A Brave New World: Protecting Information (Including Trade Secrets) in the Cloud and in Social Media

By Robert B. Milligan and D. Joshua Salinas

I. Introduction

The explosion of cloud computing has provided both large and small companies with many technological benefits, but with those well recognized benefits there are incumbent risks to valuable company data, including prized trade secrets. Companies utilizing cloud computing must employ effective measures to protect and secure their intellectual property. Vendor agreements with cloud providers should be carefully scrutinized to ensure that appropriate contractual provisions are in place to protect company data, including provisions addressing ownership, access, protection, and privacy from both a national and international perspective. Companies should attempt to incentivize their agreements with vendors to ensure that the company's business objectives, including secure data protection, are met.

Social media, which use cloud computing, have also provided companies with access to dynamic platforms for business growth. To effectively navigate in this new environment, companies must ensure that they adopt effective policies that foster creative expression yet protect company data and secrets, including employment policies, with clear direction and guidance for employees. Sensible executives will seek advice from competent counsel to ensure that the cost savings and financial opportunities in cloud computing, including social media, are not outweighed by the potential legal and business risks.

Cloud computing is a hot technology movement. Over forty-three percent of chief information officers expect to utilize cloud services within the next few years.[1] MarketsandMarkets estimates that the cloud computing market will grow from $37.8 billion in 2010 to $121.1 billion in 2015.[2] Cisco predicts that worldwide IP traffic in the cloud will increase twelvefold over the next five years and account for more than one-third of total data center traffic by 2015.[3] Verizon recently spent $1.4 billion to acquire cloud services provider Terremark Worldwide, Inc., which is expected to stimulate other rival carriers to enter the cloud industry.[4] However, the new cloud computing buzz is not new technology to many industry insiders. As Larry Ellison of Oracle stated, it is "[e]verything that we already do."[5]

Cloud computing is a metaphor for the Internet. It comes from the early days when network engineers used a cloud in their network design illustrations to indicate unknown domains. The engineer knew the domain was there, but the details of that domain were unknown. This network of clouds is how we view the Internet today. Cloud service users know their information is readily accessible but generally lack any interest in where that information is physically located. Cloud service users generally can access their information at any place, at any time, and on any device, as long as they have a network connection. Indeed, cloud computing is part of our everyday lives. If you have performed a Google search, checked Yahoo email, or signed in to Facebook, Twitter, or LinkedIn, you have reached into the cloud.

Cloud computing lacks a universal definition. Ask different people in the IT industry what cloud computing is and you will get different answers. The National Institute of Standards and Technology (NIST) has provided the most widely accepted definition: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[6] The NIST also notes five essential characteristics of cloud computing services: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.[7]

Cloud computing has numerous technical benefits. Users typically pay the cloud provider for the services and resources they use. This pay-as-you-go infrastructure allows companies to reduce costs. Companies can avoid paying for costly equipment, personnel, and maintenance. For example, if a company needs additional storage space for its data, it can purchase more from the cloud provider. Without cloud computing, the company may have to pay for additional servers, allocate space for bulky servers, and hire additional IT staff, among other costs. Cloud computing also provides scalability. The ability to adapt and quickly respond to increased market demands is invaluable to small companies that lack the finances to significantly invest in expensive IT infrastructure. The on-demand access provides access wherever a cloud user has a network connection. This mobility and convenience is one of the reasons low-cost netbooks and tablet devices such as iPads have rapidly radically increased in popularity. Companies are embracing the cloud as a cost effective way to do business. It provides smaller companies with a better chance to compete.

Cloud computing involves three general service models. The simplest model is Infrastructure as a Service (IaaS). This involves basic storage and data hosting. The second model is Software as a Service (SaaS). In this model, the cloud provider provides the software to access,

manage, and utilize the data. This is commonly seen with email (e.g., Gmail, Yahoo mail, Hotmail) and social media sites (e.g., Facebook, LinkedIn, Twitter). The third model is Platform as a Service. This model provides an operating system in which the company can develop and build its own applications. For example, Facebook allows third parties to build and distribute applications within its service. The main factor distinguishing the three models is the level of control the subscriber retains over its data.

While cloud computing is not new, expansive and accelerated network connectivity has fueled the ascent of this technology movement. Companies embracing cloud computing will move data previously stored in-house onto servers provided by third parties. However, moving confidential and proprietary information, such as trade secrets, raises numerous legal, security, and business concerns.

