Employee Privacy Laws, Emails, and Social Media: What Is Protected Under The Law

by Catherine Pastrikos Kelly

In 1986, Congress passed the Stored Communications Act (SCA), which aims to prevent people from accessing private electronic communications. At that time, there was no internet—let alone email or social media, as we know them. As a result, courts have had to adapt the language of the SCA to technology's rapid evolution. The resulting decisions are surprising.

In addition to the SCA, most states have some form of privacy laws, which protects against the intrusion upon the solitude or seclusion of a person or their private affairs, which has been interpreted to include email and social media.

This article will discuss the law from courts around the country relating to the breadth of employee's privacy in the context of email and social media accounts.

Employer's Access of Employee Personal Email Accounts

Courts have ruled that an employer can be held liable under the SCA and state invasion of privacy laws if an employer accesses an employee's personal email account—even if the employee accessed their account on a company-issued device and the employee saved the username and password on the device. For example, in *Markert v. Becker Technical Staffing, Inc.*, the United States District Court for the Eastern District of Pennsylvania suggested that a violation of privacy under Pennsylvania law occurred when an employer accessed an employee's private email messages without the employee's permission after the employee accessed his personal email on the company computer and failed to logout.[1] In that case, the employee logged into his personal Gmail account on his work computer and did not log out, causing his personal email inbox to appear on the screen of his work computer.[2] Included in this inbox was an email that discussed what the employer believed was an attempt to divert business away from the employer.[3] When the employer saw the email, he searched through the rest of the employee's personal emails.[4] The next day, the employer fired the employee.[5] The court determined that a plaintiff has a claim for invasion of privacy against a person who invaded their privacy by reviewing their personal emails and disseminating the information.[6]

Similarly, the United States District Court for the Northern District of Ohio in *Lazzette v. Kulmatvcki* determined that an employer was liable for reading a former employee's emails on a company-issued device.[7] In that case, the employer issued a BlackBerry to the employee and gave the employee permission to use it to access her personal email account.[8] When the employee left the company, she returned the BlackBerry believing that she had erased her personal account from the device.[9] Despite her efforts, however her personal email account was still on the BlackBerry.[10] Thereafter, the employee's former supervisor spent the next year and a half parsing through nearly 50,000 personal emails regarding the employee's family, financial, career and other personal matters.[11] When the employee discovered what happened, she filed an action against her former supervisor and employer under the Ohio privacy laws and SCA for reading her emails without permission.[12] The court reasoned that the former supervisor and employer did not have permission to read the employee's messages despite being left on a company-issued device.[13] Additionally, the Court ruled that the employee's failure to delete the emails from the device did not provide the supervisor or employer with authorization.[14] On the Ohio privacy claims, the Court noted that a reasonable jury may deem it highly offensive for an employer and supervisor to read a former employee's private and sensitive emails.[15]

The key inquiry for the court in employer invasion of privacy cases hinges on balancing the employee's privacy with the employer's legitimate interest in preventing misuse of its network. In *Mintz v. Mark Bartelstein and Associates Inc.*, the United States District Court for the Central District of California found an employer invaded

an employee's privacy when the employer accessed the employee's personal email account by retrieving a temporary password to obtain a copy of the employee's contract with a new employer.[16] The court held that the employee had a reasonable expectation of privacy in his personal, financial, and employment information and in his web-based, password protected personal email account that he used for personal matters.[17] Moreover, the Court found that the employer had no competing interest to justify the invasion of privacy.[18]

Conversely, employees have a lesser expectation of privacy when they communicate using a company email system. In *Smyth v. Pillsbury Co.*, the United States District Court for the Eastern District of Pennsylvania concluded that an employee did not have a reasonable expectation of privacy in emails he voluntarily sent to his supervisor over the company email system, notwithstanding assurances from the employer that such communications would not be intercepted by management.[19]

Contacting an Attorney from Your Company-Issued Device

Courts generally hold that an employee's communications with their attorney remain privileged if made via a personal email account regardless of whether the employee used a company-issued device to contact their attorney and even if the employer's computer policy says otherwise. For example, the Supreme Court of New Jersey ruled in *Stengart v. Loving Care Agency* that an employer could not review an employee's communications with her attorney via her personal email account even though they were on the employer's network and saved on the employee's company-issued computer because the employee retained a reasonable expectation of privacy.[20] In that case, the employee used her company-issued laptop to exchange emails with her lawyer through her personal email account, and she later filed an employment discrimination suit against her employer.[21] In discovery, the employer hired a computer forensic expert to recover all files stored on the employee's laptop including the emails, which were automatically saved on the hard drive.[22] The employer's attorneys reviewed the emails and used information culled from them in discovery.[23] In response, the employee's attorneys demanded that the employee's attorney-client privileged communications be identified and returned but the employer refused.[24] The court ruled that the employee can reasonably expect that emails with her lawyer on her personal email account would remain private and that sending and receiving them via a company-issued laptop did not eliminate the attorney-client privilege.[25]

