Employee Privacy for Personal Social Media Accounts

By Andrew B. Stockment

On July 1, 2015, Virginia Code § 40.1-28.7:5 ("Social media accounts of current and prospective employees") became effective, which applies to all government and private employers, regardless of the organization's size or revenue. Notably, the new law does not create a private cause of action.

OVERVIEW

Under the statute, "*social media account*" is very broadly defined to mean "a personal account with an electronic medium or service where users may create, share, or view user-generated content, including, without limitation, videos, photographs, blogs, podcasts, messages, emails, or website profiles or locations," but excluding "an account (i) opened by an employee at the request of an employer; (ii) provided to an employee by an employer such as the employer's email account or other software program owned or operated exclusively by an employer; (iii) set up by an employee on behalf of an employer; or (iv) set up by an employee to impersonate an employer through the use of the employer's name, logos, or trademarks." Thus, "social media account" means virtually any personal e-mail accounts and accounts associated with traditional social media (e.g., Facebook, Twitter, YouTube, Google+, LinkedIn), cloud storage services (e.g., Dropbox, Box, Google Drive, OneDrive, SpiderOak), photo sharing services (e.g., Flickr, Google Photos), online dating websites, message boards and other similar sites (e.g., Reddit), and many others. (It is also conceivable that a court could interpret "electronic medium" to encompass *devices*, such as an employee's smartphone.)

> 'Social media account' means virtually any personal e-mail accounts and accounts associated with traditional social media…, cloud storage services…, photo sharing services…, online dating websites, message boards and other similar sites…, and many others.'

The statute prohibits an employer from requiring current or prospective employees to:

1. Disclose the username and password to the current or prospective employee's social media account; or
2. Add an employee, supervisor, or administrator to the list of contacts associated with the current or prospective employee's social media account.

Va. Code § 40.1-28.7:5(B).

In addition, "[i]f an employer inadvertently receives an employee's username and password to, or other login information associated with, the employee's social media account through the use of an electronic device provided to the employee by the employer or a program that monitors an employer's network, the employer shall not be liable for having the information but shall not use the information to gain access to an employee's social media account." Va. Code § 40.1-28.7:5(C).

The statute further prohibits an employer from (1) taking action against or threatening to discharge, disciplining, or otherwise penalizing a current employee for exercising his rights under the statute, or (2) failing or refusing to hire a prospective employee for exercising his rights under the statute, but the law does not prohibit an employer from viewing publicly available information. Va. Code § 40.1-28.7:5(D)-(E).

EXCEPTIONS

However, the statute includes two exceptions, one of which may largely undercut the protections the new law might seem to offer for employees. First, the statute does not prevent "an employer from complying with the requirements of federal, state, or local laws, rules, or regulations or the rules or regulations of self-regulatory organizations." Va. Code § 40.1-28.7:5(F)(1). Second, and more significantly, the statute provides that: "Nothing in this section: . . . [a]ffects an employer's existing rights or obligations to request an employee to disclose his username and password for the purpose of accessing a social media account if the employee's social media account activity is reasonably believed to be relevant to a formal investigation or related proceeding by the employer of allegations of an employee's violation of federal, state, or local laws or regulations or of the employer's written policies. If an employer exercises its rights under this subdivision, the employee's username and password shall only be used for the purpose of the formal investigation or a related proceeding." Va. Code § 40.1-28.7:5(F)(2).

Thus, the second exception in the statute would potentially allow an employer to exercise its "existing rights" (whatever those may be) to require an employee to "disclose his username and password . . . if the employee's social media account activity is reasonably believed to be relevant to a formal investigation or related proceeding by the employer of an employee's violation of . . . the employer's written policies." That exception would seem to give employers broad latitude to require access to employees' personal accounts to investigate violations of the employers' written policies.

> '[T]he terms of use for most online service providers … both (1) prohibit users from sharing their passwords or allowing others to access their accounts and also (2) prohibit users from requesting passwords or accessing accounts belonging to other users.'

VIOLATING TERMS OF USE: BREACH OF CONTRACT

It is worth noting, however, that the terms of use for most online service providers

(such as Facebook) both (1) prohibit users from sharing their passwords or allowing others to access their accounts and also (2) prohibit users from requesting passwords or accessing accounts belonging to other users. Consequently, an employer who requires an employee to disclose his username and password is both (1) requiring the employee to breach the contract with the provider of the social media account, and (2) breaching the contract it entered into with the provider if the employer also has an account with the same provider.

