Bloomberg Law Reports®

February 13, 2012

Technology Law

Privacy & Information Law

Data & Information Security

Is Social Media a Corporate Spy's Best "Friend"? How Social Media Use May Expose your Company to Cyber-Vulnerability


Norris McLaughlin & Marcus, P.A.
Attorneys At Law

Contributed by Fernando M. Pinguelo and Bradford W. Muller, Norris McLaughlin & Marcus, P.A.

The rise of social media has ignited a societal change in how people across the world communicate and "stay in touch."[1] These social networking websites allow users to create personal profiles, post comments, join groups, add contacts,[2] and most important, find like-minded people with whom to share ideas, interests, and experiences. They give users the opportunity to link with others, both near and abroad, based on shared personal interests and business or academic affiliations.[3]

However, in the business community, social networking also makes companies more susceptible to corporate espionage, *i.e.*, "clandestine techniques used to steal valuable information from businesses."[4] This is caused, in part, by the fact that "[t]he general informality of social media sites like Twitter or Facebook encourages employees to let their guard down and casually share information without thinking twice."[5]

The risks created from social media use by employees are too great to ignore. For example, the development of "scraping" software allows cyber-spies to harvest personal details from thousands of users on social networking sites.[6] When scraping software[7] is targeted at the profiles of a certain company's employees and the information gathered is reconstituted, it has the potential to alert a competitor to such things as a new product launch or internal strife at the target company. Further, even top level managers occasionally post less than flattering pictures of themselves on their Facebook pages, and such personal information can easily be used for blackmail purposes.[8]

These risks are reinforced by a recent survey of large companies that found the average corporation lost $4.3 million as a result of negative consequences associated with social media, with contributing factors including damaged brand reputation or loss of customer trust, loss of data, compliance costs, regulatory fines, litigation costs, etc.[9] While these costs[10] should not negate the value active social media use offers a company and its employees, and the added benefits that such use brings to a company's marketing and brand recognition in a global market, it requires businesses to consider the growing need for adopting a comprehensive social media policy.

One way to attempt to limit a company's vulnerability to corporate espionage is to bar the use of social networks during business hours.[11] For example, Porsche SE has "blocked employees from using Facebook to help reduce potential access points for cyber spies."[12] Many commentators, however, suggest that companies should not reflexively ban the use of social media by employees,

but rather develop a measured approach for effective and safe corporate and personal use.[13] This approach is often preferable. While a company may attempt to regulate its employees' use of social media during business hours by blocking access to certain websites, it is more difficult to prevent them from discussing their work life on their MySpace pages when they are in the comfort of their own home.

Accordingly, while this article addresses a few of the innovative ways in which a company may be exposed to increased cyber-vulnerability through its employees' use of social media, it in no way suggests that a blanket anti-social media policy should be adopted. Rather, a company should follow a policy that builds off of one of the many model policies currently available,[14] and should find a balance that fits its own corporate structure.[15] This article also offers suggested measures for companies to consider.

Let's Just Keep This Among "Friends": Employees' Natural Inclination to "Bare All" on Facebook, MySpace, Google+ and Twitter Puts Their Employers' Interests at Risk

Perhaps the largest risk created by social media is that users seem to forget that what they intend to remain "private" can become public very quickly on the Internet. An obvious example of this is Weiner-Gate;[16] though in the business setting this could involve such things as raunchy photos from an overly exuberant company holiday party,[17] or an ill-timed joke (just ask Gilbert Gottfried, the former voice of the AFLAC duck).[18] However, even seemingly innocuous comments by employees on their social media[19] pages about the launch of a secret company product, or the rumored resignation of a top level executive, could have major ramifications if discovered by a cyber-spy working for a competitor.