II. Trade Secrets

A trade secret is any information not generally known that is economically valuable and that is subject to reasonable efforts to maintain its secrecy.[8] Many people think of secret formulas, such as the ingredients for Coca-Cola, KFC, or WD-40. Yet trade secrets also can include a wide variety of technical and nontechnical information. Common trade secrets include manufacturing methods, formulas, techniques, business and marketing plans, customer lists, and computer programs. There is no requirement to register or publish a trade secret to receive protection. In addition, a trade secret does not have to involve novel information. The heart of the trade secret's value is its secrecy.

A trade secret owner must take reasonable efforts to ensure the information's secrecy.[9] He or she must make actual efforts to protect the trade secret so that it is not lost through improper, illegal, or unethical means. The burden is on the trade secret owner to keep the information secret; the owner cannot expect others to keep the information secret.

Trade secret law protects against misappropriation, i.e., the illegal or unauthorized acquisition, disclosure, or use of information. Trade secrets are creatures of statute and are protected under several laws such as the Uniform Trade Secrets Act (UTSA), Economic Espionage Act of 1996 (EEA),[10] and the Computer Fraud and Abuse Act (CFAA).[11] Varying versions of the UTSA are enacted in forty-seven states.

Trade secret law holds third parties liable if they knew or had reason to know of misappropriation.[12] However, it generally does not protect against the accidental disclosure or the reverse engineering of a trade secret.[13] For example, if a trade secret is accidentally disclosed by a cloud provider or third party, it could potentially lose its trade secret status if the data leak is not promptly and effectively addressed.

Unlike patent, trademark, or copyright protection, there is no set duration for trade secret protection. A trade secret is protected as long as it is kept secret. However, once a trade secret is lost, it is lost forever. As we have seen in the post-Wikileaks world, once confidential information is disclosed, it can be distributed instantly online for hundreds of millions to see, access, and download.[14]

III. Problems

An issue with new technology is that the law is constantly behind. "[Courts] try to keep up with technology and understand it, but things move so quickly."[15] The use of cloud computing raises several problems for trade secrets. Placing confidential information in the hands of a third-party cloud provider seems contrary to maintaining secrecy. Moreover, information placed into the cloud increases the risk that the information will be accidentally or intentionally disclosed to third parties.

A threshold issue is whether placing confidential information into the cloud diminishes its status as protectable information. Can trade secrets lose their protection in the cloud? The answer may vary depending on the nature of the information and who places the information in the cloud. Courts have used six factors to determine whether a piece of information is secret. These are: (1) the extent to which the information is known outside the company; (2) the extent to which the information is known by employees and others inside the company; (3) the extent of measures taken by the company to protect the secrecy of its information; (4) the value of the information to the company and competitors; (5) the amount of time, effort, and money expended by the company in developing the information; and (6) the ease or difficulty with which the information can be properly acquired or duplicated by others.[16]

A New York district court found a company's customer list was not a trade secret because the information at issue had already been disclosed in the cloud and was publicly accessible. In *Sasqua Group v. Courtney*,[17] an executive search consulting firm alleged that a former employee stole confidential customer information from a client database and later solicited those clients. The confidential database contained client contact information, individual profiles, resumes, descriptions of interactions with clients, and hiring preferences. The court focused on the sixth factor in the six-factor analysis, i.e., the ease with which the information could be acquired by others. The former employee demonstrated how easily she could find the same client database information by searching LinkedIn, Google, Bloomberg.com, and FX Week. The court found the client database did not constitute a trade secret because the information was easily accessible to the public online. In doing so, the court noted that the protection of certain information may no longer be viable in the twenty-first century in light of new technologies.[18]

A recent New Jersey district court case, however, found that trade secret information may not necessarily lose its trade secret status despite being posted on the Internet. In *Syncsort Inc. v. Innovative Routines, Int'l, Inc.*,[19] the plaintiff data transformation software company alleged that a competitor had improperly developed software when the competitor allegedly improperly acquired and used the plaintiff's trade secrets—confidential command language. The defendant argued that portions of the command language had been posted on the Internet and thus were no longer secret. Moreover, the defendant argued that entire copies of the plaintiff's Reference Guides regarding the command language had been posted temporarily on the Internet, once in Korea and once in Japan.

The court found that the Internet postings did not defeat the command language's trade secret status because (1) the parts of command language posted were insufficient to fully disclose the complete command language and (2) the Reference Guide posts in Korea and Japan were obscure and transient such that it was not made generally known to other competitors in the industry. The takeaway from the case is that the "secrecy" of information may be determined based on the surrounding circumstances and nature of the online disclosure rather than by the mere fact that the information was posted online.

