American Bar Association • Section of Labor & Employment Law
National Symposium on Technology in Labor and Employment Law
Cyber Crimes and the Workplace
April 25 – 27, 2012

Turning the Tables on Workplace Cyber Misconduct

by Lauren E. Schwartzreich, Esq.

Employers and their counsel are keenly aware that technology-based workplace misconduct can wreak havoc on a business, damaging computer systems, straining reputations and providing competitors with an unfair advantage. Though damaging cyber-attacks by external third parties make for exciting newspaper headlines, they comprise only a portion of the technology dangers companies regularly manage. The very people who are paid to use and safeguard business property, data, and information may place the organization at an even greater risk of harm. As a result, many employers regulate and/or monitor employees' technology use. Even with effective and consistent monitoring and enforcement, damaging workplace misconduct may still occur.

Employers can mitigate the impact of workplace misconduct by understanding the various, and often interconnected legal issues that flow from work-related and non-work-related technology use. First, employers should be aware of the myriad ways in which employees may compromise employers' computer systems and data. Employers should also take note of potential civil claims that can be brought against former employees for misuse of company electronic systems and data. Finally, employers should appreciate how effective internal investigations can reveal evidentiary proof of an employee's misconduct. At the same time, however, misguided investigations can create liability for employers. By leveraging this knowledge, as well as the technical skills of computer experts and the legal knowledge of experienced counsel, employers may be able to turn the tables on workplace misconduct.

A. EMPLOYEES MAY LEVERAGE EMERGING TECHNOLOGIES TO COMMIT CYBER CRIMES

Employees who engage in technology-based misconduct often do so in seemingly innovative ways. As technology makes it easier to use, manipulate, access and move data, whether within enterprise systems or via personal electronic devices, employees who are intent on taking employer data will find it increasingly easy to do so. A few recent cases, discussed below, evidence emerging trends in workplace technology-based misconduct.

1. Breach of Restrictive Covenant Agreements via Social Media

Emerging technologies, including social media, have breathed new life into restrictive covenant violations. Departing employees with non-compete or non-solicitation agreements may attempt to

Littler Mendelson, P.C. • 900 Third Avenue • New York, NY 10022 • Tel: 212.583.9600 • Fax: 212.832.2719

work around the letter of such agreements by leveraging personal social media accounts to communicate with the prohibited audience. For example, in *Enhanced Network Solutions Group v. Hypersonic Technologies Corp.*,[1] a defendant subcontractor, who was bound to a non-solicitation agreement with the plaintiff company, posted a position description to its LinkedIn profile. The profile was viewable only to persons within a certain public LinkedIn group. One of the plaintiff's employees saw the posting and contacted the defendant for a position, and employment soon followed — as did a lawsuit for violation of the non-solicitation agreement. The court found that the defendant subcontractor did not violate the agreement by posting the position to its publicly available LinkedIn portal, and that the employee applicant had solicited employment from the defendant, not the reverse.[2] In situations like this, it is easy to see how social media tools can frustrate an employer's goal of protecting client relationships and current employees. By revising restrictive covenant agreements to account for new technologies, such as social media, employers may be able to safeguard these interests.

2. Moving Data to Competitor via Cloud Storage

Emerging technologies provide additional tools that enable an employee to move proprietary or confidential information to a future employer. An employee may set up a free cloud storage account to upload data from one employer and then download it to another. In fact some cloud tools now automatically push data from one device to others. In early 2012, a law firm sued a former partner who moved to a new firm, allegedly taking numerous files with him. The firm alleged that the partner and other defendants, among other things, uploaded files from the former firm's computer system onto a free cloud repository, Dropbox, before they departed the firm. After their departure, they continued to access — and transfer — their former firm's files.[3] Before the proliferation of free cloud storage, an enterprising former employee would have had to physically access a former employer's computer, raising the risk, and odds, of getting caught. As a result, employers must be prepared to address cloud-based misconduct by implementing effective computer use policies and securing electronic systems against unauthorized cloud access.

3. Taking Over a Social Media Persona

Employers also risk an employee absconding with the employer's social media presence, which — for some employers — may be a primary source of income. One employer recently faced such a situation and filed suit against a former employee for theft of trade secrets and interference with economic advantage. In that case, *PhoneDog v. Kravitz*,[4] the former employee had served as the voice for the employer's Twitter account. The employee left the company, taking with him the password to the Twitter account and subsequently changing the account's name to his own. He continued to post messages using the Twitter account, and these messages were read by the Twitter following that had been built during his period of employment with PhoneDog. Defending its Complaint from a motion to dismiss, the employer argued that the Twitter account's password and followers were trade secrets. The company also argued that the former employee damaged its economic relationship with Twitter advertisers when he took control of and redirected the account, thereby decreasing the traffic to the employer's website and to its advertisers' content. Although the district court denied the motion to dismiss, the outcome of the case is far from settled. Some question the viability of the trade secret claim in the context of a Twitter account. Regardless of the outcome in this case, other cases involving dispute of ownership over social media accounts continue to emerge.[5] These cases highlight the distressing reality that employers must act vigilantly to protect their own social media accounts from employees before, during and after employment.

B. EMPLOYERS' LEGAL RECOURSE FOR EMPLOYEE TECHNOLOGY-BASED MISCONDUCT

When an employee engages in misconduct involving a computer or other electronic device, the employer may have various courses of action to consider. Where a current employee is involved, the first appropriate step may be preservation of evidence revealing the misconduct. Implementing an IT solution to stop the action, or to reduce the hemorrhaging borne out by the misconduct, should also be a

1 2011 WL 2582870 (Ind. Ct. App. June 30, 2011).

