DEBORAH A. JEON
LEGAL DIRECTOR

January 25, 2011

VIA TELECOPY AND U.S. MAIL

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

Dear Secretary Maynard:

AMERICAN CIVIL
LIBERTIES UNION OF
MARYLAND FOUNDATION
3600 CLIPPER MILL ROAD
SUITE 350
BALTIMORE, MD 21211
T/410-889-8555
F/410-366-7838
WWW.ACLU-MD.ORG

I write on behalf of the American Civil Liberties Union of Maryland and Division of Correction (DOC) Officer Robert Collins, concerning DOC's blanket requirement that applicants for employment with the Division, as well as current employees undergoing recertification, provide the government with their social media account usernames and personal passwords for use in employee background checks. As discussed below, we believe the DOC policy constitutes a frightening and illegal invasion of privacy for DOC applicants and employees -- as well those who communicate with them electronically via social media.

Neither Officer Collins nor his Facebook "friends" deserve to have the government snooping about their private electronic communications. Login information gives the DOC access to communications that are intended to be private, such as personal email messages and wall postings viewable only by those selected individuals who have been granted access. For social media users who maintain private accounts, the DOC demand for login information is equivalent to demands that they produce all of their private correspondence and photographs for review, or permit the government to listen in on their personal telephone calls, as a condition of employment. Such demands would be unconscionable, and there is no basis for treating electronic communications differently. While employers may permissibly incorporate some limited review of public internet postings into their background investigation procedures, review of password-protected materials overrides the privacy protections users have erected and thus violates their reasonable expectations of privacy in these communications. Accordingly, we ask that you direct the Department immediately to cease this practice.

Facts Giving Rise to this Inquiry

Robert Collins was employed as a Corrections Supply Officer with the Maryland Department of Public Safety and Correctional Services, at Patuxent Institution, from July 2007 until he voluntarily took a personal leave in April of 2010. In his

position at Patuxent, Officer Collins was responsible for care and custody of inmates, ordering supplies, and running the commissary. After four months of leave, he sought to return to work last July. Because his job at Patuxent had been filled in his absence, Collins began the process of locating another position within the corrections system. In November, he was alerted that a comparable position was open at Maryland Correctional Institution at Jessup (MCIJ), and he submitted his name for that job.

As you know, DOC policy requires that corrections officers who have had a break in service undergo a recertification before returning to work at the Department. Recertification includes fingerprinting, a renewed background check and interview. Once the initial steps in this process had been completed, Officer Collins was called for an interview with a DOC investigator on December 1. After an uneventful beginning to the interview, Mr. Collins was asked if he uses any social media, and he replied that he uses Facebook. He was then directed to provide his username and password. He was taken aback by this demand, and asked why the Department needed that kind of information, since he maintains his Facebook account privately, with his settings designed to heighten privacy and limit viewing of his materials to those he has specifically authorized. The investigator said a blanket requirement that all interviewees provide social media login information is now a standard part of the DOC's process for hiring and recertification.[1] The reason, the investigator said, is to enable the government to review wall postings, email communications, photographs, and friend lists, in order to ensure that those employed as corrections officers are not engaged in illegal activity or affiliated with any gangs.

AMERICAN CIVIL
LIBERTIES UNION OF
MARYLAND

Officer Collins understood the investigator to be saying that he had no choice but to provide this information if he wanted to continue his employment with DOC. For this reason only, he gave the investigator his Facebook username and password. While Collins was sitting there, the investigator informed Officer Collins that he was logging into the account and reviewing Collins' materials (though the back of the computer faced Mr. Collins, so he could not see the screen.) Officer Collins asked how long the DOC would need the login information, and what would happen if he changed his password. The investigator said background checks can take a month or two, and that DOC would likely need the information to log into the account again during that time.

Legal Consequences of the DOC Policy

While we appreciate the DOC's need to ensure that applicants and employees are not engaged in illicit activity, here there is no basis whatsoever for the

[1]Valerie Tracey, a Personnel Officer in the Division's Centralized Hiring Unit, later confirmed to Officer Collins that this is DOC policy, when he telephoned the Division to inquire about the matter.

Department to suspect Officer Collins of gang involvement or illegal activity of any kind. As such, an intrusion upon his private, off-duty communications in this manner is unjustified and unacceptable. The DOC policy is illegal under the federal Stored Communications Act (SCA), 18 U.S.C. §§2701-11 and its state analog, Md. Courts & Jud. Proc. Art., §10-4A-01, *et seq*.[2] These laws were enacted to ensure the confidentiality of electronic communications, and make it illegal for an employer or anyone else to access stored electronic communications without valid authorization. Additionally, the DOC practice constitutes the common law tort of invasion of privacy,[3] and arguably chills employee speech and due process rights protected under the First and Fourteenth Amendments to the U.S. Constitution.[4]

AMERICAN CIVIL
LIBERTIES UNION OF
MARYLAND

[2]Section 2701 of the SCA makes it illegal to intentionally (1) access a facility through which an electronic communication service is provided, without valid authorization; or (2) exceed an authorization to access that facility, thereby obtaining an electronic communication while it is in electronic storage in such a system. 18 U.S.C. §2701(a)(1)-(2). The Maryland law establishes these same prohibitions, offering both criminal and civil penalties for violations.