Further, "vulnerable" employees may be targeted by cyber-spies. Such employees include those who provide minute-by-minute details of their life through frequent "status" updates on their Facebook pages, or who post seemingly endless amounts of photos, or those who "friend" anyone who makes a request (even complete strangers). Using publicly available data, including information found on social media websites, these employees may be induced or coerced to cooperate with bad-actors, or face a targeted "spear phishing" attack[20] that uses social engineering to trick the employee into disclosing sensitive corporate information or access codes.[21] Such an attack was recently executed against WilmerHale, as an e-mail from a fictitious WilmerHale attorney was sent, instructing recipients to click on a link to respond to a subpoena. The link contained a malicious program that was designed to infiltrate the recipient's computer system.[22] This type of malware could cause massive data breaches that require costly reporting to state, and perhaps, federal authorities.[23] Accordingly, employee awareness of the dangers posed to both themselves and the company through free-wheeling social media use must be a component of any effective social media policy.

When Does Corporate Espionage Move From Competitive Due Diligence To Cybercrime?

The dearth of case-law discussing the intersection of corporate espionage and social media begs the question: When does the use of social media to gain insight into the non-public information of a competitor go from being savvy use of digital tools to illegal corporate cyber-espionage? There is obviously a monumental difference in the ethics and legality between following the Twitter feed of a competitor's CEO and engineering a "dirty-tricks" campaign, but where is that line and when is it crossed?[24]

One example of when cyber "tricks" go too far may be seen in the HBGary Federal Security firm's alleged plans to use social media and other digital tools to undermine supporters of WikiLeaks and opponents of the U.S. Chamber of Commerce.[25] HBGary first gained public notoriety in early 2011 when its chief executive claimed to have discovered the identities of leaders of the hacktivist[26] group Anonymous[27] by using publicly available information from various social media outlets.[28] Not amused, hackers promptly attacked HBGary's computer system and website, causing the security company great public embarrassment, eventually leading to its CEO's resignation.[29]

That hacking incident revealed damaging HBGary emails which showed that the firm had planned some of its own borderline illegal, and completely unethical, cyber tricks as part of a sales pitch to the Hunton & Williams law firm whose clients included Bank of America and the U.S. Chamber of Commerce.[30] Although these plans were never acted upon, they involved efforts to sabotage the WikiLeaks website on behalf of Bank of America through such measures as cyberattacks and a digital misinformation campaign. Similarly, a second plan was developed to combat foes of the U.S. Chamber of Commerce by, among other things, monitoring their communications, planting false information to embarrass them, using software programs to scrape social media sites for opponents' personal information, and creating fake personas on social media websites to gain more access to opponents.[31]

Organized misinformation campaigns such as those contained in HBGary's alleged sales pitch are troubling and certainly straddle the line of legality. This is but one example of the many ways in which social media can be used to infiltrate and undermine an organization.

The Corporate Response: How to Address the Social Media "Threat" Without Sacrificing Employee Morale, Marketing Opportunities, Innovation, Business Growth, and the "Plus" Side

Faced with this pervasive threat, many corporate leaders may find it easier to simply bar the use of social media during work hours, warn employees not to post any work related information on their social media pages during their personal time outside the office, monitor, and keep their fingers crossed that a mis-Tweet does

not lead to their company's undoing. Indeed, the luxury German car-maker Porsche, despite having an expansive Facebook page, adopted a policy that forbids staff from accessing social media during work hours,[32] as the company was acting out of concern that "foreign intelligence services may be spying on workers posting 'confidential' information" on their social networks.[33] However, the effectiveness of such a policy is dubious, as smart-phones allow for unbridled social media access during work hours, and any attempt to police employee use of social networks off-site would likely have little success.[34] Indeed, an anti-social media policy may reduce employee morale, and breed a culture of skirting company rules.[35] Further, exceedingly expansive restrictions on employee social media use are not the answer either, especially because such restrictions have emerged as a major issue in recent National Labor Relations Board reviews.[36] Even when a company has harsh restrictions in place, an attempt to enforce the policy through, for example, terminating offending-employees, may be fodder for a lawsuit.[37]

