

Employee Rights and Social Media

by Lynn D. Feiger and Stephen E. Kapnik

As the use of social media increases, so does its perceived importance to employers as a source of information about their employees. This article addresses legal remedies available to employees to protect their privacy and private information posted online and in social media.

According to a recent survey by the Pew Research Center, nearly half of all adult Internet users in the United States use Facebook and other social networking sites; vast numbers use them every day.¹ No doubt their lawyers (when consulted) advise them never to post—or at least to be mindful when posting—very personal (or compromising) information and (never) photographs, and never to use their employers' computers or network systems to post (or even e-mail) negative information about work. Nevertheless, employees often do post personal and sometimes professionally sensitive information on Facebook and similar sites. Despite employees' unrealistic expectations of privacy, their employers have gained or may gain access to this information and may use it against the employees.

Once employees provide passwords to company e-mail accounts, networks, and company social media accounts (such as LinkedIn) to their employers, they generally should expect their employers to have full and open access to all such communications and posts, and harbor no expectations of privacy. More difficult questions arise when employers intercept private posts from off-premises computers or from private accounts accessed from company computers. Using advanced software or sometimes more nefarious means, employers may obtain access to password-protected employee and applicant blogs and social media posts. Once in litigation, employers also may access that information in discovery directed either to the employee or to the website or social media site itself.

Employees are not without protection. This article provides an overview of legal remedies and protections available to employees to insulate themselves from private employers' abuses of information obtained from social media sites. The article does not address the growing protections available to government employees in this

regard. New doctrines and federal statutes provide some significant legal remedies. The three most important sources of protection for Colorado employees in the private sector are the Federal Stored Communications Act, the Colorado Lawful Activities Statute (CRS § 24-34-402.5), and the right to privacy tort.

Stored Communications Act

Since 1986, the Electronic Communications Privacy Act (ECPA) has restricted certain kinds of access to data communicated through computer systems. Title II of the ECPA, commonly referred to as the Stored Communications Act (SCA),² prohibits unauthorized access to remote computing operations and stored electronic communications. Congress intended through the SCA to protect individual privacy.³

The SCA limits compelled disclosure of subscriber information held by Internet service providers (ISPs).⁴ In general, the SCA delineates how third parties may obtain authorized access to ISPs and criminalizes unlawful access.⁵ The SCA does not apply to information stored on personal computers that are not tied to large electronic storage systems.⁶

Significantly, the SCA also provides the subscriber/employee ("or other person aggrieved") a private right of action for an employer's knowing or intentional unauthorized access to social media sites or personal e-mail accounts.⁷ The employee can obtain both equitable or declaratory relief and damages (with a statutory-imposed floor of \$1,000), plus attorney fees and costs.⁸ Punitive damages are recoverable for willful or intentional conduct.⁹ The SCA's statute of limitations is two years after the date when the employee first discovered or had a reasonable opportunity to have discovered the violation.¹⁰

Coordinating Editor

John M. Husband, Denver, of
Holland & Hart LLP—(303)
295-8228, jhusband@
hollandhart.com



About the Authors

Lynn D. Feiger is a shareholder of Lohf Shaiman Jacobs Hyman & Feiger PC. Her practice focuses on plaintiffs' employment law—(303) 753-9000, lfeiger@lohfsheiman.com. Stephen E. Kapnik is a shareholder of Lohf Shaiman Jacobs Hyman & Feiger PC. His practice focuses on civil litigation—(303) 753-9000, skapnik@lohfsheiman.com.

Labor and Employment Law articles are sponsored by the CBA Labor and Employment Law Section to present current issues and topics of interest to attorneys, judges, and legal and judicial administrators on all aspects of labor and employment law in Colorado.