[3]Under Maryland law, one form of the tort of Invasion of Privacy is defined as an intentional intrusion upon the solitude or seclusion of another *or of his private affairs* that would be highly offensive to a reasonable person. Md. Law Enc. Torts, 21 M.L.E. Torts §24; *Mitchell v. Baltimore Sun Co.,* 164 Md. App. 497, 883 A.2d 1008 (Md. App. 2005). As established by the outraged public reaction nationally when the City of Bozeman attempted to implement a policy like this, reasonable people find it highly offensive. *See infra,* n.5.

[4]In a different context factually, the National Labor Relations Board (NLRB) made headlines last November by issuing a complaint against a Connecticut company that fired an employee who criticized the company on Facebook, in violation of the company's social media policy. *E.g.,* "Feds: Woman Illegally Fired Over Facebook Remarks," available at: http://www.myfoxdc.com/dpp/news/offbeat/feds-woman-illegally-fired-over-facebook-remarks-110910?CMP=201011_emailshare; "Labor Board: Facebook Vent Against Supervisor Not Grounds for Firing," available at: http://www.cnn.com/2010/TECH/social.media/11/09/facebook.firing/index.html The NLRB maintains that both the firing and the social media policy itself violate employees' protected speech rights under the National Labor Relations Act. *See* NLRB Press Release, http://www.nlrb.gov/shared_files/Press%20Releases/2010/R-2794.pdf. While the Connecticut case involves the employee's right to engage in particular speech protected under the NLRA, it also addresses the limits that federal law places on employers' interference and monitoring of employees' social media use more generally, and thus is worthy of notice.

While the case law in this area is sparse, that is not because the DOC policy presents a close call legally, but because a blanket requirement that applicants and employees turn over social media login information as a part of certification is so outrageous and rare that few courts have been required to confront it. For example, when the City of Bozeman, Montana instituted a policy requiring job applicants to produce login information in 2009, a public outcry ensued nationally, resulting in a quick abandonment of the policy.[5]

Courts that have been required to address the issue have ruled that wall postings and email on Facebook and other social media sites are protected communications under the SCA, making efforts to access them without proper authorization illegal. *E.g., Crispin v. Christian Audigier, Inc.,* 717 F.Supp. 2d 965 (C.D. Cal. 2010) (Private, undeleted messages and wall postings on Facebook and MySpace are protected stored communications for purposes of the SCA, and thus were only subject to subpoena issued consistently with the strict requirements of the Act.) *See also Konop v. Hawaiian Airlines, Inc.,* 302 F.3d 868, 879-80 (9th Cir. 2002) (Claim was properly stated under the SCA where it was undisputed that communications on a password-protected website were in storage, and management accessed the site without proper authorization by obtaining the password from a third party non-user.) Here, there can be little question but that forced "authorization", such as that demanded of Mr. Collins, is not proper authorization under the SCA, given the disparate bargaining power of the employer and employee or applicant. *Pietrylo v. Hillstone Restaurant Group,* 29 IER Cases 1438, 2009 WL 312420 (D.N.J. 2009). Indeed, a federal jury in the *Pietrylo* case awarded punitive damages against an employer who violated the SCA when two of its managers accessed a "chat group" on an employee's MySpace account through coerced consent like this.

For these reasons, we ask that you rescind the DOC policy, and direct the Division immediately to discontinue demands for social media login information during background checks. Mr. Collins also asks that the login information obtained from him during his recertification and any notations made during viewing of his Facebook materials be destroyed.

AMERICAN CIVIL
LIBERTIES UNION OF
MARYLAND

---

[5] *See, e.g.,* "Want a job? Give Bozeman your Facebook, Google passwords," http://news.cnet.com/8301-13578_3-10268282-38.html and "Montana City Asks Job Applicants for Facebook Passwords," available at: http://www.huffingtonpost.com/2009/06/19/montana-city-asks-job-app_n_218152.html.

Please advise us, or have your attorney advise us, of your intentions in this regard at your earliest opportunity. Thank you for your prompt attention to this matter.

Sincerely,

Deborah A. Jeon
Legal Director

Cc: Stuart M. Nathan, Esq.

AMERICAN CIVIL
LIBERTIES UNION OF
MARYLAND