Similarly, a current Northern District of California case, *PhoneDog v. Kravitz*,[20] involves a dispute over whether a Twitter account's followers constitute trade secrets even when they are publicly visible. The court denied the defendant's motion to dismiss and ruled that PhoneDog, an "interactive mobile news and reviews web resource," could proceed with its lawsuit against Noah Kravitz, a former employee, who it claims unlawfully continued using PhoneDog's Twitter account after he quit. The court held that PhoneDog had described the subject matter of the trade secret with "sufficient particularity" and satisfied its pleading burden as to Kravitz's alleged misappropriation by alleging that it had demanded that Kravitz relinquish use of the password and Twitter account but that he refused to do so. With respect to Kravitz's challenge to PhoneDog's assertion that the password and the account followers do, in fact, constitute trade secrets—and whether Kravitz's conduct constitutes misappropriation—the court ruled that such determinations require the consideration of evidence outside the scope of the pleading and should, therefore, be raised at summary judgment rather than on a motion to dismiss. This case merits attention.

Another issue arises when cloud providers use the hosted information for secondary purposes. For example, information containing customer lists or contact information is highly valuable for market studies and behavioral targeting. Providers can earn substantial revenues reselling this raw data to advertisers and other third parties.

Perhaps more threatening to trade secrets are cyber attacks. Hackers have recently targeted their attacks at corporate trade secrets and proprietary information. McAfee reported on the Night Dragon cyber attacks that have targeted oil and gas industry trade secrets.[21] IBM's X-Force cyber security team also reported that cyber criminals now pinpoint valuable corporate data.[22] There is a thriving criminal market for converting stolen trade secrets into cash.[23] In fact, criminal gangs in China, Russia, and the Ukraine will steal information for companies looking to undercut their rivals.[24] Hackers are eagerly awaiting more corporations to embrace cloud computing and to release prized data into the cloud.

The inherent risks in utilizing cloud computing were demonstrated last year with one of the largest security breaches in United States history—the March 2011 Epsilon security breach.[25] Epsilon is one of the largest permission-based email marketing companies. It sends over forty billion emails each year on behalf of over 2,500 clients. Its clients include US Bank, Capital One, Chase, Citi, JPMorgan, Best Buy, Hilton, Target, and Disney. On March 30, 2011, Epsilon detected an unauthorized entry into its customer databases. It discovered that hackers had obtained access to thousands of names and email addresses. As a result, these hackers now have the ability to send highly effective spear-phishing emails to their recently acquired targets.[26]

The following scenario could arise from the Epsilon or other cloud computing breaches: (1) hacker reviews improperly obtained customer information and discovers that the customer works at a large corporation or firm; (2) hacker crafts a well designed email posing as the company to which the client gave its email address (e.g., Best Buy, Target, Citi); (3) customer opens the email at work, clicks a provided link, and undetectable software is downloaded onto the customer's computer; and (4) undetectable software quietly sits inside the corporate network, searches for trade secrets or confidential information, and sends it back to the hacker. Security software company Symantec reports that in 2011 at least fifty companies in the defense and chemical industries were targeted by these spear-fishing attacks, which were specifically aimed at prized research and development information.[27]

Aside from the intentional theft by outside parties, trade secrets always have been susceptible to misappropriation by current or former employees. The typical case involves the disgruntled employee who discloses or uses trade secrets after termination. Yet, the use of cloud services such as social media increase the risks of both intentional and accidental disclosure by such employees.

A related issue involves the ownership of data. If a provider or employee modifies the data, do they have any ownership rights in it? Taking the case of a customer list, if an employee "friends" clients and adds them to a LinkedIn profile, does the contact belong to the em-

ployee or to the employer? If the employee leaves his or her employer, can he later contact previous clients? This issue was the underlying dispute in *TEK Systems v. Hammernik*.[28]

In *TEK Systems*, the plaintiff, an IT staffing firm, alleged that a former employee violated a non-solicitation agreement when the employee contacted previous clients on LinkedIn. The non-solicitation agreement lacked any social media restrictions. The issue was whether the employee violated the non-solicitation agreement when she allegedly contacted the clients through her personal social media account after she had gone to work for a competitor. The parties eventually stipulated to the enforcement of the non-solicitation agreement and the return of TEK Systems' documents. Unfortunately, no ruling or precedential decision arose from this case.

