Client Alert

pillsbury

Litigation

Employment

Communications

Privacy, Data Security & Information Use

Social Media, Entertainment & Technology

October 16, 2012

Drawing the Line Online: Employers' Rights to Employees' Social Media Accounts

By Julia E. Judish, Thomas N. Makris, and Amy L. Pierce

With the unprecedented popularity of social media, employees have increasingly used LinkedIn and other online forums to network for business and social purposes. When the line between personal and business use is blurred, litigation may ensue. A federal court recently ruled that an employer did not violate federal computer hacking laws by accessing and altering its recently departed CEO's LinkedIn account, but that the former CEO could proceed to trial on her state law misappropriation claim. In addition, California, Illinois, and Massachusetts recently joined Maryland in enacting laws prohibiting the practice of requesting access to prospective employees' password-protected social media accounts.

In *Eagle v. Morgan*, *et al*., Linda Eagle, former CEO of Edcomm, Inc. ("Edcomm"), filed a complaint in U.S. District Court in Pennsylvania alleging that Edcomm hijacked her LinkedIn social media account after she was terminated. While Eagle was CEO of Edcomm, she established a LinkedIn account that she used to promote Edcomm's banking education services, to foster her reputation as a businesswoman, to reconnect with family, friends and colleagues, and to build social and professional relationships. Edcomm employees assisted Eagle in maintaining her LinkedIn account and had access to her password. Edcomm encouraged all employees to participate in LinkedIn and contended that when an employee left the company, Edcomm would effectively "own" the LinkedIn account and could "mine" the information and incoming traffic.

After Eagle was terminated, Edcomm, using Eagle's LinkedIn password, accessed her account and changed the password so that Eagle could no longer access the account, and then changed the account profile to display Eagle's successor's name and photograph, although Eagle's honors and awards, recommendations, and connections were not deleted. Eagle contended that Edcomm's actions violated the federal Computer Fraud and Abuse Act ("CFAA"), Section 43(a) of the Lanham Act, and numerous state and common laws. In an October 4, 2012 ruling on the company's summary judgment motion, U.S. District Judge Ronald L. Buckwalter dismissed Eagle's CFAA and Lanham Act claims against Edcomm but held that Eagle had the right to a trial on whether Edcomm had violated state misappropriation law and other state laws.

The *Eagle case* is just one example of how the absence of a clear and carefully drafted social media policy can lead to protracted and expensive litigation. This area of law appears to be garnering increasing attention on the legislative front as well as the judicial front, as three more states recently enacted laws prohibiting employers from requiring, or in some cases even requesting, access to prospective employees' social media accounts. The attached chart includes more detail about the California, Illinois, Massachusetts and Maryland laws and the provisions of similar legislation pending in the various states and in the U.S. Congress.

A common theme connects the Eagle case with the recent password access legislation: the importance of defining the lines of ownership and demarcating the boundary between the professional and the personal. If Edcomm, for example, had established a LinkedIn account for its CEO's use and had asserted its property interest in the account at the outset of the employment relationship, Edcomm's CEO would have had no reasonable expectation of ownership in it. Under that scenario, Edcomm likely would not be facing trial on a misappropriation claim. Similarly, the social media password legislation definitively declares that employers and prospective employers have no right to access the social media accounts that applicants and employees have established for their personal use.

In addition, as explained in our recent Client Alert on enforcement actions under the National Labor Relations Act in connection with employer discipline of employees for social media postings, employer responses to employee use of social media can also result in government agency action against employers. These developments all point to the same message: employers wishing to avoid legal risk should be proactive in implementing well-defined policies and procedures relating to the LinkedIn, Pinterest, Twitter, Facebook and other social networking and media accounts of prospective, current and former employees, including clearly identifying rights to those accounts when the employee leaves the company.

Click here to read our prior Client Alert, First NLRB Decisions on Social Media Give Employers Cause to Update Policies, Practices, issued 10/10/2012.

Click here to read our prior Client Alert, Employ Me, Don't Friend Me ~ Privacy in the Age of Facebook, issued 6/11/2012.