Coerced Access

Employers cannot compel employees to allow management access to private employee-only chat groups or boards. In *Pietrylo v. Hillstone Rest. Group*, the employer coerced employees to allow managers access to an invitation-only private employees' chat group on MySpace.com. The jury awarded statutory damages, compensatory damages, and punitive damages.¹¹

SCA cases often center on what conduct constitutes "coercion." For example, in *Konop v. Hawaiian Airlines, Inc.*, the Ninth Circuit held that a management-friendly "non-user" cannot validly authorize management to access an employee-only message board.¹²

Access Through Information on Employer-Owned Hardware

The SCA prohibits an employer's unauthorized access to personal sites (such as Gmail) gained through mining passwords and similar private information, even when such information is found on employer-owned devices. Mere ownership of the hardware does not authorize the employer to access protected personal information, such as e-mails in private e-mail accounts, by using passwords stored on the hardware.¹³ The SCA prohibits the unauthorized access, irrespective of the use or abuse of any particular technological means to obtain it.¹⁴

SCA Damages and Violations

The SCA explicitly provides for actual, statutory, and punitive damages. Courts have reached varying results in applying these provisions.

Actual Damages

Courts are split over whether an employee must prove actual damages to be entitled to recover \$1,000 in statutory damages. In *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp*, the U.S. District Court for the Southern District of New York held that courts can award SCA statutory damages even without a showing of actual damages.¹⁵ In *Van Alstyne v. Elec. Scriptorium, Ltd.*, on the other hand, the Fourth Circuit explicitly required a showing of actual damages.¹⁶

Statutory Damages

SCA cases also consider what constitutes separate "violations" of the act because each violation results in a \$1,000 award. Generally, multiple intrusions in close succession may constitute a single violation, whereas intrusions separated by longer periods of time or accessing different accounts may be considered separate violations invoking separate statutory damage awards.¹⁷ In *Pure Power Boot Camp*, the court determined that even though the employer had accessed 546 electronic communications over a period of nine days, it committed only four violations (one for each e-mail system accessed) and thus awarded the plaintiff \$4,000.¹⁸

Punitive Damages

Other than some privacy protections and the fee-shifting provision, the biggest advantage the SCA provides employees is punitive damages for willful or intentional violations. However, few reported cases discuss this aspect of the SCA.

In *Pietrylo*, the court affirmed a jury determination that an employer's repeated access to an employee message board by coerced employee "authorizations" justified imposition of punitive damages. By stipulation, the punitive damages were limited to four times the compensatory damages.¹⁹

One court has directly addressed the willfulness requirement. The Ninth Circuit in *Wyatt Tech. Corp. v. Smithson* agreed with the district court that the employer's repeated and intentional hacking of a private e-mail account, in knowing violation of the SCA, to perpetrate acts of unfair business competition, was "reprehensible" and supported the district court's finding that such actions satisfied the willfulness prong of the statute. However, the court reversed the \$100,000 punitive damages award in *Smithson* for a reason familiar to Colorado lawyers: the district court had awarded punitive damages without awarding compensatory damages. The Ninth Circuit held that punitive damages could not be awarded without compensatory damages.²⁰

Although the Ninth Circuit is not alone in this view, the Fourth Circuit in *Van Alstyne* held that punitive damages can be awarded without proof of any actual damage. The court reached this conclusion based solely on the statutory language, which imposes punitive damages for "willful or intentional" conduct.²¹

Pure Power Boot Camp, like *Wyatt Tech*, focused on the employer's lack of knowledge regarding the SCA.²² Finding that the employer simply was ignorant of the SCA when it read the employee's e-mails, the court refused to characterize the employer's conduct as malicious. Further, the employer's liability was based not on electronically accessing the accounts, but rather only on reading the e-mails after another employee printed them and brought them to the employer.²³ Perhaps understandable as a case at the dawn of the information age, the *Pure Power Boot Camp* holding is troubling to attorneys representing employees because it appears to excuse continuing violations of an employee's rights.

