MELISSA GOEMANN
LEGISLATIVE DIRECTOR

AMERICAN CIVIL LIBERTIES UNION of MARYLAND

Testimony for the Senate Finance Committee
SB 971 - Labor and Employment – User Name and Password Privacy Protection

March 24, 2011

SUPPORT

AMERICAN CIVIL
LIBERTIES UNION
OF MARYLAND

MAIN OFFICE
& MAILING ADDRESS
3600 CLIPPER MILL ROAD
SUITE 350
BALTIMORE, MD 21211
T/410-889-8555
or 240-274-5295
F/410-366-7838

FIELD OFFICE
6930 CARROLL AVENUE
SUITE 610
TAKOMA PARK, MD 20912
T/240-274-5295

WWW.ACLU-MD.ORG

The ACLU of Maryland urges a favorable report on SB 971, a bill to prohibit employers from requiring employees or applicants to disclose their user names or passwords to Internet sites and Web-based accounts as a condition of employment.

This issue was recently brought to the attention of the ACLU of Maryland when Division of Corrections (DOC) Officer Robert Collins approached us because of his concern regarding 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. Robert Collins was an employee with the Maryland Department of Public Safety and Correctional Services when he took a voluntary leave of absence. Because his job had been filled in his absence, Mr. Collins applied for a comparable position within the corrections system when he returned. DOC policy required that corrections officers who had a break in service undergo a recertification before returning to work at the Department. During this process, Mr. Collins first learned that providing social media login information was now a standard part of the DOC's process for hiring and recertification and that he had to provide his Facebook username and password. He was also told that background checks can take a month or two, and that DOC would likely need his account information to log into the account again during that time. After the ACLU of Maryland objected to this practice, the DOC decided to suspend the practice for a period of 45 days, beginning on February 22nd, so that they could study it further. No final determination on this practice has been made yet by the DOC.

We believe that policies such as the DOC's that require employees or applicants to disclose user names and/or passwords to their private internet or web-based accounts constitute a frightening and illegal invasion of privacy for those applicants and employees -- as well those who communicate with them electronically via social media. We are concerned that other employers may also begin to require this information from job applicants without clear statutory language against it. 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. As such, we believe that policies such as this are 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*.[1] These laws were

[1] 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

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, such practices constitute the common law tort of invasion of privacy,[2] and arguably chill employee speech and due process rights protected under the First and Fourteenth Amendments to the U.S. Constitution.[3]

Job applicants and employees should not have to give up their first amendment rights as well as risk the security of their private information by being forced to divulge their passwords to accounts in order to gain or maintain employment. Accordingly, we urge a favorable report on SB 971.

AMERICAN CIVIL
LIBERTIES UNION OF
MARYLAND

---

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.

[2] 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).

[3] 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.