The ownership of a social media account is also at issue in the previously discussed *PhoneDog* case—specifically, whether the employer or employee owns the subject Twitter account. PhoneDog asserted a conversion claim, which Kravitz challenged on the ground that PhoneDog had not sufficiently alleged that it owns or has the right to immediately possess the Twitter account. Kravitz also argued that PhoneDog failed adequately to allege that he had knowingly or intentionally engaged in the alleged act of conversion. The court, however, found that these issues lie "at the core of [the] lawsuit" and that, accordingly, an evidentiary record had to be developed before the court could resolve such fact-specific issues.

In *Eagle v. Morgan*,[29] the court held that an employer may claim ownership of its former executive's LinkedIn connections where the employer required the executive to open and maintain the account; the executive advertised her and her employer's credentials and services on the account; and the employer had significant involvement in the creation, maintenance, operation, and monitoring of the account. Similar to *Sasqua Group*, the court found that the contact lists in the LinkedIn account could not constitute trade secrets because they were publicly accessible online. The takeaway in *Eagle*, however, is that employers should consider getting more involved in their employees' social-networking activities and utilize contracts to assign ownership in such accounts.

The nature of trade secrets as digital information within the cloud raises potential litigation concerns. For example, data is often transitory, moving between various servers and facilities. Trade secrets may move from state to state and even across international borders. Thus, difficulties may arise in establishing jurisdiction in cases of trade secret theft. Moreover, a cloud provider's obligation to comply with electronic discovery demands may compromise the integrity of trade secrets or confidential information if secrecy protections such as protective orders and confidentiality agreements are not employed.

Finally, problems may arise with data access continuity. What happens when the contract or subscription for cloud services terminates? The cloud provider may withhold data when a company fails to pay for services. Additionally, what happens when a small startup provider goes bankrupt or is purchased by another company? These and many of the problems discussed above may be addressed with effective and well drafted contracts as part of a well developed cloud computing strategy before placing your company's data in the cloud.

IV. Solutions

The problems of storing data in the cloud are not insoluble. The first step is to conduct a trade secret audit or inventory before placing information in the cloud. Determine what information is sensitive and confidential. Highly valuable trade secrets can remain off the cloud and stored in-house on secured networks or in physical areas. Keeping information out of the cloud inherently reduces the risk it will not be disclosed on the cloud. When in doubt, do not make the information available on the cloud. To the extent you determine that certain trade secret information can be placed in a secure cloud, keep track of such data, as well as of the security measures in place to protect such data (encryption, confidentiality designations, written agreements, etc.) and of who has access to the data.

Once you decide to utilize cloud computing, take all prudent and necessary measures to select the correct provider. Perform diligent checks on all potential providers. Obtain references. Determine whether they have the capability to provide the type of services you desire. Conduct interviews with the providers. Find out their financial viability. View their security and privacy policies and find out how many security breaches they have experienced. Determine whether your data will be encrypted and whether your cloud provider subcontracts its services with third parties. Evaluate choice-of-law, choice-of-forum, and indemnification provisions carefully. Security rather than price should be your top priority. You may want to consider diversifying your portfolio of data stored on the cloud with multiple providers or backup locally all information stored in the cloud.

State law may require you to contract with the cloud provider to ensure that reasonable security procedures and practices are in place. California requires businesses that possess personal information about California residents to implement and maintain reasonable security procedures and practices.[30] Businesses that disclose this personal information to third parties (e.g., cloud providers) must contract with the third party to implement and maintain reasonable security procedures and practices. Massachusetts also requires contracts to implement and maintain appropriate security measures when providing personal information to cloud providers.[31] Nevada requires businesses to use encryption on data storage devices that contain personally identifiable information.[32]

After the provider is chosen and a trade secret audit or inventory has been conducted, the best way to protect trade secrets and other information is through well-drafted contracts and policies and periodic audits of the cloud provider. This includes contracts with both cloud providers and with the company's own employees who may access the information. First, define the ownership rights in the data. For example, you may want to explicitly state that the cloud provider and employees have no ownership rights in the data. The agreement can state that the provider and employees have limited access to the data only for certain reasons. Defining the limits of authorization also can help establish rights under the CFAA if the provider or employee violates the scope of their authorizations.

Next, define the scope of the protected information. Specifically indicate which information is considered trade secret or confidential. The Economic Espionage Act's language may be preferable because it provides a broad definition of a trade secret. Also include language protecting confidential and propretiary data. Prohibit the unauthorized use or disclosure of company data, including trade secrets and confidential and proprietary information. Contracts also can provide for injunctive relief, liquidated damages, arbitration, and attorneys' fees.