2 In a footnote, the court explained that the non-solicitation agreement could have been drafted to prevent the defendant from considering applications, regardless of who initiated contact.

3 *See Elliot Greenleaf & Siedzikowski v. Balaban, et al.*, 2:12-CV-00674 (E.D. Pa. Feb. 18, 2012).

4 No. C 11-03474 MEJ (N.D. Cal. Jan. 30 2012).

5 *See e.g., Eagle v. Morgan*, No. 2:11-cv-04303 (RB) (E.D. Pa., Dec. 22, 2011) (denying motion to dismiss claims for conversion and unfair competition, but granting motion to dismiss claim for misappropriation of trade secret where former employee regained control of LinkedIn account that had been created at employer's instruction, via employer's email account and with employer's profile template); *Ardis Health, LLC, et al v. Nankivell*, No. 1:11-cv-05013 (NRB) (S.D.N.Y., Oct. 19, 2011) (granting preliminary injunction upon claim of conversion where former employee retained access to employer's various website and social media accounts).

priority. However, once the employer has done everything under its power to ameliorate the situation, the employer should consider a few potential avenues of civil recourse.

A few federal technology-related criminal laws, and their state counterparts, provide a civil cause of action against individuals who access others' technology systems or data without valid authorization. Such laws may provide employers with an opportunity to recover damages against employees who engage in severe technology-based misconduct. The method by which an employee engaged in harmful technology-based conduct, such as by recording others' electronic conversations or accessing a computer system in excess of prior authorization, may determine whether one of these laws would apply. A few relevant federal criminal laws providing civil causes of action for victims include the Computer Fraud and Abuse Act[6] ("CFAA"), the Stored Communications Act ("SCA"),[7] and the Wiretap Act[8]. Each of these is discussed below.

1. Employees' Unauthorized Access to Computer Systems

Any employee may violate the CFAA where she exceeds her access to data and takes it to a competing business. Employers may turn to the CFAA for civil[9] recovery where an employee accesses the employer's computer system without authorization (or by exceeding authorization) in furtherance of a fraud and obtains something of value.[10] An employer who suspects a CFAA violation will need to conduct a thorough and defensible investigation of not only the employee's actions, her intent, and the value of data obtained, but the employer must also assess the amount of monetary loss suffered as a result of the employee's actions. The CFAA requires a threshold demonstration of loss incurred, in the amount of $5,000 or more.[11]

After fully vetting and investigating potential CFAA claims, employers should carefully consider two consistent hurdles to bringing such claims against employees. Many CFAA cases involving misconduct by an employee turn on one of two issues: (a) whether the employer has demonstrated adequate loss and (b) whether an employee "exceeds authorization" by acting contrary to the employer's interests or in violation of the employer's policies.

As for the "loss" element, loss flowing from misuse of confidential or proprietary information generally will not satisfy the threshold amount. Some courts have held that loss must be related to computer impairment or computer damages.[12] In a uniquely plead case, one court recently ruled that loss of employee productivity time in hours spent surfing the Web and using Facebook would not satisfy this requirement.[13] In lieu of focusing on such soft costs, employers may want to quantify their loss in terms of resources expended investigating harm caused by the unauthorized access, recreating the lost data, and replacing electronic devices under investigation, among other things.[14]

6 18 U.S.C. § 1030.

7 18 U.S.C. §§2701-1.

8 18 U.S.C. §§ 2510-2522.

9 The CFAA states that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

10 18 U.S.C. § 1030(a)(4) (it is a violation of the Act when a person "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value.") The intent to defraud is not required under all provisions of the CFAA. For example, §1030(a)(2)(C), makes it a crime to exceed authorized access of a computer connected to the Internet *without* any culpable intent.

11 18 U.S.C. §§ 1030(a)(2), (a)(4).

12 *See Oil States Skagit Smatco, LLC v. Dupre*, No. 09-4508, 2010 WL 2605748, at *2-3 (E.D. La. June 21, 2010) (dismissing CFAA claim, because plaintiffs did not establish "loss" where economic losses were caused by misappropriation of proprietary information rather than interruption of service, and data restoration costs did not meet jurisdictional threshold).

13 *Lee v. PMSI*, 8:10 cv 2904 T 23TBM (M.D. Fla May 6, 2011)(lack of productivity due to excessive internet usage to visit personal websites was not "loss" under the statute).

14 *See* Harry W. Wellford, Missouri Court Paves the Way for Federal Jurisdiction for Claims of Misappropriation of Electronic Information by Departing Employees (June 2, 2009) (http://www.littler.com/publication-press/publication/missouri-court-paves-way-federal-jurisdiction-claims-misappropriation-) (discussing effective reliance on" the cost of computer forensic expert fees and the delay in return of company property, such as laptop computers, in addition to any loss caused by the actual misuse of information.")

For the "exceeds authorization" issue, some courts have found that acting disloyally or in violation of an employer's computer use policy places the employee beyond the bounds of valid authorization.[15] Other courts have rejected this contention.[16] Most recently, in April 2012, the Ninth Circuit issued an opinion, *en banc*, joining the latter group of circuits.

