Social Media Privacy (Note)

Overview:
The growing use of social media in the U.S. has had implications in both the employment and educational contexts. In recent years, some employers and educational institutions have asked current and/or prospective employees or students to grant the employer or school access to social media accounts. From 2012-2014 (as of September 2014), nineteen states enacted varying legislation addressing access of this type (Arkansas, California, Colorado, Delaware, Illinois, Louisiana, Maryland, Michigan, Nevada, New Hampshire, New Jersey, New Mexico, Oklahoma, Oregon, Rhode Island, Tennessee, Utah, Washington, and Wisconsin), and numerous additional bills on the topic were introduced.

In the summer of 2013, the Executive Committee of the Uniform Law Commission (ULC) authorized the appointment of a Study Committee on Social Media Privacy to study the need for and feasibility of drafting an act on social media privacy. The committee studied the topic for close to a year, including soliciting and considering stakeholder feedback. The committee's work culminated in a recommendation to the ULC Committee on Scope and Program that the ULC establish a drafting committee to draft an act on social media privacy that addresses the specific issues considered by the Study Committee. At its 2014 Annual Meeting in Seattle, Washington, the ULC Executive Committee authorized the appointment of a Drafting Committee on Social Media Privacy. This newly appointed committee will draft legislation concerning employers' access to employees' or prospective employees' social media accounts and educational institutions' access to students' or prospective students' social media accounts; the committee's charge is limited to these issues.

Common Issues:
The current state social media privacy statutes vary with regard to many issues, but have commonly addressed the following (non-exhaustive) categories: types of entities covered; types of access prohibited; non-retaliation requirements; remedies available for non-compliance; and exceptions. Below is a general overview of how states have dealt with common categories of issues.

Categories of Entities Covered by the Statute:
Currently, states have (and continue to introduce) laws governing: (1) employers' access to employees' and/or prospective employees' social media accounts; *and/or* (2) educational institutions' access to students' and/or prospective students' social media accounts. Of the nineteen current (as of September 2014) state social media privacy laws, eleven are applicable to both categories (Arkansas, California, Illinois, Louisiana, Michigan, New Jersey, New Mexico, Oregon, Rhode Island, Utah, and Wisconsin), seven states cover employers only (Colorado, Maryland, Nevada, New Hampshire, Oklahoma, Tennessee, and Washington), and one – Delaware – addresses only schools. One state, Wisconsin, also addresses a landlord's access to a tenant or prospective tenant's personal internet accounts.

States also vary within the broad categories of entities covered as to what types of sub-categories are included. Most of the existing laws that address schools, for instance, are limited to postsecondary institutions/institutions of higher education. But several address broader

categories. Michigan's social media privacy statute, for example, covers educational institutions including kindergarten, nursery, elementary schools, and more.

While most of the states with legislation on this topic address both prospective and current employees/students (where applicable), New Mexico addresses both in the school realm, but only applicants in the employment context, and Illinois addresses both in the employment context, but only current students in the school realm.

Types of Access Prohibited:
State statutes currently vary in the scope and types of access that are restricted. Access limitations range from prohibiting the entity from requesting the person's username and password only, to barring the entity from requesting/requiring the person add someone affiliated with the entity as a contact in their social media network, to disallowing the entity from requesting/requiring the person to alter their privacy settings, to preventing the entity from accessing the person's social media account through a third party (e.g., someone who is already connected to the person), to prohibiting the entity from requesting/requiring to observe the person access their own social media account (sometimes known as "shoulder surfing"), to restricting the entity from inquiring whether a person has a social media account (in the case of New Jersey's school-specific statute).

Non-Retaliation Provisions:
The vast majority of the states' social media privacy laws include non-retaliation provisions, prohibiting the entity from penalizing a person for failing to grant access to the information protected under the act.

Remedy:
To the extent the state statutes make relief available for a violation of the law, the remedial options vary. More than half of the states that have laws on the topic contain a civil or administrative remedy, several of which include a private cause of action. (States with civil and/or administrative remedies include: Colorado, Michigan, New Jersey, New Hampshire, Oklahoma, Oregon, Rhode Island, Utah, Washington, and Wisconsin.) In addition to making a civil action available to a person aggrieved by a violation of the statute, Michigan provides that a person in violation is guilty of a misdemeanor, punishable by a fine of $1,000 or less.

Exceptions:
The state statutes also differ with regards to the type of exceptions available to entities, or instructive provisions regarding what the act does *not* restrict an entity from doing. In very general terms, common exceptions/non-limitations include:
(a) allowing an entity to request/require access to an electronic communications device that is paid for by the entity, or likewise a social media account that is provided by the employer or used for work-related purposes, or non-personal accounts that provide access to an employer's computer or information systems;
(b) allowing access to or use of information that is publicly available about the person;
(c) allowing an entity to request access to an individual's social media account if relevant to an investigation;
(d) allowing an employer to monitor electronic mail and equipment;

(e) allowing an employer to prohibit the transfer of propriety or confidential information or financial data to an employee's personal social media account without permission;
(f) making clear that the act's limitations do not prohibit an entity from complying with laws or regulations, including complying with a duty to screen or monitor applicants or employees established by federal law or a self-regulatory organization;
(g) providing that inadvertently receiving an individual's social media account login information is permissible (i.e., the employer is not liable for having that information), but once the inadvertent information is received the employer may not use it to access the individual's social media account; and
(h) providing that the act does not create a duty for an entity to search or monitor a personal social media account.