Accordingly, companies would be well served adopting a comprehensive, reasonable social media policy that incorporates vigorous employee training and awareness.[38] Such training must inform employees of the risks of posting even seemingly innocuous comments about confidential company information on their social media accounts. In the realm of protecting trade secrets and other intellectual property, this training is key, along with other reasonable measures, such as posting signs to remind employees to keep private company information confidential, requiring key employees and contractors to sign non-disclosure agreements or restrictive covenants, barring visitors from sensitive areas of the company's facilities, and marking important documents "confidential." [39] Despite the potential risks noted above, every policy should incorporate a provision (subject to relevant state law), widely disseminated within the company, and agreed to in a written consent form, which makes all employees subject to discipline for work-related misconduct that occurs through a social networking site, even if the act is perpetrated while the employee is outside the office.[40] However, it is critical that once a social media policy is adopted, a subsequent management system is developed to ensure that the policy is actively and fairly enforced.[41]

Further, mechanisms should be created for identifying and dealing with "high risk" employees whose social media use could pose a danger to the company.[42] Finally, top-level staff must be made aware of their vulnerability to both phishing attacks and blackmail campaigns. While all employees should avoid posting information or pictures/video on their social networks that could be embarrassing or compromising, it is especially important for upper-level staff, who are likely under the watchful eye of competitors' representatives, to avoid such conduct. Indeed, if the CEO of a large company were to have his or her own "Weiner-Gate," it could be disastrous for the corporation's stock price, brand, and reputation in the business community.

Conclusion

Social media has brought with it a world of new marketing opportunities, making our society a smaller, more close-knit community, while allowing its users to reconnect with long-forgotten friends and meet new colleagues from across the globe. However, like every new technology, social media's rewards are balanced by equally staggering risks. Although these risks do not merit a wholesale repudiation of social media use by a company and its employees, they do require the adoption of a comprehensive social media policy focused on educating employees and reducing vulnerabilities. While no policy is foolproof, as a simple mis-Tweet or rogue Facebook post about confidential company information could have a devastating effect on a business's competitive position, taking a proactive approach to employee social media use can reduce any company's risk of exposure.

Fernando M. Pinguelo, a Partner at Norris, McLaughlin & Marcus, P.A. and Chair of its Cyber Security & Data Protection Law Group, is a United States-based trial lawyer who devotes his practice to complex business lawsuits with an emphasis on how technology impacts disputes. He has lectured globally and written dozens of articles on this topic; and appeared on television as a legal commentator on various high-profile cases. He works closely with businesses to develop strategies to manage business and legal issues related to electronic data. As an adjunct law professor at Seton Hall University School of Law, Mr. Pinguelo developed and teaches a state-of-the art course on electronic discovery ("eDiscovery") and how technology impacts lawsuits. Recently, the U.S. Fulbright Program designated him a Fulbright Specialist for his work in eDiscovery; and he will guest lecture at Mackenzie University, São Paulo, Brazil. Mr. Pinguelo also founded and contributes to the ABA Journal award-winning blog, eLessons Learned – Where Law, Technology, & Human Error Collide. To learn more about Mr. Pinguelo and effective training programs to address business vulnerabilities to cyber activities, visit www.nmmlaw.com or email him at fmp@nmmlaw.com.

Bradford W. Muller, an Associate at Norris, McLaughlin & Marcus, P.A., is a member of the firm's Litigation and Internet Law groups. Muller has published in the area of cybercrime and cloud computing, and has spoken at international conferences held at the University of Virginia School of Law, Seton Hall University School of Law, and The Masters Conference in Washington, D.C. Muller is a graduate of Seton Hall University School of Law, magna cum laude, where he was a Comments Editor on the Seton Hall Law Review. Prior to his current position, Muller was a Judicial Law Clerk to the Honorable Anthony J. Parrillo, New Jersey Superior Court, Appellate Division.