Companies also should control access to their data. Agreements with cloud providers should restrict the use of data to outside vendors or third parties and should hold the provider and any subcontractors liable for security breaches. This is especially important in light of the 2011 Epsilon security breach. Companies should require heightened security standards, such as ISO standards. These standards represent an international consensus on good-quality management practices. For example, they require quality audits, effective training, and corrective actions for problems. In addition, the Federal Trade Commission has provided five key principles for sound data security plans: (1) know the personal information you have; (2) scale down and keep only what you need; (3) protect the information you want to keep; (4) properly dispose of what you no longer need; and (5) create a plan to respond to security incidents.[33]

Contracts should include ongoing confidentiality obligations in case of termination, and they should require the return or deletion of any copies of the data (as appropriate) by the provider or employee after the termination of the agreement. Finally, there should be a provision prohibiting the withholding of data by the provider or employee in the case of a dispute.

As part of a comprehensive policy to address data protection in the cloud, companies should establish effective security and social media policies to prevent employee disclosure of information. Information security measures include password protection, email and electronic data policies, departmental trainings, and exit interviews to remind employees of confidentiality obligations.

Social media policies are even more critical today with explosion of social media in the workplace. Well-drafted and communicated policies can effectively reduce the amount of sensitive information disclosed both accidentally and intentionally on the Internet. Social media policies can restrict employees from posting confidential information on sites such as Facebook, Twitter, or LinkedIn. Employees should be educated about the implications of posting information to these sites through recurring training. For example, Facebook grants itself a license to any information posted on its site,[34] and Twitter grants itself a license to make any posted content available to other companies.[35] Employers should provide constant reminders to employees not to disclose confidential data on such sites.

Employers should, however, be very cautious in the drafting of their social media policy. An overly broad policy could violate employee rights. Employers must align their policies with the National Labor Relations Act (NLRA) to avoid the ire of the National Labor Relations Board (NLRB). Section 7 of the NLRA protects both unionized and non-unionized employees' right to engage in concerted activities in the United States. The NLRB has criticized several employers' social media policies for being overly broad and violative of employee rights.

In *NLRB v. American Medical Response of Connecticut*, an employer terminated an employee who allegedly posted negative remarks about her supervisor on Facebook.[36] The employer's policy prohibited employees from describing the company in any way on the Internet without its permission. The NLRB alleged that this policy violated the employees' right to engage in concerted activities and discuss her work environment. The parties eventually reached a settlement, and the NLRB thus did not officially rule on the legality of the employer's policy.

Several other social media-employment dispute cases caused the NLRB's Acting General Counsel to release a report on January 24, 2012.[37] In his report, Acting General Counsel Lafe E. Solomon analyzed fourteen recent social media-employment dispute cases and reaffirmed the NLRB's position that social media policies that restrict the ability of employees to discuss working conditions and wages are unlawful. In particular, Mr. Solomon found unlawful social media policies that (1) provide no clear guidance to employees as to what online communications and postings are appropriate; (2) do not provide specific examples of the types of confidential or sensitive information that are prohibited from online disclosure; and (3) "would reasonably tend to chill employees in the exercise of their section 7 rights." The underlying concern is that overbroad social media policies may cause employees to believe that their rights under section 7—to discuss their

workplace environment and self-organize—are otherwise prohibited.

Employers should employ specifically tailored social media policies that protect trade secrets and confidential information. Indeed, the NLRB found an employer's social media policy that restricted employees from using or disclosing confidential and or proprietary information are lawful and compliant with the NLRA. However, the NLRB requires that these restrictions sufficiently describe and provide examples of what the employer considers proprietary, confidential, and/or trade secret information. Employers should distance the company from personal social media use by employees that attempts to associate the employee with the company. For example, employers should prohibit the use of company trademarks, graphics, or logos for personal use. Companies also should prohibit, or at least limit, the use of company-provided email addresses for personal social media activity. Companies must be vigilant to ensure that their cloud computing policies and agreements, including social networking policies, remain current with changing technology to protect their most valuable assets.

V. Conclusion

Cloud computing provides significant benefits for the development and growth of businesses, but companies that embrace this technology and venture into the cloud must be careful and thoughtful. Companies should scrutinize what they put into the cloud and select reliable and security-conscious cloud providers. Well-drafted agreements and policies with both providers and employees can help reduce the risk of the disclosure of trade secrets in the cloud. A comprehensive cloud computing strategy can help companies realize the cost savings and financial opportunities in cloud computing, including social media, while ensuring that these benefits are not outweighed by the potential legal and business risks.