VIOLATING TERMS OF USE: CRIMINAL OFFENSE?

In addition, using another person's password to access a third party's Internet-connected computer in violation of that third party's terms of service (or other computer use policy) could be construed as a criminal offense under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, particularly in jurisdictions that interpret the CFAA broadly (namely, the First, Fifth, Seventh, and Eleventh Circuits). It is uncertain how jurisdictions that interpret the CFAA narrowly (the Ninth Circuit and the Fourth Circuit) will construe these actions.

The Ninth Circuit, which interprets the CFAA similarly to the Fourth Circuit, heard oral arguments on October 20, 2015, in *United States v. Nosal*, Nos. 14-10037, 14-10275 (9th Cir.) (hereinafter *Nosal II*), in which one of the issues before the court is whether the use of another person's password, with that person's consent, but in violation of a company's computer use policy, constitutes accessing a computer "without authorization" under the CFAA. In *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (en banc) (hereinafter *Nosal I*), the Ninth Circuit previously held that "the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions." *Id*. In *Nosal I*, the court touched on the issue of password sharing and observed that "Facebook makes it a violation of the terms of service to let anyone log into your account . . . . but few imagine they might be marched off to federal prison for doing so." *Nosal I* at 861 (citations omitted). In my opinion, the CFAA should not be construed to

> '[U]sing another person's password to access a third party's Internet-connected computer in violation of that third party's terms of service…could be construed as a criminal offense under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030….'

create criminal liability for password sharing (and use of such shared passwords) in violation of an agreement between private parties, which appears to be supported by the Ninth Circuit's opinion in *Nosal I*. It remains to be seen how the Ninth Circuit will address the issue of password sharing in *Nosal II*. It is likely that the Fourth Circuit would reach a conclusion similar to that of the Ninth Circuit. Nevertheless, businesses should be cautious about engaging in conduct that could give rise to criminal liability. ■

Save the Date: November 18

Get to Know the VBA!

Save the date, Wednesday, November 18, 2015, for the "Get to Know the VBA" happy hour with Supreme Court of Virginia Justice Jane Marum Roush and Fairfax County Circuit Court Judge Daniel E. Ortiz. From 5:30pm-7:30pm Justice Roush and Judge Ortiz will engage in an information discussion about the benefits of VBA membership at Auld Shebeen, 3971 Chain Bridge Road (Downstairs Cellar) Fairfax, VA 22030. Beer, wine and hors d'oeuvres will be provided by the VBA Young Lawyers Division. Come out to network and get to know the VBA with two of Virginia's finest from the bench! Please RSVP to elizabethfoskey@vba.org.

Support VBA Foundation

The VBA Foundation funds numerous programs, including the ***Ask A Lawyer Project***, the ***Pro Bono Hotlines***, the ***Model Judiciary Project***, the ***Veterans Issues Task Force***, and ***Regional Mentoring Programs***. To donate or to learn more, visit: **vba.org/foundation**.

Andrew B. Stockment
Associate, Lenhart Pettit (Charlottesville)

Practice Areas: Intellectual Property and Technology Law, Business Law, and Securities and Private Equity
Law School: University of Virginia School of Law (2009)
VBA Leadership: YLD Executive Committee (2014 – Present), Intellectual Property and Information Technology Law Section Council (YLD Representative, 2012 – Present), Law Practice Management Division Executive Council (YLD Representative, 2014 – Present), ABA Awards of Achievement Committee (Co-Chair, 2015 – Present), *Opening Statement* (Editor-in-Chief, 2012 – Present), YLD Communications/Publicity Committee (Chair, 2012 – Present)
Awards: Super Lawyers Rising Stars (2013 – 2015), VBA YLD Emerson G. Spies Award (2012)
Bio: Andrew was a software engineer before becoming an attorney, and he has been a lifelong technology and innovation enthusiast (including a particular interest in data security and privacy). When he is not practicing law or working on bar projects, Andrew and his wife Martha enjoy hiking and watching U.Va. Men's Basketball. Andrew's other articles and projects are available at: www.andrewstockment.com.

Contact Info: abs@lplaw.com or 434.220.9386 **Twitter:** @AndrewStockment