[1] *See* David Kirkpatrick, *Social Power and the Coming Corporate Revolution: Why Employees and Customers will be Calling the Shots*, Forbes, p. 74 (Sept. 26, 2011), *available at* http://www.forbes.com/forbes/2011/0926/feature-techonomy-social-power-corporate-revolution-kirkpatrick.html.

[2] Steven C. Bennett, *Ethics of Lawyer Social Networking*, 73 Alb. L. Rev. 113, 115 (2009).

[3] *Id.*

[4] The Honorable Robert Menendez, United States Senate & Fernando M. Pinguelo, *Reducing Cybersecurity Risks – Government And Business*

Working Together, The Metropolitan Corp. Counsel, p. 19 (Sept. 2011). We have already noted the growing risk that corporate espionage poses to American companies in the current Internet Age. Fernando M. Pinguelo and Bradford W. Muller, *Virtual Crimes, Real Damages: A Primer On Cybercrimes In The United States and Efforts to Combat Cybercriminals*, 16 Va. J.L. & Tech. 116, 125 (2011).

[5] Carolyn Elefant, *The "Power" of Social Media: Legal Issues & Best Practices For Utilities Engaging Social Media*, 32 Energy L. J. 1, 23 (2011).

[6] Julia Angwin & Steve Stecklow, *'Scrapers' Dig Deep for Data on Web*, The Wall St. J. (Oct. 12, 2010), *available at* http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html; *see also* Fernando M. Pinguelo, Renato Opice Blum, and Kristen M. Welsh, *New Age Technology: Brazilian and U.S. Courts "Scraping" the Surface of Legal Boundaries of Internet Use*, Bloomberg Law Reports® - Technology Law, Vol. 3 No. 23 (Nov. 14, 2011).

[7] *See EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003) (one of the first cases to consider the legality of scraping software use against a competitor); *see also* Raymond T. Nimmer, *Information Law* § 2:17 (May 2011); Ian C. Ballon, *E-Commerce and Internet Law* § 5.01 (March 2011). For an example of scraping software, *see* Visual Web Ripper, http://www.visualwebripper.com/ (last visited Jan. 26, 2012).

[8] Indeed, insurers such as Chubb Group and Chartis Inc. are offering insurance protection that will cover cyber-extortion, providing coverage for the payment of ransoms. Michael Bradford, *Can You Keep A Secret: Thieves Seek Corporate Info*, Business Insurance (Feb. 14, 2011)

[9] David F. Carr, *Could Social Media Flub Cost you $4.3 Million?* InformationWeek (July 25, 2011), *available at* http://www.informationweek.com/thebrainyard/news/industry_analysis/231002459.

[10] For an example of the relative ease with which competitors can find key information about another company through social media, including information on your potential and current clients and key staffers, *see* Mario Zelaya, *Spying On Competition Using Social Media*, (Aug. 8, 2010), http://sixrevisions.com/project-management/spying-on-competition-using-social-media/.

[11] Rather than an outright bar of social media, some companies may prefer a "Big Brother" approach where they monitor their employees' Facebook, MySpace, and Twitter usage. *See* Elefant, *supra* 5, at p.17.

[12] Pinguelo & Muller, *supra* note 4, at p.125 (citing Andreas Cremer, *Porsche Blocks Staff Access to Facebook as Espionage Shield, WiWo Reports*, Bloomberg News, (Oct. 9, 2010)..

[13] *See* Elefant, *supra* note 5, at p.51. For an example of a model social media policy, *see id.* at p. 54-55; *see also* Beth Citron, *Why companies can no longer ignore social networking websites*, N.Y. Employment L. Letter (2009).

[14] *See, e.g.*, Nurul Nuha Abdul Molok, Shanton Chang & Atif Ahmad, *Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats*, 8th Australian Information Security Management Conference. (Nov. 30, 2010).