Colorado's Lawful Activities Statute

The Colorado Lawful Activities Act, commonly known as the "Smoker's Rights Statute," is another means of protecting employees' private information. This law provides broad coverage to employees' lawful activities off the premises of the employer during nonworking hours.²⁴ An employer cannot terminate the employment of "employees who engage in activities that are personally distasteful to their employer, but which activities are legal and unrelated to an employee's job duties."²⁵ However, the statute provides no protection for less extreme adverse employment actions, such as demotion or imposing new working conditions.

Under the statute, a wrongfully terminated employee may recover "wages and benefits that would have been due him or her up to and including the date of the judgment had the discriminatory or unfair employment practice not occurred."²⁶ The statute also provides mandatory court costs and reasonable attorney fees for prevailing employees.²⁷

Use of social media networks fits squarely into the protection afforded by this statute. It nonetheless is prudent for employees to cleanse social networking profiles of comments and pictures that their employer might find distasteful, even though the Colorado Lawful Activity Act provides protection to an employee against termination for those legal activities.

Employers have successfully argued that "lawful" conduct excludes more than acts of a criminal nature. In *Marsh v. Delta Air*

Lines, Inc., the employer successfully argued that an employee's duty of loyalty also circumscribes the protected conduct.²⁸ The district court held that the implied duty of loyalty is a "*bona fide* occupational requirement" under § 402.5(1)(a) that limits the employee's right to make negative public comments about the employer.²⁹ Public comments on blogs, social media sites, and websites are no less public than the letter to the newspaper editor Marsh's employer used to justify his termination for breach of the implied duty of loyalty.³⁰

Employees should assume that their employers will gain access to their personal, "private" off-duty information and conduct "publicly" posted on social media, and recognize the ways in which they are protected. Although the Smoker's Rights Statute provides no protection for unlawful or publicly disloyal communications, it does protect the employee from termination for communicating lawful comments and pictures.

Invasion of Privacy

Quite apart from statutory protections, Colorado employees enjoy the right to privacy. Colorado first recognized the common law tort of invasion of privacy in the context of debt collection practices.³¹ In *Doe v. High-Tech Inst., Inc.*, Colorado further extended the privacy right to "intrusions into a person's private concerns"—such as results of an HIV test—"based upon a reasonable expectation of privacy in that area."³²

One limiting factor in proving the tort is the employee's showing a "reasonable expectation of privacy."³³ Although no Colorado case has applied the privacy tort in the social media context, the employee's protection—that is, expectation of privacy—should be in proportion to the care the employee takes to maintain the privacy of and restrict access to the online information.

An employer cannot eliminate its employees' right to privacy by purporting to negate the right in an ostensibly neutral electronic policy that allows the employer access to information, such as e-mail, stored on a company computer. *Stengart v. Loving Care Agency, Inc.*, a New Jersey case, discusses the limits on an employer's power to retrieve electronic information stored on employer-owned devices.³⁴ *Stengart* found that employees have a reasonable expectation of privacy in, and therefore barred an employer from accessing, employees' personal e-mail account communications with counsel, even if available on or from an employer-owned laptop.³⁵ The employer was barred from accessing the information even though it had a company electronic communications policy that permitted the employer to review, audit, intercept, and access anything stored on company media systems, and which specifically stated that such voicemail, Internet use and communications, and computer files were considered part of the company's business and client records.³⁶

To prove the tort of invasion of privacy in Colorado, the employee must show that a reasonable person would find the employer's intentional intrusion on the employee's "seclusion or solitude" offensive or objectionable.³⁷ The more publicly accessible the social media information is, the less privacy employees can reasonably expect. Because the test is objective, the employee's understanding of the public nature of social networking sites does not alone define the expectation of privacy. An employee would have a greater expectation of privacy on a site where the public cannot find a private profile or see information other than a general blog or comment post on a publicly accessible website.