In *U.S. v. Nosal*,[17] an employee was criminally charged under the CFAA for, among other things, having colleagues download confidential database information from the employer's computer system and transfer the data to him to start a competing business. The employees had authorization to access the database, but the employer maintained a policy that prohibited disclosing confidential information. The government contended that someone with unrestricted physical access to a computer system may be limited in the ways in which he can *use* computer data and may therefore exceed authorization by misusing the data. In Nosal's case, the government argued that he violated the CFAA by exceeding any authorization he may have had to access the database when he *used* the information in violation of company policy.[18] The court rejected this reading of the CFAA, opting instead to narrowly construe the criminal statute to cover only breaches of access, not mis*use* of data.[19]

The court's ruling emphasized several public policy considerations involving the employment and consumer context. According to the court, employer-employee and company-consumer relationships are traditionally covered by tort and contract law and a broader reading of the CFAA, as espoused by the government, "allows private parties to manipulate their computer use and personnel policies to turn these relationships into ones policed by the criminal law."[20] The court cautioned that, under the government's reading of the statute, "millions of unsuspecting individuals would find that they are engaging in criminal conduct."[21]

These public policy considerations should not be lost on employers, as employers may benefit from their protections. The *Nosal* ruling may save some employers from liability under the CFAA. For example, the court's ruling could impact employers who request social media login information from prospective or current employees. As the court noted in *Nosal*, social media sites maintain user policies that limit the terms of service,[22] such as use of passwords and content. Further, "website owners retain the right to change the terms [of service] at any time and without notice."[23] Had the Ninth Circuit ruled that improper use (as defined by the entity implementing the usage policy) triggered unauthorized access under the CFAA, employers might find themselves unintentionally satisfying a critical element of the criminal statute. With social media sites, like Facebook, publicizing their intent to pursue claims against employers who violate the site's terms of use,[24] decisions like *Nosal* might reduce Facebook's chance of successfully pursuing CFAA claims against employers who request applicants'

15 *See, e.g., U.S. v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding that SSA employee exceeded his authorized access under the CFAA when he obtained personal information about former girlfriends and potential paramours and used that information to send flowers or to show up at women's homes.); *United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010) (upholding criminal conviction under CFAA where former employee intended fraudulent use of employer's computer thereby exceeding authorization under the employer's policy, and explaining that "[an employer may 'authorize' employees to utilize computers for any lawful purpose but not for unlawful purposes and only in furtherance of the employer's business"); *U.S. v. Salum*, 257 Fed. Appx. 225, 230-31 (11th Cir.2007) ("[A]lthough [the defendant] may have had authority to access the [computer] database, there was sufficient evidence to establish that ... [the defendant] exceeded his authority by accessing it for improper purpose."); *Int'l Airport Ctrs. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006) (CFAA claims upheld where employee destroyed files on employer's laptop, because authorization to access laptop terminated when employee violated duty of loyalty); *P.C. Yonkers Inc. v. Celebrations The Party and Seasonal Superstore LLC*, 428 F.3d 504, 510 (3d Cir.2005) (CFAA extends to actions against "former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system"); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581 (1st Cir.2001) ("We conclude that because of the broad confidentiality agreement[,] appellants' actions 'exceed[ed] authorized access.'"); *Guest-Tek v. Pullen*, 665 F. Supp. 2d 42, 45-46 (D. Mass. 2009) (CFAA claim upheld against employee who allegedly violated duty of loyalty by copying files and planning a competitive venture while still employed).

16 *See e.g., Sloan Fin. Group, LLC v. Coe*, Slip Copy, 2010 WL 4668341 (D. S.C., November 18, 2010) (rejecting argument that "an employee acts 'without authorization' or 'exceeds authorized access' when he accesses a computer or protected computer with an intent that is contrary to the interests of his employer."); *Océ North Am., Inc. v. MCS Servs., Inc.*, No. WMN- 10-CV-984, 2010 WL 3703277, at *4 (D. Md. Sept.16, 2010) (while employee remained employed, he had authorization to use computers and software and although "copying software onto his own laptop may have been a violation of his employment agreement, [...] that does not constitute a violation of the CFAA"); *Cvent, Inc. v. Eventbrite, Inc.*, No. 1:10-cv-00481, 2010 WL 3732183, at *4 (E.D. Va. Sept.15, 2010) ("a mere allegation that a defendant 'used the information [which it had been given lawful authority to access] in an inappropriate way' did not state a claim for relief [under the CFAA]") (quoting *State Analysis, Inc. v. Amer. Fin. Servs., Assoc.*, 621 F.Supp.2d 309, 317 (E.D. Va.2009)).

17 No. 10-10038, Slip. Op., (9th Cir. April 10, 2012).

18 The CFAA defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

19 *Nosal*, at 3860.

20 *Id*. at 3867.

21 *Id* at 3866.

22 *Id* at 3868 (discussing Google's recent policy change that previously forbade use by minors and Facebook's policy prohibiting users from allowing others to log into their accounts).

23 *Id*. at 3869.

