder of the defendant company had sent those emails from the plaintiff's computer, as opposed to sending them from a home computer during his off time. As for the implied consent, the court found the founder of the defendant company's carelessness in leaving his username and password auto-populated did not constitute consent for the plaintiff to access and review his personal email.

While *Van Alstyne* and *Pure Power Boot Camp* involve accessing personal email accounts of employees or former employees, the extension of the protections of the SCA to private Facebook posts in *Ehling* is not unexpected and follows a similar decision in *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 991 (C.D.Cal. 2010). Facebook posts are electronic communications that are often stored in perpetuity. Posters can use privacy settings to prevent them from being public. In light of this reality, best practices for employers who are tempted to review the personal social media or email accounts of employees or former employees include:

- Ensure your applicable computer, internet and email use policy clearly notifies employees that there should be no expectation of privacy in their use of any company-owned equipment, their use of personally-owned devices used for work purposes pursuant to a "Bring Your Own Device" policy, or in their use of personal email or social media accounts accessed through company-owned equipment. Although such policies cannot fully insulate an employer from SCA liability if the employer accesses an employee's personal account, the employer would be better positioned to argue that its accessing of the personal account was authorized by such a policy and, therefore, did not violate the SCA. Notably, there are no reported decisions directly addressing such an argument.
- Use appropriate internal or external resources to take a forensic image of the employee's or former employee's company-owned computer or other relevant electronic device in the course of litigation or when litigation is anticipated. The search of that image, which may include discovery of copies of personal employee emails captured from the temporary files on the computer, will not violate the SCA as it does not involve accessing the servers of a third-party like Microsoft or Google.
- Do not access the personal email or social media accounts of employees or former employees without express written authorization of the individuals. This prohibition applies even if the username and password for the account are auto-populated, as in the *Pure Power Boot Camp* case noted above. That being said, employers can and should actively monitor, manage and access company-owned social media and email accounts without running afoul of the SCA.
- Do not coerce or pressure employees or former employees to provide that authorization, or to provide you with screenshots from the accounts of other employees or former employees with whom they are "friends." Courts have found that such coercion destroys the authorization necessary to avoid SCA liability. Moreover, a number of states have already enacted or are considering laws that prohibit employers from requiring employees or applicants to provide the passwords for, or otherwise provide access to, their personal social media accounts in most circumstances, including in support of a job application, or other employee conduct not involving an internal company investigation of a matter.
- Do not create, or encourage any employee or former employee to create, a social media or email account using a fake identity in order to "friend" the employee or former employee from whom you are trying to discover information.

- If, however, an employee or former employee voluntarily provides screenshots from the personal social media account of another employee or former employee, or provides you emails between the parties, you may use those documents (assuming they were not obtained using a fake identity) in dealing with the targeted employee or former employee without violating the SCA.
- If you are in litigation with the targeted employee or former employee, use robust discovery requests related to personal social media or email accounts to obtain communications or posts contained in such accounts. If an employee has threatened litigation, consider issuing a preservation notice, instructing the employee (or his or her counsel) to refrain from deleting any relevant documents that may be stored in personal email accounts, Facebook, or other social media.

Employers who follow the practices above will be in the best position to obtain the desired information about the particular employee or former employee at issue without creating any potential criminal or civil liability under the SCA.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Kris D. Meade
Partner – Washington, D.C.
Phone: +1 202.624.2854
Email: kmeade@crowell.com