[15] Although protecting trade secrets and confidential corporate information from nefarious social media uses is the main concern of this article, companies should also be aware of government regulators' growing interest in social media. *See* Kenneth N. Rashbaum, Esq., *Social Media Under The Privacy Microscope*, PM360 (Oct. 2010); *see also* David J. Goldstone & Daniel B. Reagan, *Social Networking, Mobile Devices and the Cloud: The Newest Frontiers of Privacy Law*, The Metropolitan Corp. Counsel, p. 5 (Aug. 2011); Charlie Savage, *Federal Contractor Monitored Social Network Sites*, N.Y. Times, Jan. 13, 2012, *available at* http://www.nytimes.com/2012/01/14/us/federal-security-program-monitored-public-opinion.html.

[16] Former U.S. Representative Anthony Weiner was forced to resign his seat in Congress after private photos he sent to Twitter followers became public. Emma Mustich, *A Weinergate Timeline*, Salon.com, (Jun. 1, 2011), http://www.salon.com/news/politics/war_room/2011/06/01/weinergate_timeline; *see also* Matt Friedman, *Blogger has mixed feelings about toppling Cumberland County politician with nude photos*, Star Ledger (Aug. 7, 2011), *available at* http://www.nj.com/news/index.ssf/2011/08/activist_has_mixed_feelings_ab.html.

[17] Commentators have noted that sensitive photos and videos made available through unrestricted albums on social media sites may cause embarrassment to the employee and the organization. Molok, Chang & Ahmad, *supra* note 15.

[18] *See* Christina Warren, *10 People Who Lost Jobs Over Social Media Mistakes*, Mashable (Jun. 16, 2011), http://mashable.com/2011/06/16/weinergate-social-media-job-loss/#17015Gilbert-Gottfried-Former-Aflac-Spokesman.

[19] Google+ has adopted a system aimed at reducing the inadvertent sharing of information with wide audiences, as the social network allows users to build "circles of audiences" for their personal content, promising to let users "share just the right things with just the right people." Geoffrey A. Fowler & Amir Efrati, *Facebook Revamps Privacy Controls*, Wall Street J., B6 (Aug. 24, 2011).

[20] *See* The Federal Bureau of Investigation, *Spear Phishers: Angling to Steal Your Financial Info* (April 1, 2009), http://www.fbi.gov/news/stories/2009/april/spearphishing_040109/.

[21] Molok, Chang & Atif, *supra* note 15, at 74.

[22] *See* Martha Neil, *Malicious Phishing Scheme Targets WilmerHale*, ABA Journal, (Jan. 5, 2011), http://www.abajournal.com/news/article/malicious_phishing_scheme_targets_wilmerhale_dont_open_subpoena_e-mail_law_.

[23] Fernando M. Pinguelo & Bradford W. Muller, *Epsilon Breach: Small Businesses Who Get "Hacked" Must Act – Now,* Bloomberg Law Reports® - Privacy & Information Law, Vol. 4, No. 6 (June 6,2011).

[24] *See infra.* Pinguelo, *et al. New Age Technology: Brazilian and U.S. Courts "Scraping" the Surface of Legal Boundaries of Internet Use* (offering a comprehensive survey of recent U.S. and Brazilian courts' decisions addressing the legal boundaries of extracting information from public websites).

[25] Dan Eggen, *Web a Useful Tool in Dirty-Tricks Campaign*, The Wash. Post, (Mar. 7, 2011).

[26] "Hacktivism refers to politically motivated attacks on publicly accessible Web pages or email servers. These groups and individuals overload email servers and hack into Web sites to send a political message." U.S. Gov't Accountability Office, Statement for the Record to the Subcommittee on Terrorism and Homeland Security, Sen., Cybersecurity: Continued Efforts are Needed to Protect Information Systems from Evolving Threats 4 (2009), *available at* http://www.defense.gov/home/features/2010/0410_cybersec/docs/d10230t.pdf; *see also* Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. Cal. Interdisc. L.J. 63, 80 (2001), *available at* http://wwwbcf.usc.edu/~idjlaw/PDF/11-1/11-1%20Rustad.pdf.

