December 4, 2012

VIA ELECTRONIC AND FIRST CLASS MAIL

Secretary Gary D. Maynard
Maryland Department of Public Safety
And Correctional Services
300 East Joppa Road
Suite 1000
Towson, Maryland 21286

AMERICAN CIVIL LIBERTIES UNION OF MARYLAND FOUNDATION
3600 CLIPPER MILL ROAD
BALTIMORE, MD 21211
T/410-889-8555
F/410-366-7838

6930 CARROLL AVENUE
TAKOMA PARK, MD 20912
T/240-274-5295

WWW.ACLU-MD.ORG

Dear Secretary Maynard:

We write on behalf of the American Federation of State, County and Municipal Employees (AFSCME) and the American Civil Liberties Union of Maryland (ACLU), to inquire about measures being taken by the Department of Public Safety and Correctional Services to comply with Maryland's first-in-the-nation social media privacy law.[1] In light of this path-breaking new law, as well as Attorney General Douglas Gansler's initiative on internet privacy as President of the National Association of Attorneys General,[2] we expect that all Maryland agencies are reevaluating their policies on social media privacy to ensure compliance with best practices and all legal requirements. And given the role the Division of Corrections played in catalyzing action by the General Assembly to enhance social media privacy protections, we are particularly interested in learning about policy changes being made at the DOC pursuant to the law.

You probably recall AFSCME member Robert Collins's 2010 complaint that the DOC required him to provide social media usernames and passwords during a background check conducted as part of his recertification following medical leave. After Mr. Collins and the ACLU objected to this practice, you ordered a suspension of the policy during an internal review, then later a policy refinement. Rather than specifically seeking login information as had occurred in the past, the reformed policy asked applicants for employment and recertification to "voluntarily" share

---

[1] S.B. 433, 2012 Leg., 430th Sess. (Md. 2012), to be enacted as §3-712(B)(1), *available at* http://mlis.state.md.us/2012rs/chapters_noln/Ch_233_sb0433T.pdf. The law was signed by Governor O'Malley on May 2 and took effect on October 1.

[2] Attorney General Gansler has been speaking around the country about his initiative, "Privacy in the Digital Age," and will hold a national conference on the subject in April of 2013. *See, e.g.*, http://www.naag.org/privacy-in-the-digital-age.php.

their social media content with interviewing officials.[3] As discussed below, however, the practice of peering over applicants' shoulders while they log into social media accounts – so-called "shoulder surfing" -- conflicts with the privacy protections put into place by the new Maryland law. Accordingly, we would like to know if further changes have been made to the DOC policy in response to the new law, and what those changes are. If no changes have yet been made, we urge you revisit and reform the DOC policy in order to bring it into compliance with the law.

Scope and Purposes of the New Maryland Law

Maryland's Social Media Privacy Law – which was sparked by the Robert Collins controversy[4] – passed unanimously in the Senate and by a significant margin in the House, garnering widespread national attention.[5] This law prohibits employers in Maryland from asking *or* requiring current and potential employees "to disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device."[6] As is evident from the language of the statute itself, as well as testimony provided at the hearing, the law prohibits employers both from requesting user names and passwords so they may directly open and review employee accounts, and also from asking applicants to use "other means" to give them access to these accounts. The point of the law, as the sponsors discussed in promoting it, is to prevent the dissemination to employers of any

AMERICAN CIVIL
LIBERTIES UNION OF
MARYLAND

---

[3] That is, employees and applicants were asked to voluntarily enter their usernames and passwords into a computer during the interview so the interviewer could review their social media content. Written notice was given that the process was not mandatory, and applicants were asked to initial a consent form if they agreed to the sharing.

[4] *See, e.g.*, AFSCME testimony, March 7, 2012, ("The genesis of this bill stems from a case involving an AFSCME MD member who felt coerced into giving his personal email and social network passwords during a job interview."); Ben Giles, *Maryland bans employers from asking for Facebook passwords*, Washington Examiner (May 2, 2012), http://washingtonexaminer.com/maryland-bans-employers-from-asking-for-facebook-passwords/article/564481.