24 *See* Erin Egan, Protecting Your Passwords and Your Privacy, (March 23, 2012) (https://www.facebook.com/notes/facebook-and-privacy/protecting-your-passwords-and-your-privacy/326598317390057) (Statement by Facebook's Chief Privacy Officer expressing alarm at employers' requests for Facebook login information from applicants, explaining that the company "made it a violation of Facebook's Statement of Rights and Responsibilities to share or solicit a Facebook password" and that Facebook will "take action to protect the privacy and security of [its] users, whether by engaging policymakers or, where appropriate, by initiating legal action[.]"

login information.[25] Even so, such civil claims might not be viable due to other reasons, such the threshold $5,000 damages requirement. The decision may also dissuade the government from pursuing *criminal* convictions against employers who request social media login information.[26] As media reports reflect a growing backlash in pre-employment social media screenings, including states adopting laws to prohibit requests for login access,[27] employers should carefully consider their potential liability before requesting login information.[28]

Although the *Nosal* ruling may be the most *recent* circuit court ruling on the role of the CFAA in employment relationships, it is not *controlling* on the majority of other courts that have reached different conclusions.[29] Regardless of whether the U.S. Supreme Court decides to resolve the circuit split involving the CFAA, employers may want to reconsider their social media screening strategies.

2. Employees' Unauthorized Access of Electronic Communications

Where employees access workplace electronic communications without authorization, employers may be able to seek damages under the SCA[30] or the Wiretap Act[31]. Both statutes prohibit unauthorized access to electronic communications and provide civil remedies[32] in addition to criminal penalties. While there is limited case law involving employers seeking civil redress against employees for violating these statutes, employers may look to cases involving criminal enforcement for guidance. In *United States v. Szymuszkiewicz*,[33] the Seventh Circuit upheld the conviction of an employee who created an auto-forward prompt on another employee's email account, such that he would receive copies of all emails received and sent via that email account. The jury found him guilty under the Wiretap Act for intentionally intercepting electronic communications.[34] Interestingly, the employee argued on appeal that he the emails were not "intercepted" as required by the Wiretap Act, but were collected after the communication occurred — a process which, he acknowledged, violated the SCA. Specifically, he contended that the auto-forwarding process did not constitute an "interception" of a communication in transmission (as required under the Wiretap Act). Instead, he attempted to explain, the auto-forwarding was a collection process that occurred after the emails had come to rest on a computer system (thereby triggering the SCA).[35] The appellate court rejected this argument as well as other circuits' interpretation of the Wiretap Act's critical term "interception."[36] These other circuits have interpreted "interception" in such a way as to exclude emails from the Wiretap Act's coverage. As a result, and depending on the circuit, employee liability for unauthorized email access may be found under either the SCA or the Wiretap Act.

Depending on the circumstances of the employee's unauthorized access, an employer may not always have standing to recover under the Wiretap Act, whereas an employer may have a greater chance of establishing standing under the SCA. The Wiretap Act permits civil recovery for "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this

25 Facebook and other services providers could potentially have standing to recover damages. *See* §1030(g) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."); and (e)(12)(defining "person" as "any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity").

26 The Department of Justice has, in fact, prosecuted such violations in the past – though with limited success. *See e.g., U.S. v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) (rejecting DOJ's argument that mother violated 18 U.S.C. 1030(a)(2)(C) by creating a false MySpace account, a violation of MySpace terms of service, to harass a teenage girl).

27 *See* Martha Neil, New Md. Law May Be First in Country Banning Employers From Seeking Workers' Social Media Passwords (Apr 10, 2012) (http://www.abajournal.com/news/article/new_md._bill_may_be_first_in_country_banning_employers_from_seeking_worker_/) (Maryland lawmakers unanimously "enacted a bill that would prohibit employers from demanding personal passwords to social media sites such as Facebook from job applicants and workers.")

28 *See* Chris M. Leh, Though Not Yet Banned, Requiring Social Media Information Is a Bad Idea (March 27, 2012) (http://www.littler.com/publication-press/publication/though-not-yet-banned-requiring-social-media-information-bad-idea) ("In light of the likelihood of new legislation and the internal and public backlash against employers that request or require social media login information, the best practice is simply not to ask unless the employer has a strong and legitimate business reason for doing so."); Senators Question Employer Requests for Facebook Passwords (March 26, 2012) (http://www.nytimes.com/2012/03/26/technology/senators-want-employers-facebook-password-requests-reviewed.html) (discussing senators' call for an inquiry into whether the practice of asking applicants for social media login information violates the Stored Communications Act or the Computer Fraud and Abuse Act); Employers ask job seekers for Facebook passwords (March 20, 2012) (http://online.wsj.com/article/AP35b6fb378cc64062a3bceb87e17e2e03.html). Employers may face liability under other laws for requesting social media login information, including privacy laws, anti-discrimination statutes and the Stored Communications Act. *See* Wendi S. Lazar and Lauren E. Schwartzreich, Limitations to Workplace Privacy: Electronic Investigations and Monitoring, The Computer & Internet Lawyer, at 2 (Jan. 2012).

29 In the following cases, courts have applied the CFAA to violations of corporate computer use restrictions or violations of a duty of loyalty: *U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *U.S. v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006).

30 18 U.S.C. §§2701-11.

31 18 U.S.C. §§ 2510-2522.

32 18 U.S.C. § 2520 (civil damages under Wiretap Act), 18 U.S.C. §2707 (civil damages under SCA).

33 622 F.3d 701 (7th Cir. 2010).

34 See 18 U.S.C. § 2511(1)(a).

35 *Szymuszkiewicz,* 622 F.3d at 703.