[27] Anonymous is a hacktivist group who made headlines when it engaged in coordinated attacks on major companies that had withdrawn their services from WikiLeaks. Scott Shuey, "Old School Hacking and Our Stupidity," Gulf News (Feb. 19, 2011) ; *see also* Jana Winter, *16 Suspected 'Anonymous' Hackers Arrested in Nationwide Sweep*, Foxnews.com (July 19, 2011), http://www.foxnews.com/scitech/2011/07/19/exclusive-fbi-search-warrants-nationwide-hunt-anonymous/.

[28] Eggen, *supra* note 25; *see* Nate Anderson, *How one man tracked down Anonymous – and paid a heavy price*, ars technica, http://arstechnica.com/tech-policy/news/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price.ars.

[29] Eggen, *supra* note 25; *see* Fahmida Y. Rashid, *HBGary Federal CEO Aaron Barr Quits Due to Anonymous Attack*, eweek.com, http://www.eweek.com/c/a/Security/HBGary-Federal-CEO-Aaron-Barr-Quits-Due-to-Anonymous-Attack-325042 (Mar. 1, 2011).

[30] Eggen, *supra* note 25.

[31] *Id.*

[32] Vikki Chowney, *Porsche risks alienating its biggest group of social media advocates*, New Media Age Online (Oct. 18, 2010), *available at* http://www.nma.co.uk/opinion/porsche-risks-alienating-its-biggest-group-of-social-media-advocates/3019446.article.

[33] Cremer, *supra* note 13.

[34] Chowney, *supra* note 32.

[35] Chowney notes that Porsche's policy likely created negativity amongst employees and led to detrimental comments being posted by staff on Facebook. *Id.* This risk has not prevented a state court from adopting a strong social media policy that bars court employees from posting "intoxicated" pictures of themselves, making negative comments about co-workers, and from using hand-held devices to access social media while at work. Associated Press, *Indiana court employees face limit to social networking*, Daily Herald (Sept. 3, 2011), *available at* http://www.dailyherald.com/article/20110903/news/709039867.

[36] Michael J. Eastman, *A Survey of Social Media Issues Before the NLRB*, U.S. Chamber of Commerce, 1 (Aug. 5, 2011), *available at* http://www.uschamber.com/sites/default/files/reports/NLRB%20Social%20Media%20Survey.pdf.

[37] *See* Press Release, "National Labor Relations Board, Administrative Law Judge finds New York nonprofit unlawfully discharged employees following Facebook posts" (Sept. 7, 2011), *available at* https://www.nlrb.gov/news/administrative-law-judge-finds-new-york-nonprofit-unlawfully-discharged-employees-following-fac; *but see Doninger v. Niehoff*, 642 F.3d 334 (2d Cir. 2011) (dealing with intersection of student's First Amendment rights and off-campus social media usage).

[38] Molok, Chang & Atif, *supra* note 15, at 75 (noting that employee security education, training, and awareness should be a cornerstone of any company's social media policy).

[39] *See Hertz v. The Luzenac Group*, 576 F.3d 1103 (10th Cir. 2009).

[40] Daniel Ornstein, *Employee Misuse of Social Networking Found at 43 Percent of Businesses, According to Proskauer International Labor & Employment Group Survey*, The Metropolitan Corp. Counsel, p. 6 (Aug. 2011).

[41] Jason Ray, *Controlling Data in a Social Media World*, The Metropolitan Corp. Counsel, p. 7 (Aug. 2011).

[42] *See, e.g, Baer v. WikiLeaks*, 535 F. Supp. 2d 980 (N.D. Cal. 2008) (case involving a disgruntled employee who posted confidential information on the WikiLeaks website).