Similarly, the United States District Court for the Eastern District of New York ruled in *Pure Power Boot Camp v. Warrior Fitness Boot Camp* that an employer's access of an employee's personal emails, including attorney-client privileged communications, was unauthorized and violated the employee's privacy.[26] There, the employer accessed and printed emails from three of the employee's personal email accounts.[27] The employer was able to access the first account because the employee left the username and password stored on the employer's computer.[28] The employer accessed the second account by having the email provider send the credentials to the first account.[29] The employer accessed the third account by making a "lucky guess" at the employee's password.[30] The employer's handbook stated that employees have no right of privacy in anything sent over the employer's system, including personal email accounts.[31] The court determined, however, that the employee had a subjective belief that his personal email accounts would be private and that nothing in the employer's policy suggested that it could extend beyond the employer's own systems.[32] In addition, the court determined that there was no evidence the employer's policies were clearly communicated to employees or consistently enforced in a manner that would have alerted employees to the possibility that their private email accounts could be accessed and viewed by their employer.[33]

The Eastern District of New York also ruled in *Curto v. Medical World Communications, Inc.* that despite a computer policy prohibiting personal use of email and advising that the employer could monitor employee computer usage, an employee's email communications to her attorney were privileged.[34] In that case, an employee working from a home office sent emails to her attorney on a company laptop using her personal email account.[35] Although the messages did not go through the employer's server, they were retrievable by the employer.[36] The court ruled these messages were privileged despite the computer policy because the employee took reasonable precautions to prevent inadvertent disclosure in that she sent the emails through her personal email account and the employer did not regularly monitor employee computer usage.[37]

Employer's Access of Employee Social Media Accounts

Courts have held that an employer can be liable under the SCA or state privacy laws for accessing an employee's social media accounts if the employee has not "friended" the employer. In *Pietrylo v. Hillston Restaurant Group*, the United States District Court for the District of New Jersey held that the employer was liable for invasion of the employee's privacy after a manager requested that an employee provide him the username and password to an employee MySpace group messaging site.[38] The employee who gave the manager the log-in credentials testified that she felt compelled to provide the manager with the credentials or her job would be at risk.[39] The Court ruled that the manager and employer accessed the group messaging site without authority, thereby violating the employee's privacy.[40] As a result, the Court determined that the manager and employer were liable under the SCA and state invasion of privacy law.[41]

Much turns on the facts of the case, however. For example, in *Ehling v. Monmouth-Ocean Hospital Service Corp.*, a hospital supervisor accessed a nurse's personal Facebook account by using a co-worker's Facebook log in who was friends with the nurse.[42] The supervisor read one of the nurse's posts that the supervisor believed showed a lack of regard for patient safety and, as a result, the nurse sued the hospital for invasion of privacy.[43] The hospital argued that the nurse could not have had an expectation of privacy in statements she posted publicly on Facebook.[44] The District of New Jersey determined the nurse did not have a reasonable expectation of privacy because her employer was "authorized" to access her Facebook post as she voluntarily became Facebook friends with the co-worker, who could then see her posts, and the co-worker voluntarily provided the plaintiff's Facebook posts to the supervisor.[45]

Conclusion

Violations of the SCA and state privacy laws are severe and can include fines and jail time. Therefore, it is important for employers and employees alike to understand the implications of invasion of these claims. ■

Catherine Pastrikos Kelly is a partner at Meyner and Landis LLP and specializes in complex commercial litigation in forums around the country.

Endnotes

1. *Markert v. Becker Technical Staffing, Inc.*, 2010 WL 1856057 (E.D. Pa. May 7, 2010).
2. *Id.* at *1, *6-*7.
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.* at *7.
7. 949 F. Supp. 2d 748 (N.D. Ohio 2013).
8. *Id.* at 751.
9. *Id.*
10. *Id.*
11. *Id.*
12. *Id.*
13. *Id.* at 755.
14. *Id.* at 756-57.
15. *Id.* at 760-61.
16. *Mintz v. Mark Bartelstein and Assoc. Inc.*, 906 F. Supp. 2d 1017 (C.D. Cal. 2012).
17. *Id.* at 1032-35.
18. *Id.*
19. *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 100-01 (E.D. Pa. 1996).
20. *Stengart v. Loving Care Agency,* 201 N.J. 300, 316 (2010).
21. *Id.* at 307.
22. *Id.* at 307, 325-26.

23. *Id.* at 307.
24. *Id.*
25. *Id.* at 308, 321.
26. *Pure Power Boot Camp v. Warrior Fitness Boot Camp,* 587 F. Supp. 2d 548, 551-52 (S.D.N.Y. 2008).
27. *Id.* at 552.
28. *Id.*
29. *Id.*
30. *Id.*
31. *Id.* at 552-53.
32. *Id.* at 561.
33. *Id.* at 561-62.
34. *Curto v. Medical World Commc'ns, Inc.*, 99 Fair Empl. Prac. Cas. (BNA) 298, 2006 WL 1318387, at *1 (E.D.N.Y. May 15, 2006).
35. *Id.*
36. *Id.*
37. *Id.* at *8-*9.
38. *Pietrylo v. Hillston Rest. Grp.*, 2009 WL 3128420 (D.N.J. Sept. 25, 2009).
39. *Id.*
40. *Id.*
41. *Id.*
42. *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 662-63 (D.N.J. 2012).
43. *Id.*
44. *Id.*
45. *Id.* at 669-671.