VERMONT
VERMONT DEPARTMENT OF LABOR

January 14, 2014

Vermont Department of Labor: 2013 Summer Study Committee Report on Social Media Privacy

The Senate Judiciary Committee established a Committee under Act 47 (following S.7) to examine the issue of prohibiting employers from requiring employees or applicants for employment to disclose a means of accessing the employee's or applicant's social network account. The Commissioner of the Department of Labor was assigned to chair the committee and prepare the report. Report Due: January 15, 2014. This report is submitted by Commissioner Annie Noonan, VDOL.

The Committee was tasked with the following:

- Examine existing social networking privacy laws and proposed legislation in other states
- Examine the interplay between state law and existing or proposed federal law on the subject of social networking privacy and employment
- Any other issues relevant to social networking privacy or employment
- Make recommendations, including proposed legislation

Members of the Committee

Annie Noonan, Commissioner; Erika Wolffing, Deputy; Matt Hill, Research Assistant, Vermont Dept. of Labor	Paco Aumand, Division Director, Public Safety; Capt. David Notte and Lt. Tom Hango, Vermont State Police	Brian Dunkiel, Attorney, Dunkiel Associates
Julio Thompson, Director, Civil Rights, Vt. Attorney General's Office	Karen Richards, Executive Director, and Ellen Maxon, Civil Rights Investigator, Human Rights Commission	Maureen McElaney, Digital Advisor, Dealer.com
Susan Donegan, Commissioner, Dept. of Financial Regulation	Kate Duffy, Commissioner and Alison Powers, Staff Attorney, Dept. of Human Resources	David Mickenburg, Attorney, representing Working Vermont
	Allen Gilbert, Executive Director, Vermont ACLU	Steve Howard, Legislative Director, Vermont State Employees Association

Introduction

In an age of rapidly advancing technology, legislation to protect citizens from undue incursion into their personal information and lives has become more important and more difficult. In response, approximately 13 states have adopted legislation– in varying means – to protect the privacy rights of employees, job applicants and students. Maryland was the first state to pass a social media privacy bill for employees, while California was the first to pass a "comprehensive social-media privacy" law which prohibits universities and employers from demanding user-names and passwords for social media sites. Some of the states have carved out exceptions for certain occupational titles and/or government entities, in most cases for law enforcement and financial regulation positions. The committee discussed privacy needs and exceptions thereto. Most existing state privacy laws do not curtail subpoena powers of government entities, and some privacy laws allow an employer to request an employee to divulge personal social media access in furtherance of misconduct investigations.

Privacy laws also make clear that employer-issued devices (computers, cell phones, etc.) are the property of the employer and that there is no right to privacy on activity conducted through the employer's own equipment.

Committee Meetings

The committee met three times. The meeting agendas included a review of the discussion at the Vermont statehouse that led to this committee and its charge, a review of other states' statutory provisions relating to social network privacy, a sharing of current activities or needs by certain departments, discussions on privacy rights, and sharing of thoughts where points of agreement might exist, if any, among the stakeholders' positions.

Human Resources and Financial Regulation:

The Department of Human Resources (DHR) stated that they were seeking an exemption as it relates to their need to conduct personnel investigations which may include a review of an employee's social media sites that may demonstrate they have compromised their ability to perform their work on behalf of the State and citizens. DHR said their exemption would be utilized during misconduct investigations. They reported that they had encountered a situation this past year where the exemption might have been utilized; but in the specific case, they did not ask for the user name or password, because the employee provided them a print out of the Facebook page related to the accusation. DHR noted that their HR Commissioner has subpoena power if needed.

Steve Howard of the Vermont State Employees Association (VSEA) stated that DHR's current power is sufficient to enforce compliance in misconduct investigations. Allen Gilbert of American Civil Liberties Union (ACLU) argued that if you create an exemption for DHR, he believes that every private employer will want the exception for the same reasons articulated by DHR. DHR reiterated that they deal with confidential and sensitive information daily, and to ensure compliance, an exception to the law would be helpful. The Department of Financial Regulation (DFR) has also stated that they would want an exception to monitor activities by financial industry employees, including using personal social media accounts for business purposes, which make it harder to monitor inappropriate or illegal activity in the financial regulation arena. Several states have adopted exemptions to privacy laws for financial regulation agencies.