Endnotes

1. According to a 2010 survey, http://www.gartner.com/it/page.jsp?id=1526414.
2. http://www.marketsandmarkets.com/Market-Reports/cloud-computing-234.html.
3. "Cisco Global Cloud Index: Forecast and Methodology, 2010–2015," http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1175/Cloud_Index_White_Paper.pdf.
4. http://news.businessweek.com/article.asp?documentKey=1376-LFPBHT6JIJUX01-4B7UIEITJ82MA34J8V0CJMEHFP.
5. Quoted in the Wall Street Journal, Sept. 26, 2008.
6. NIST Definition of Cloud Computing, v. 15, http://csrc.nist.gov/groupsSN/Sloud-computing/.
7. Identified by NIST as part of its definition of cloud computing.
8. *See, e.g.*, 18 U.S.C. § 1839 (3) (A), (B) (1996); Cal. Civ. Code § 3426.1(d).
9. *J. T. Healy & Son, Inc. v. James A. Murphy & Son, Inc.*, 357 Mass. 728, 730-31 (1970).
10. 18 U.S.C. § 1831.
11. 18 U.S.C. § 1030.
12. *See Kozuch v. CRA-MAR Video Ctr., Inc.*, 478 N.E.2d 110 (Ind. Ct. App. 1985).
13. *Kewanee Oil Co. v. Bicron Corp.*, 94 S. Ct. 1879, 1883 (1974).
14. WikiLeaks website publishes classified military documents from Iraq, http://articles.cnn.com/2010-10-22/us/wikileaks.iraq_1_wikileaks-website-classified-documents-iraq-wiki-leaks-iraqis?_s=PM:US.
15. Judge Alex Kozinski, Ninth Circuit U.S. Court of Appeals, speaking at Golden Gate University's Intellectual Property Distinguished Speaker Program, April 13, 2011.
16. These factors are the "most-cited listing of the objective criteria for determining the existence of a trade secret." *M. Jager*, Trade Secrets Law § 5.05 (1995).
17. No. CV 10-528 ADS AKT, 2010 WL 3613855 (E.D.N.Y. Aug. 2, 2010), *report and recommendation adopted*, No. 10-CV-528 ADS ETB, 2010 WL 3702468 (E.D.N.Y. Sept. 7, 2010).
18. *Id.* at *22.
19. No. CIV. 04-3623 WHW, 2011 WL 3651331 (D.N.J. Aug. 18, 2011).
20. No. C 11-03474 MEJ, 2011 WL 5415612 (N.D. Cal. Nov. 8, 2011).
21. Global Energy Cyberattack, "Night Dragon," http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.
22. *Available at* http://www-03.ibm.com/security/landscape.html.
23. http://www.usatoday.com/tech/news/2011-03-31-hacking-attacks-on-corporations.htm.
24. *Id.*
25. "Epsilon data security breach expands, could be history's largest," http://www.digitaltrends.com/computing/epsilon-data-security-breach-expands-could-be-historys-largest/.
26. "Epsilon hacking shows new 'spear-phishing' risks," http://www.reuters.com/article/2011/04/04/us-hackers-epsilon-idUSTRE7336DZ20110404.
27. "The Nitro Attacks: Stealing Secrets from the Chemical Industry," Eric Chien and Gavin O'Gorman, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf.
28. No. 0:10-cv-0081 (D. Minn).
29. No. 11-4303, 2011 WL 6739448 (E.D. Pa. Dec. 22, 2011).
30. Cal. Civ. Code § 1798.81.5.
31. 201 C.M.R. 17.00 et seq.
32. Nev. Rev. Stat. 603A.010 et seq.
33. http://www.ftc.gov/bcp/edu/microsites/infosecurity/.
34. http://www.facebook.com/terms.php.
35. http://twitter.com/tos.
36. *American Med. Response of Conn.*, NLRB Reg. 34, No. 34-CA-12576, *complaint issued* Oct. 27, 2010.
37. Report of the Acting General Counsel Concerning Social Media Cases, Lafe E. Solomon, Jan. 24, 2012, http://www.faegrebd.com/webfiles/OM_12_31_Report_of_the_Acting_General_Counsel_Concerning_Social_Media_Cases.doc.pdf.

Robert B. Milligan is a partner in the Litigation and Labor & Employment Departments of Seyfarth Shaw LLP in Los Angeles. D. Joshua Salinas is an attorney in the firm's Los Angeles office.