[5] *See, e.g.,* Associated Press, *Proposed laws would forbid employers from asking for job seekers' social media passwords,* http://www.foxnews.com/politics/2012/03/20/proposed-laws-would-forbid-employers-from-asking-for-job-seekers-social-media/#ixzz2BeyPok39 (March 20, 2012); Larry Magid, *Maryland Passes Bill To Ban Employers From Requesting Facebook Passwords*, Forbes (April 10, 2012, 4:04 PM), http://www.forbes.com/sites/larrymagid/2012/04/10/maryland-passes-bill-to-ban-employers-requesting-facebook-passwords/; Kevin Rector, *Social-Media Privacy Law Passes; Curb on Employers Needs O'Malley's Signature*, Baltimore Sun, April 11, 2012, at A1, *available at* http://www.baltimoresun.com/news/maryland/politics/bs-md-privacy-law-20120410,0,4565780.story; Michelle Maltais, *Maryland Passes Bill Banning Employers From Seeking Online Passwords*, Los Angeles Times (April 10, 2012), http://articles.latimes.com/2012/apr/10/business/la-fi-tn-facebook-password-employers-maryland-bill-20120410

[6] *Id.*

information intended to be kept private by employees and applicants – through whatever means are employed to access this private information.

Those testifying about the reach of the bill during the legislative process clearly articulated that the law was intended to protect social media content itself, not merely to protect login information. After all, it is the private photos, emails, and posts that require protection, while usernames and passwords merely serve as gatekeepers to such information. Thus, in introducing the law, Senate Sponsor Ron Young specifically stated that asking job applicants to disclose their personal writings on social media sites "is a clear violation of the 1st and 4th amendments. … Their accounts and what they do personally should remain private."[7] Sen. Young further stated: "Asking for a password or access to what someone does on their internet webpage is the same as asking if you can tape phone calls or monitor their mail. It's a private matter under the Constitution and I think it should be protected." Additionally, in describing the bill's origins in connection to the Collins incident, and the continuing need for reforms at the Maryland DOC, ACLU Legislative Director Melissa Goemann testified that while the DOC "no longer demands user names and passwords, they do in fact ask applicants to type in their user name and passwords, so that they can then view their page in front of them. So, they still are invading people's privacy."[8] Likewise, AFSCME representative Michelle Lewis testified that the bill goes further than simply barring password collection, as it also protects individuals from the practice of employers looking over their shoulder while they are typing their passwords into their personal social media accounts.[9]

AMERICAN CIVIL
LIBERTIES UNION OF
MARYLAND

Maryland's Social Media Privacy law is at the vanguard of a movement to protect citizens' private information. Similar efforts, some modeled after Maryland's law, have gained momentum with the passage of laws in California, Illinois, and Delaware. These laws spring from the same spirit and intent to protect the privacy of social media users' online communications, and are not limited to mere password protections. Also sparked by the Collins case and positive reaction to the Maryland social media bill, United States Senators Richard Blumenthal (D-CT) and Charles E. Schumer (D-NY) have called on the U.S. Department of Justice and the Equal Employment Opportunity Commission to investigate online privacy violations in the employment context. Importantly, their March 25, 2012 letter emphasizes the intrinsically private nature of the communications at issue as much as it does the protection of the usernames and passwords that shield them: "With few exceptions, employers do not have the need or the right to demand access to applicants' private, password-protected information. Employers have no right to ask job applicants for their house keys or to read their diaries – why should they be able to ask them for their Facebook passwords and gain unwarranted access to a trove of private

---

[7] User Name and Password Privacy Protections and Exclusions: Hearing on S.B. 433 Before the S. Comm. on Fin., 2012 Leg., 430th Sess. (Md. 2012) (statement of Sen. Ronald Young, Sponsor).

[8] *Id.* (statement of Melissa Goemann, legislative director of the ACLU of Maryland).

[9] *Id.* (statement of Michelle Lewis, representative of AFSCME).

information about what we like, what messages we send to people, or who we are friends with?" The Senators' comments suggest a common sense rule that employers must respect the private information itself, as that is what usernames and passwords seek to protect.