If you have questions please contact the Pillsbury attorney with whom you regularly work, or the authors:

Julia E. Judish (bio)
Washington D.C.
+1.202.663.9266
julia.judish@pillsburylaw.com

Thomas N. Makris (bio)
Sacramento
+1.916.329.4734
tmakris@pillsburylaw.com

Amy L. Pierce (bio)
Sacramento
+1.916.329.4765
amy.pierce@pillsburylaw.com

James G. Gatto (bio)
Northern Virginia
+1.703.770.7754
james.gatto@pillsburylaw.com

STATE AND FEDERAL SOCIAL MEDIA BILLS (As of October 15, 2012)

					Applies To[1]		Prohibits[2] Requesting[3] or Requiring*[4]		
	Bill No.	**Act, Statutory Reference**	**Signed Into Law**	**Proposed or Actual Effective Date**	**Employers**	**Educational Institutions[5]**	**Confirmation of Social Media Account(s)[6]**	**Username(s)/ Password(s)**	**Access to Social Media Account(s)**
CA	**SB 1349**	**Social Media Privacy Act, Cal. Ed. Code § 99120, *et seq.***	**09/27/12**	**01/01/13**		√	√	√	√
CA	**AB 1844**	**Cal. Lab. Code § 980, *et seq*.**	**09/27/12**	**01/01/13**	√[7]		√	√	√
DE	HB 308	Workplace Privacy Act, Del. Code tit. 19, § 710		When Signed Into Law	√[8]			√	√[9]
IL	**HB 3782**	**Right to Privacy in the Workplace Act, 820 ILCS § 55/10**	**08/01/12**	**01/01/13**	√			√	√
MA	**Dkt. No. 04323**	**Mass. Gen. Laws ch. 149, § 189**	**08/01/12**	**01/01/13**	√			√	√
MD	**SB 433**	**Md. Code, Lab. & Empl. § 3-712**	**05/02/12**	**10/01/12**	√			√	√
MD	**HB 964**	**Md. Code, Lab. & Empl. § 3-712**	**05/02/12**	**10/01/12**	√			√	√
MI	HB 5523	Social Network Account Privacy Act			√	√		√	√
MN	HF 2963 HF 2982 SF 2565	Minn. Stat. § 181.53		Day After Signed Into Law	√			√*	√*
MO	HB 2060	Mo. Rev. Stat. § 285.600			√			√	√
NJ	AB 2878				√		√	√*	√*
NY	SB 6938	N.Y. Lab. Law § 215-d		When Signed Into Law	√			√*	√*
OH	SB 351	OH Rev. Code § 4112.02, *et seq.*			√			√	√
SC	HB 5105	S.C. Code § 41-1-187		When Signed Into Law	√			√	√
WA	SB 6637	Wash. Rev. Code § 49.44			√			√*	√*
FED LAW	HR 5050	Social Networking Online Protection Act			√	√		√	√
FED LAW	HR 5684	Password Protection Act of 2012, 18 U.S.C. § 1030			√			√	√
FED LAW	SB 3074	Password Protection Act of 2012, 18 U.S.C. § 1030			√			√	√

[1] Most of the bills govern current and prospective employees and/or students.
[2] Some states' bills permit employers to bar employees from accessing social networking sites during work hours. *See, e.g.*, DE HB 308. Others permit employers to *request*, but not *require*, access to social media accounts in connection with formal investigations.
[3] California SB 1349 prohibits requiring or "formally request[ing] in writing" a social media account username and account password.
[4] Most of the bills expressly prohibit requiring and requesting the current or prospective employee or student to provide the employer or institution with social media account information. A √* indicates that the bill only expressly prohibits requiring this information.
[5] Each state's bill that regulates educational institutions refers to the particular institution(s) intended to be governed by the new law.
[6] Several states define terms, including the term social media account.
[7] The Labor Commissioner is not required to investigate or determine any violation of this act.
[8] Delaware HB 308 would not apply to any person from any state, local or municipal law enforcement agency or organization as listed in § 9200(b), Del. Code tit. 11, or prohibit the Department of Corrections from requesting and achieving access to an employee's social networking site for purposes of monitoring that employee's compliance with the Department of Corrections' policies and procedures.
[9] Delaware HB 308 would also prohibit an employer from accessing an employee's or applicant's social networking site profile or account indirectly through any other person who is a social networking contact of the employee or applicant.