36 The court rejected other rulings that said that to violate § 2511 of the Wiretap Act, an interception must be "contemporaneous" with the communication: *Fraser v. Nationwide Mutual Ins. Co*., 352 F.3d 107, 113 (3d Cir.2003); *Steve Jackson Games, Inc. v. Secret Service*, 36 F.3d 457 (5th Cir.1994); *Konop v. Hawaiian Airlines*, Inc., 302 F.3d 868 (9th Cir. 2002); *U.S. v. Steiger*, 318 F.3d 1039 (11th Cir.2003).

chapter[.]"[37] Unless an employer successfully argues that it is a "person" under the Act and that the communication was the *company's* communication, the employer may not have standing to bring suit under the Wiretap Act. However, the SCA's standing provision is a bit broader. It permits civil suit by "any provider of electronic communication service, subscriber, or other person aggrieved[.]"[38] Under this definition, more employers might be permitted to seek civil recovery under the SCA.

The differing standing standards, as well as the varying circuit interpretations of the Wiretap Act's "intercept" requirement, should give employers pause before filing a claim under either statute. First, the employer should gain a clear understanding of the technology used and then research the interpretation adopted by its circuit. The employer should then determine whether it has standing to sue under the appropriate statute. Finally, the employer's Complaint should demonstrate standing and satisfy each element of the corresponding statute.

C. WORKPLACE INVESTIGATIONS AND REDUCING EMPLOYER LIABILITY

An employer can benefit from investigating incidents involving technology and misconduct. For example, the results of an investigation can help an employer improve its cyber security, adjust its technology use policies, identify other responsible employees, and determine whether the law has been violated. Most importantly, investigation results may provide evidence in defense, or prosecution, of a civil action by or against the employee. The electronic data trail left behind by an employee who misused an employer's computer system could reveal enough evidence to prove that the employee engaged in actionable misconduct. The resulting litigation may turn on the reliability of the employer's investigation. However, just as a good investigation can help prove the misconduct, a poor investigation could trigger liability for the employer. Employers and their counsel should adequately vet technology investigations in advance, to prevent mishandled investigations that create new liabilities for the employer.

1. Leveraging Effective Investigations to Prove Misconduct

Effective workplace investigations will maintain the integrity of relevant data. Particularly in theft of trade secret litigation, employers may need targeted forensic collection and/or review of data. An employer's internal IT personnel may not be qualified or experienced in conducting effective investigations that not only uncover the truth about what happened to the data at issue, but that also protect and preserve the data for use in litigation.

An employer may be able to collect and preserve critical evidence of misconduct by investigating a suspect-employee's computer and portable devices. Just as an employer must prepare to conduct an effective investigation that maintains the integrity of its data, it should pursue a high-quality investigation of a suspected employee's devices. Forensic analysis of an employer's computer system or the employee's workplace electronic device may reveal that the employee improperly accessed those devices. Following the trail of data, employers may find that the last known access point to the data was an employee's mobile electronic storage device, online email account or other data repository. Where the data trail ends with a litigant-employee, the employer may benefit from forensic discovery of the employee's electronic devices.

Forensic review of a competing employee's devices, and the devices of its new employer, may provide critical evidence for a theft of trade secrets case. For example, in *Weatherford U.S., L.P. v. Innis, at al.*,[39] an employer filed a motion to compel production of all computers used by a competitor who recently hired a former employee. The employee allegedly saved files from the company's computer system onto a separate drive before leaving for the competitor. The competitor returned the drive to the former employer, who, upon forensic review, determined that the drive had been accessed by other devices and that the files on the device could have been copied.[40] The former employer propounded discovery requests seeking production of all computers used by the new employer, as well as portable storage devices that had been connected to these computers,. In its motion, the former employer sought to have its own forensic expert image the drives, at the former employer's expense (while providing the new employer an opportunity to pre-screen the images for any confidential documents). The court granted the request, explaining that "[i]t is not unusual" for courts to allow mirror imaging of hard drives "that contain documents responsive to an opposing party's request for production … particularly in cases where trade secrets and electronic evidence are both involved."[41] The court recognized that courts have been cautious where a request is "extremely broad" and "the connection between the

37 18 U.S.C. § 2520.

38 18 U.S.C. §2707

39 No. 4:09-cv-061, 2011 WL 2174045 (D. N.D. June 2, 2011)

40 *Id*. at *2.

41 *Id*. at *4.

computers and the claim in the lawsuit are unduly vague or unsubstantiated in nature[.]" However, it reasoned that the former employer's claims were "neither vague nor unsubstantiated"[42] because the employee admitted he downloaded the files onto a separate drive without permission, thus "provid[ing] a nexus between [the former employer's] claims and its need for images of [the] computers."[43] The court also noted that the former employer's review of the drive contradicted the former employee's claims that he had not accessed the drive. Where, as here, an employer lays a proper foundation for its argument that an employee has possession, custody or control over proprietary data and has refused to allow its electronic devices to be examined, the employer may be able to drive the search process in an effective and efficient way. In situations like this, forensic analysis may provide the basis for a broad motion to compel.

To fully appreciate the benefits of forensic collection, employers may need to reconsider the scope of their own internal IT investigations. Internal IT personnel may not be trained or equipped to conduct internal investigations. Their investigations may overwrite evidentiary data, including critical metadata. As a result, the resulting investigatory data may be inaccurate and ultimately inadmissible.

Although forensic collection and analysis can be extremely effective,[44] not all employee misdeeds necessitate forensics work. Some employers may be able to resolve disputes involving misappropriated data through negotiations with the employee or the employee's counsel, without triggering the need for forensic preservation. Because forensic collection and review may be costly in some circumstances, employers would be wise to contact their employment counsel and e-discovery counsel for advice and cost-saving strategies.