The U.S. Supreme Court recently discussed the contours of such privacy expectations in the context of the Fourth Amendment.³⁸ The Court held that employers' "clearly communicated" policies can "shape the reasonable expectations of their employees."³⁹ Employees must be aware of their workplace policies and that such policies may affect the reasonableness of their expectation of privacy in social media posts.

In no reported decision has a Colorado employee successfully upheld the privacy right in online information against the employer's invasion. Few other states have published cases and none has found violations. In *Pietrylo*, for example, the jury found against the plaintiffs on their invasion of privacy claims.⁴⁰

At least one court has held that a person has no reasonable expectation of privacy for information publicly posted on a social networking site. In *Moreno v. Hanford Sentinel, Inc.*, a California appeals court held that no information on the plaintiff's Myspace posting was private because "anyone with Internet access" could read it.⁴¹ The lesson here is that the more an employee acts to restrict access to posted information, the greater the expectation of privacy. Even the *Moreno* court held that information disclosed to only "a few people may remain private."⁴²

Mandated Disclosures and Discovery

Increasingly, disclosure of social media is requested directly from social media companies and in formal discovery in litigation.⁴³ The threshold of relevance frequently is met in employment litigation by employers seeking information relevant to

claims or issues of sexual harassment, breach of fiduciary duty, or emotional distress.

Subpoenas

Employers may obtain employee information by serving subpoenas on social networking sites. Because an individual has "a personal right in information in his or her profile and inbox" in the same way that an individual "has a personal right in employment and bank records," the employee may contest the subpoena through a motion to quash.⁴⁴

The ECPA gives protection to social media companies that comply with subpoenas requesting personal information, providing that:

No cause of action shall lie in any court against any provider of wire or electronic communication service . . . for providing information, facilities, or assistance in accordance with the terms of a . . . subpoena . . . under this chapter.⁴⁵

However, courts have refused to interpret this provision as permitting or applying to civil subpoenas.⁴⁶ Accordingly, some social media sites will produce only "public" information, and refuse to produce private communications.⁴⁷

Other Discovery

Courts have not protected employees' private information on social media sites when the employees' emotional or physical well-being is at issue.⁴⁸ Although courts have been more reluctant to permit discovery of private e-mails than social media profiles, sev-

eral courts, including the U.S. District Court for the District of Colorado, have allowed discovery of social media if the requesting party can show that the information is relevant and at issue.

EEOC v. Simply Storage Mgmt., LLC provides a useful guide to how courts may view the discovery of information stored on social networking sites.⁴⁹ The employer in that case sought the employees' social network site profiles, arguing that they might be relevant to emotional distress claims of sexual harassment plaintiffs. Rejecting the employees' assertion that "locking" or privately posting information on a social media site shields it from discovery, the court held that such information must be produced if relevant to a claim or defense.⁵⁰ The court limited production of social media site information (including photographs) to the employees' first-party communications that

reveal, refer, or relate to any emotion, feeling, or mental state, as well as communications that reveal, refer, or relate to events that could reasonably be expected to produce a significant emotion, feeling or mental state, and third-party communications that placed the employee's own communications in context.⁵¹

Conclusion

Employers may be able to obtain even privately designated information from employee social network site profiles and posts. Nevertheless, employees should be aware that they have specific legal rights that limit their employers' access to—and use of—private information and material.