Law Enforcement:

Law Enforcement exceptions to social network privacy laws are included in at least two states. New Mexico and Utah have law enforcement exceptions for employment applications for law enforcement and for law enforcement officers' conduct investigations. The Vermont State Police would like a law enforcement exemption, and believe that such exemption should be provided to all law enforcement agencies under 20 VSA. Lt. Dave Notte told the committee that the VSP is held to a higher standard and needs to use multiple resources to ensure they are hiring the right people. Alan Gilbert of ACLU stated that he does not believe that reviewing a social media account can be an effective way to screen job applicants. He stated that no one asks to look at a person's diary when screening them as an applicant. David Notte stated that a diary and a social media account are fundamentally different, "a diary is traditionally for the author's eyes only, whereas a Facebook page is shared among more than one person". Currently, during the background check process, VSP asks job applicants to log onto their Facebook and scroll through pictures and links. Some states have prohibited this type of inquiry, also known as "shoulder surfing." In states that have adopted restriction, they have carved out exceptions for law enforcement agencies for these activities. Alan Gilbert expressed concern over

the fact that a third party could have posted something on Facebook that might be in conflict with the law, and asked if it would it be the duty of law enforcement to act on such a post, even if it was inadvertently seen by the police. Dave Notte said police would, in fact, look into such a situation if it was a potential law violation. In discussion, the VSP noted that they do not have a formal protocol or policy relating to what the VSP staff, who conduct the website review, are to report (or not to report) about the applicant in the written summary of the applicant's acceptability to become a state police officer. The committee felt that VSP should have a written protocol for the officers conducting the review of applicant's personal social media accounts.

Conflict with Discrimination Law, and the Federal Electronic Privacy Law

Julio Thompson from the Attorney General's Office (AG) and other committee members noted that allowing access to a person's social media account may cause unintended liability to the employer, such as a discrimination claim if the access to the hiring entity revealed otherwise protected information, such as health care issues or sexual orientation. Julio Thompson noted that someone might disclose protected information to a family member via a social media account, and yet, through an employer's 'access' the information is then revealed to the employer. Julio Thompson also advised and briefed the committee on the federal Electronic Communications Privacy Act and the Stored Communications Act, and expressed his concern that carving out an exemption might put Vermont at odds with current federal legislation or pending proposals to strengthen privacy protections.

Federal Law

The privacy of many electronic communications has a six-month expiration date. The federal Electronic Communications Privacy Act (ECPA)[1] permits government and law enforcement officials to access private online information—emails, social media accounts, photos, and online documents without a warrant from a judge, once it is six months. Before the six-month expiration date, the government must have a warrant. Under that law, government entities can force the service providers to turn over their customers' private data. When the law was enacted electronic communication had limited storage ability, and at the time it was thought that if something was 180 days old it was deemed "abandoned." The law was written before the age of Facebook, Twitter, and cloud computing. An updated proposal, including eliminating the 180-day rule, providing disclosure to the individual whose account was accessed including what information was accessed, and requiring search are pending in the US Senate Judiciary Committee, but have not been acted upon, including the Leahy-Lee Electronics Communications Privacy Act Amendments, see at:
http://www.leahy.senate.gov/download/section-by-section-ecpa-reform-bill

Committee Recommendations:

The committee members did not reach consensus on the issue of social network privacy provisions, and, therefore, were unable to make a recommendation for proposed legislation.

[1]**Electronic Communications Privacy Act of 1986** (**ECPA**, 18 U.S.C. §§ 2510–2522) was enacted by Congress to extend government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer. Specifically, ECPA was an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 which was primarily designed to prevent unauthorized government access to private electronic communications. While technology has advanced dramatically since ECPA was enacted, the statute's privacy standards have not been updated. Meanwhile, the courts have been slow in extending the warrant requirement of the 4th Amendment to new technologies. The ECPA added provisions prohibiting access to stored electronic communications Stored Communications Act,18 U.S.C. §§ 2701-12. The **Stored Communications Act** addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers (ISPs).