2. Internal Investigations Can Result in Employer Liability

While technology investigations may reveal smoking-gun evidence of an employee's misconduct, counsel should first vet investigations, as they may create liability for the employer. A few cases highlighting this point involve employer liability under the SCA.[45] The first, *Van Alstyne,*[46] involves a former employee who sued her employer for discrimination and, as a result of the employer's investigation of her laptop computer, for violating the SCA as well. After the employee claimed harassment and was separated from employment, her employer examined her work laptop computer and thereby obtained login information for her password-protected personal Web-based email account. Thereafter, the employer repeatedly accessed her personal email account and read her correspondence with her attorney. These actions were found to violate the SCA.[47] Similarly, in *Pure Power Boot Camp*, an employer investigated a former employee's desktop computer and discovered that the employee's personal online email account login information was saved on the computer and automatically populated in the Internet browser window.[48] The employer used the auto-populated information and accessed the former employee's online email accounts. Even though the employer maintained a computer use policy that, it argued, gave the employee no expectation of privacy, the act of accessing the employee's personal email account violated the SCA.[49] In each of these situations, the employer started with an investigation of the employee's computer and ended with SCA liability. Had each employer sought the underlying evidence in discovery, it might have avoided SCA liability.

Employers' liability under the SCA may also extend to investigation of employees' social media accounts. In *Pietrylo v. Hillstone Restaurant Group*,[50] a district court upheld a jury verdict and punitive damages against an employer for violating the SCA. The employer violated the Act by accessing, without authorization, a group of employees' password-protected and invite-only online forum maintained by a group of employees. The plaintiff-employees created the restricted-access discussion forum, located on MySpace, so that they and other invited employees could air grievances concerning their employment. Upon request from a manager, a participant in the discussion turned over her login information.[51] The manager subsequently accessed the forum, reviewed the content and fired the plaintiffs. The district court concluded that a reasonable jury could find that the managers knew their access was unauthorized, and that the employee who provided

42 *Id*.

43 *Id*. at *5.

44 There are numerous e-discovery risks associated with conducting internal IT investigations, including loss or alteration of critical metadata.

45 *See* Lauren Schwartzreich, The Internet is Written in Ink: Workplace Liabilities & Litigation Hurdles In The Age of Web 2.0, ABA Annual Meeting (August 7, 2011).

46 *Van Alstyne v. Elec. Scriptorium, Ltd.*, 560 F.3d 199 (4th Cir. 2009).

47 *Id*.

48 *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC,* 759 F. Supp. 2d 417 (S.D.N.Y. 2010)

49 *Id*. Ultimately, the employer was awarded significant damages for its claims against the defendant-employee, but the employer's own employees were held liable for $4,000 in damages for violating the SCA. *See Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 813 F. Supp. 2d 489 (S.D.N.Y. 2011).

50 No. 06-5754 (FSH), 2009 WL 3128420 (D. N.J. 2009). *See* discussion *supra* Part II.B.2.

51 The parties disputed whether this employee was coerced into turning over her password to her managers.

access to the MySpace forum was coerced into doing so.[52] While the precedential value of this case may be limited by its unique facts, it should serve as a reminder that employers may need to obtain valid authorization before examining social media content protected by the SCA.[53]

Employers may also be liable under the SCA for improperly accessing employee text messages. Employers that own their employees' cell phones, pay the bills and are parties to the cellular service contracts may be liable under the SCA where they access employees' personal text messages via the cell phone provider's servers.[54] However, where an employer collects text messages directly from employer-owned cell phones, or routes all text messages through a corporate network, and has obtained lawful consent in advance, the employer may be able to limit liability under the SCA.[55]

Listening to employees' video chats or phone calls may trigger liability under the Wiretap Act. In *Garza v. Bexar Metropolitan Water District*,[56] the court denied an employer's motion to dismiss a Wiretap Act claim where the employer intercepted and listened to entire telephone conversations. Although the employer maintained a handbook that aimed to reduce employees' expectations of privacy, the handbook only addressed authorization to listen to voicemails and read emails, but did not seek authorization to listen to telephone conversations.[57] Had the employer's policy addressed monitoring of phone calls, it might have succeeded in its motion. A similar Wiretap Act claim might also survive where an employer uses spyware applications to track employees' email communications by recording keystrokes — a real-time monitoring that is arguably similar to recording telephone conversations. Consequently, employers who install spyware on employees' computers may also incur liability under the Wiretap Act.[58] In contrast, an employer is less likely to face liability under the Wiretap Act for more traditional forms of email monitoring, such as by reviewing emails stored on the company's email server.[59] Again, a clear computer-use policy might reduce liability.

Investigations of an employee's computer use may also trigger ethical obligations for the employer and its counsel. In *Stengart v. Loving Care Agency*,[60] an employer investigated a former employee's laptop computer and discovered her communications with counsel. These emails had been sent from the laptop via a personal password-protected online email account. The employer's counsel failed to immediately notify the employee's counsel and also failed to return the documents or seek relief from the court when the employee's counsel sought their return. In the end, the employer was not permitted to use the emails. The court held that the employee could "reasonably expect that e-mail communications with her lawyer through her personal account would remain private, and that sending and receiving them via a company laptop did not eliminate the attorney-client privilege that protected them."[61] The court found that the employer's computer-use policy was ambiguous in the way it addressed employees' expectations of privacy.[62] The court also found that the employer's counsel violated

52 The employee that provided her password and log-in information to the managers testified that she felt she had to comply with her managers' request for the information or risk adversely affecting her job.