A policy like the DOC policy that asks applicants to let the employer view their private social media content presents a serious invasion of privacy for those individuals, as well as for all others who communicate with them electronically via social media. Coerced review of private posts, photos, emails, and instant messages overrides the privacy protections users have erected and thus violates their reasonable expectations of privacy in these communications. When an employer asks an employee or applicant to share private social media material, the situation is an inherently coercive one, placing pressure on the applicant to accede to this privacy violation or risk being perceived as someone with something to hide. As one legal commentator noted recently, "When employers ask job applicants for their *consent* to such access, applicants are presented with two unpleasant choices: (1) sacrifice privacy and expose private and possibly embarrassing information, or (2) lose a job opportunity in a difficult labor market."[10] Likewise, Senate Sponsor Ron Young has called employer requests for social media access a "subtle threat." He told the Daily Record, "If you apply for a job and they ask you for this information … you're thinking, 'If I don't give it to them, I'm not going to get the job.' It's a form of intimidation." [11] Any "consent" given thus cannot be truly voluntary.

AMERICAN CIVIL
LIBERTIES UNION OF
MARYLAND

While DOC has previously taken the position that its practice of requesting consent to view applicants' social media content is not coercive, and that no adverse actions are taken against those who decline access requests, the legislature disagreed with this assessment. Based on its view of the inherent coerciveness of such inquiries, the General Assembly banned even *requests* for access to social media accounts. Accordingly, the DOC must reform its practices in order to come into compliance with Maryland's law.

Job Applicants Cannot Properly Consent to Privacy Violations for Third Parties

Even if the legislature had accepted the DOC position that consent to social media account review could be validly obtained, and had not expressly prohibited access requests, there would remain a serious threat to the privacy of third parties who interact with the applicants via social media. These third parties are offered no opportunity to object to the intrusion, yet their private electronic correspondence with the applicant, their photographs, and postings are exposed to scrutiny, just as are the applicant's communications. Such a practice clearly is problematic.

---

[10] Daniel I. Prywes, *Should Employers Ask Job Applicants or Employees for Their Social-Media Passwords?*, BNA Insights, July 17, 2012.

[11] Mike Bock and Josh Cooper, *Legislature tackling social media privacy issues*, The Daily Record (Feb. 27, 2012), http://thedailyrecord.com/2012/02/27/legislature-tackling-social-media-privacy-issues/.

Indeed, Facebook policy condemns this type of backdoor privacy violation. Facebook's Terms of Use expressly prohibit third party access to the private information and communications found within Facebook, and do not limit its prohibition to disclosure of logon credentials. Facebook's Statement of Rights and Responsibilities states, "You will not share your password (…), let anyone else access your account, or do anything else that might jeopardize the security of your account."[12] Erin Egan, Facebook's Chief Privacy Officer, has threatened legal action against violators. Egan stated on March 23, 2012, "If you are a Facebook user, you should never have to share your password, let anyone access your account, or do anything that might jeopardize the security of your account or violate the privacy of your friends."[13] DOC's revised policy induces employees and applicants to compromise third party privacy and to violate Facebook user policy.

AMERICAN CIVIL
LIBERTIES UNION OF
MARYLAND

For all of these reasons, we ask that you let us know of any changes you have made to the DOC policy on social media privacy since 2011. If you have not yet made any changes to the policy we strongly urge you to revisit the DOC policy and to reform your policy to bring it into compliance with Maryland's new Social Media Privacy Law. We very much appreciate your attention to this matter.

Sincerely,

Deborah A. Jeon
Legal Director
ACLU of Maryland

Ronald E. Barillas
Assistant Director
AFSCME Maryland

cc: Senator Ronald Young
Secretary of State John McDonough
Stuart M. Nathan, Esq.
Mr. Patrick Moran, Director, AFSCME Maryland
Mr. Robert Collins

---

[12] Facebook, *Statement of Rights and Responsibilities*, http://www.facebook.com/legal/terms.

[13] Egan, *supra* note 10.