Notes

1. Pew Internet & American Life Project, "Adults and social networks," available at pewinternet.org/Reports/2010/Social-Media-and-Young-Adults/Part-3/2-Adults-and-social-networks.aspx?r=1.
2. Stored Wire and Electronic Communications and Transactional Records Access Act, codified at 18 USC §§ 2701 to 2712.
3. *United States v. Councilman*, 418 F.3d 67, 80-81 (1st Cir. 2005).
4. 18 USC § 2701 bars unauthorized access to an Internet service provider's stored wire or electronic communications and transactional records.
5. 18 USC §§ 2701 to 2703.
6. *See* 18 USC § 2701.
7. 18 USC § 2707.
8. 18 USC § 2707(b) and (c).
9. 18 USC § 2707(c).
10. 18 USC § 2707(f).
11. *Pietrylo v. Hillstone Rest. Group*, No. 06-5754, 2009 WL 3128420 (D.N.J. Sept. 25, 2009).
12. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 880 (9th Cir. 2002).
13. *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 759 F.Supp.2d 417, 420-24 (S.D.N.Y. 2010).
14. *Doe v. City and County of San Francisco*, C10-04700, 2012 WL 2132398 (N.D.Cal. June 12, 2012).
15. *Pure Power Boot Camp, Inc.*, *supra* note 13 at 428 ("Defendants are accordingly entitled to the statutory minimum of \$1,000 per violation of the statute, whether or not they have suffered actual damages.").
16. *Van Alstyne v. Elec. Scriptorium, Ltd.*, 560 F.3d 199, 208 (4th Cir. 2009) ("A 'straightforward textual analysis' leads us to conclude that the district court erred in permitting the jury to award Van Alstyne statutory damages without requiring her to prove that she sustained actual damages.").
17. *See In re Hawaiian Airlines, Inc.*, 355 B.R. 225, 232 (D.Haw. 2006).
18. *Power Boot Camp, Inc.*, *supra* note 13 at 428-29.
19. *Pietrylo*, *supra* note 11.
20. *Wyatt Tech. Corp. v. Smithson*, 345 F.App'x 236, 239 (9th Cir. 2009).
21. *Van Alstyne*, *supra* note 16 at 209.
22. *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 08 CIV. 813 F.Supp.2d 489, 554-56 (S.D.N.Y. Sept. 2011).
23. *Id.*
24. CRS § 24-34-402.5.
25. *Marsh v. Delta Air Lines, Inc.*, 952 F.Supp. 1458, 1462 (D.Colo. 1997).
26. CRS § 24-34-402.5(2)(a).
27. CRS § 24-34-402.5(b)(I).
28. *Marsh*, *supra* note 25 at 1463.
29. *Id.*
30. *See id.* at 1460-62.
31. *Rugg v. McCarty*, 471 P.2d 753, 755 (Colo. 1970).
32. *Doe v. High-Tech Inst., Inc.*, 972 P.2d 1060, 1068 (Colo.App. 1998).
33. *Id.*
34. *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650, 660-64 (N.J. 2010).
35. *Id.* at 655. *But see Aventa Learning, Inc. v. K12, Inc.*, 830 F.Supp.2d 1083, 1109-10 (N.D.Wash. 2011).
36. *Stengart*, *supra* note 34 at 655.
37. *High-Tech Inst., Inc.*, *supra* note 32 at 1067.
38. *City of Ontario, Cal. v. Quon*, 130 S.Ct. 2619, 2629-30 (2010).
39. *Id.* at 2630.
40. *Pietrylo*, *supra* note 11.
41. *Moreno v. Hanford Sentinel, Inc.*, 172 Cal.App.4th 1125, 1128 (2009).
42. *Id.* at 1130.
43. *See* Mix, "Discovery of Social Media," 40 *The Colorado Lawyer* 27 (June 2011), available at www.cobar.org/tcl/tcl_articles.cfm?articleid=7058.
44. *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965, 974 (C.D.Cal. 2010).
45. 18 USC § 2703(e).
46. *Crispin*, *supra* note 44 at 974-76.
47. *See, e.g., Mackelprang v. Fid. Nat'l Title Agency of Nevada, Inc.*, No. 2:06-cv-00788, 2007 WL 119149 (D.Nev. Jan. 9, 2007).
48. *See Ledbetter v. Wal-Mart Stores, Inc.*, No. 06-cv-01958, 2009 WL 1067018 (D.Colo. April 21, 2009). *See also Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650 (Sup.Ct. 2010).
49. *EEOC v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430, 434 (S.D. Ind. 2010).
50. *Id.* at 437.
51. *Id.* at 436. ■