53 Not all social media content will be protected by the SCA. See *Crispin v. Christian Audigier, Inc.*, 2010 U.S. Dist. Lexis 52832 (C.D. Cal. Oct. 14, 2010) (subpoena seeking private email messages, Facebook "wall" posts, and comments the defendant's web mail, Facebook, and MySpace accounts was unenforceable and violated the SCA to the extent it sought private messages and wall postings, except that wall posts and web comments accessible to the general public might not be covered by the Act and remanding for factual inquiry into user's privacy settings).

54 The Ninth Circuit upheld civil liability under the SCA for a cell phone wireless provider that disclosed to an employer the transcripts of an employee's text messages sent to and from his employer-issued pager. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008), *petition for reh'g en banc denied,* 554 F.3d 769 (9th Cir. 2009), *cert. denied sub nom. USA Mobility Wireless, Inc. v. Quon*, 130 S. Ct. 1011 (2009). In *Quon,* the employee did not allege that the employer also violated the SCA by demanding production of the employee's text message communications. Arguably, the employee might have made such a claim and succeeded based on the court's reasoning.

55 *See* Philip Gordon, Quon Ruling Not Significant Obstacle to Employers' Accessing Text Messages (June 20, 2008) (http://privacyblog.littler.com/2008/06/articles/electronic-monitoring/quon-ruling-not-significant-obstacle-to-employers-accessing-text-messages/) ("Employers can easily and lawfully circumvent the [9th Circuit] court's ruling [in *Quon*]. Employers, for example, can prohibit employees from conducting any company business other than over the corporate network, and they can limit company-issued electronic devices to those, such as a Blackberry, that can be configured to route all communications through the corporate network.")

56 639 F.Supp.2d 770 (2009).

57 *See also, Hay v. Burns Cascade Co.*, No. 5:06-CV-0137 (NAM/DEP), 2009 WL 414117 (N.D.N.Y 2009) (denying summary judgment of employee's Wiretap Act claims where employer maintained policy stating that it could monitor any transmission but employee presented evidence that she did not receive the policy and was never alerted that her calls were monitored); *but see Arias v. Mut. Cent. Alarm Serv., Inc.*, 202 F.3d 553 (2d Cir. 2000) (recording employees' telephone conversations was within ordinary course of business for company which regularly monitored incoming and outgoing calls).

58 *See Brahmana v. Lembo*, No. C-09-00106, 2009 WL 1424438 (N.D. Cal. May 20, 2009) (denying motion to dismiss Wiretap Act claim, in part, where employer used keystroke monitoring software; issue of whether means of monitoring affected interstate commerce was left to discovery). *But see*, *Rene v. G.F. Fishers, Inc.*, No. 1:11-CV-514, 2011 WL 4349473 (S.D. Ind. Sept. 16, 2011) (dismissing Wiretap Act claim where capture of keystrokes occurred internally on computer, separated from connection to interstate commerce).

59 *Cf. Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994) (seizure of stored emails did not violate Wiretap Act because they were no longer in transmission).

60 990 A.2d 650, 655 (N.J. 2010).

61 *Id*.

62 *Id*. at 659 (policy was ambiguous where it stated that emails were not to be considered private and yet also stated that employees were permitted to use emails for occasional personal use, and was also unclear in that it did not address personal Web-based email accounts).

state ethics rules, which follow the ABA's Model Rules of Professional Conduct, by failing to immediately disclose that it had obtained the communications, and the case was remanded for a hearing on appropriate sanctions.[63] While numerous courts have rejected the notion that an employee retains an expectation of privacy within the employer's computer system,[64] employers should still keep in mind the potential ethical triggers and the risks associated with using attorney-client communications as evidence.

In addition to the liabilities listed above, employers' investigations may trigger liability under the National Labor Relations Act ("NLRA"). In *Hispanics United of Buffalo v. Ortiz*,[65], an employer terminated five employees after an investigation revealed that those employees posted comments on Facebook concerning a sixth employee who had accused the workers of poor performance. The ALJ held that the comments constituted protected concerted activity and that the employer could not prohibit such online communication. As recently reiterated by the NLRB's Office of General Counsel in a report on social media cases, online speech for "mutual aid or protection" in the workplace may constitute concerted activity under Section 7 of the NLRA.[66]

While workplace misconduct can greatly impede any business, proper investigation of such activities may provide employers with some protection and perhaps legal recourse. However, reckless internal investigations may increase an employer's liability and tempt employees to file claims against the employer. Truly effective investigations, including those aided by forensic collection and review, may reveal and confirm important details about employee conduct and provide the employer with an edge in subsequent litigation.

One additional and logical extension of this discussion concerning workplace misconduct and technology use is how e-discovery impacts workplace investigations. An employer who mishandles an investigation increases its exposure to not only the types of civil actions discussed above, [67] but also to unfavorable litigation rulings based on a failure to comply with rules of civil procedure or evidence. This litigation liability includes sanctions for failure to preserve evidence[68] or denial of a motion to admit evidence into the record.[69] For example, where an employer investigates an employee's computer use in a theft of trade secrets action but inadvertently overwrites the computer's critical metadata in the process, the employer may have spoliated critical evidence. Altering metadata during the investigatory process can result in sanctions for failing to preserve evidence, including, dismissal of the lawsuit.[70] Likewise, if the employer retains a copy of a critical smoking-gun file, but fails to collect the evidence needed to authenticate the file, the employer may be precluded from admitting the file into evidence.[71] Such a ruling might destroy the employer's case. These procedural and evidentiary liabilities, combined, may place an employer in a worse situation than if the original investigation had never occurred. To reduce this double-whammy of civil liability (discussed above) and litigation liability, employers would be wise to leverage the skills of e-discovery counsel and, where appropriate, technology experts.

63 *Id*. at 666.

64 *Compare U.S. v. Slanina*, 283 F.3d 670, 676-77 (5th Cir. 2002) (reasonable expectation of privacy in employee's computer and files where he took precautions to limit access and the employer did not disseminate any policy preventing the storage of personal information and did not inform its employees that their computer use might be monitored), *vacated on other grounds*, 537 U.S. 802 (2002); *Haynes v. Office of the Attorney Gen.*, 298 F.Supp.2d 1154, 1161-62 (D. Kan. 2003) (reasonable expectation of privacy in private computer files, despite computer screen warning of no expectation of privacy where employer's practice permitted personal use and no evidence was offered to show that the employer ever monitored private files or employee e-mails) *with U.S. v. Simons*, 206 F.3d 392, 398 & n. 8 (4th Cir. 2000) (no reasonable expectation of privacy in office computer and downloaded Internet files where employer had a policy of auditing employee's use of the Internet, and the employee did not assert that he was unaware of or had not consented to the policy); *Muick v. Glenayre Elec.*, 280 F.3d 741, 743 (7th Cir. 2002) (no reasonable expectation of privacy in workplace computer files where employer had announced that he could inspect the computer); *Thygeson v. U.S. Bancorp*, No. CV-03-467-ST, 2004 WL 2066746, at *20 (D. Or. Sept. 15, 2004) (no reasonable expectation of privacy in computer files and e-mail where employee handbook explicitly warned of employer's right to monitor files and e-mail); *Kelleher v. City of Reading*, No. Civ. A. 01-3386, 2002 WL 1067442, at *8 (E.D. Pa. May 29, 2002) (no reasonable expectation of privacy in workplace e-mail where employer's guidelines "explicitly informed employees that there was no such expectation of privacy"); *Garrity v. John Hancock Mutual Life Ins. Co.*, No. Civ. A. 00-12143-RWZ, 2002 WL 974676, at *1-2 (D. Mass. May 7, 2002) (no reasonable expectation of privacy where, despite the employee created password to limit access, the company periodically reminded employees that its e-mail policy prohibited certain uses and the e-mail system belonged to the company).

65 N.L.R.B. (No. 3-CA-27872, 2011).

66 N.L.R.B., Office of Gen. Counsel, Div. of Operations-Mgmt., Memorandum OM 11-74 (Aug. 18, 2011), *available at* http://www.palaborandemploymentblog.com/uploads/file/Report%20of%20the%20Acting%20 General%20Counsel%20Concerning%20Social%20Media%20Cases.pdf.

67 *See* discussion, *supra*, of *Pietrylo* and *Pure Power Boot Camp*, cases.

68 *See Amron Intnl. Diving Supply, Inc. v. Hydrolinx Diving Commc'n.*, 3:11-cv-01890, Slip Op. (S.D. Ca Feb. 22, 2012) (former employee accused of theft of trade secrets wiped contents of hard drives and threw some away, resulting in monetary sanctions); *Passlogix, Inc. v. 2FA Tech.*, LLC, 2010 WL 1702216 (S.D.N.Y. Apr. 27, 2010) (company's failure to preserve e-mails and text and Skype messages constituted gross negligence and sanctions in the amount of $10,000 were awarded to the opposing party); *Kvitka v. Puffin Co.*, LLC, 2009 WL 385582 (M.D. Pa. Feb. 13, 2009) (dismissing plaintiff's lawsuit because plaintiff threw away "old" laptop upon purchasing a new one, after the duty to preserve had been triggered)

69 *See* Fed. R. Evid. 901(a) ("To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.")

70 See *Micron Tech., Inc. v. Rambus Inc.*, 645 F.3d 1311 (Fed. Cir. 2011) (duty to preserve evidence arises where litigation is "pending or reasonably foreseeable"); *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir.1998) (duty to preserve evidence arises upon reasonable anticipation of litigation).

71 See *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (D. Md. 2007) (denying cross-motions for summary judgment each side had failed to properly authenticate electronic evidence and warning that authentication of electronic evidence "may require greater scrutiny" than that of ordinary physical evidence.)

E-discovery counsel can advise employers as to best practices for workplace investigations and preservation and collection of evidence for use in litigation. In addition, e-discovery counsel can oversee and guide technology experts in their investigations, collections and review.

As a final note, employers should be aware that one of the most effective tools for preventing workplace electronic misconduct is consistent enforcement of clear and targeted technology use policies. Effective policies, combined with appropriate monitoring, can improve workplace morale while protecting the employer's systems, data, devices and reputation.[72] Where employees have a clear understanding of the dos and don'ts of workplace technology, and receive consistent reminders, they may be less tempted to put their employer's data at risk. Effective policies are a step toward prevention, and, like Benjamin Franklin wisely said, "[a]n ounce of prevention is worth a pound of cure.

72 For updates on current trends and case law involving workplace computer use policies, visit Littler's blogs: http://privacyblog.littler.com/ and http://www.digitalworkplaceblog.com/.