YOU AIN'T NO FRIEND OF MINE: A REVIEW AND ANALYSIS OF LEGISLATION PROHIBITING EMPLOYERS FROM DEMANDING ACCESS TO EMPLOYEES' AND JOB APPLICANTS' SOCIAL MEDIA ACCOUNTS

by

Robert Sprague*

INTRODUCTION

In December 2010, Robert Collins re-applied for his job as a Corrections Supply Officer with the Maryland Department of Public Safety and Correctional Services after he had taken a leave of absence the previous year.[1] Before they can be rehired, corrections officers who have had a break in service must undergo a recertification, which includes fingerprinting, a renewed background check, and an interview.[2] During his recertification interview, Collins was asked whether he uses social media and when he replied that he uses Facebook, he was then asked for his Facebook username and password.[3]

In April 2011, Kimberly Hester, an elementary school teacher's aide in Michigan, posted a photo on her Facebook page of a coworker's pants around her ankles and a pair of shoes, with the caption "Thinking of you."[4] A parent and Facebook Friend of Hester's saw the photo and complained to the school.[5] When Hester refused the school superintendent's demand for access to her Facebook account, she was placed on unpaid leave.[6]

These two incidents, one involving a job applicant and the other an employee, sparked national media attention, which evidently caught the eye of a number of state and U.S. legislators. In 2012, bills were introduced in Congress and fourteen states prohibiting employers from requesting or requiring access to employees' and job applicants' personal online accounts. Four of the state bills passed.[7] So far in 2013, Arkansas,[8] Colorado,[9] New Mexico,[10] and Utah[11] have passed similar legislation, with bills introduced or reintroduced in Congress and twenty-eight states.[12]

This paper examines this recent legislative phenomenon from a variety of perspectives. First, the various legislation, enacted and proposed, is summarized and analyzed. Next, this paper raises the issue of whether this legislation is even needed, from both practical and legal perspectives, focusing on: (a) how prevalent the practice is of requesting employees' and job applicants' social media access information; (b) whether alternative laws already exist which prohibit employers from requesting employees' and job applicants' social media access information; and (c) what benefits can be derived from this legislative output. This paper then concludes with an analysis of the potential impact of this legislation on employees, job applicants, and employers.

PROPOSED LEGISLATION—SOME SIMILARITIES BUT NO UNIFORMITY

Fundamentally, the statutes and bills prohibit employers from requesting or requiring employees and job applicants to provide access to their personal online communications that are not normally available to the general public. While similar in concept, this "employee password protection"[13] legislation lacks uniformity in a number of respects. For example, New Mexico's recently enacted law is the only one that applies just to job applicants and not to employees as well.[14] As discussed below, the statutes and bills contain varying definitions, different types of specific prohibitions, a wide range of employer activities that are exempted from coverage, and many do not articulate any remedies in the event of violation.

Definitions

The definitions contained in the statutes and bills reflect much of the nonuniformity of the (potential) laws. While there is some commonality among the legislation, a review of just the definitions reveals the various approaches the legislative bodies are using to address employer social media access and employee password protection.

Employer

Arkansas, Colorado, Maryland, Michigan, and Utah, and most of the pending bills define an employer as both private and public.[15] California, Illinois,[16] and New Mexico do not include a definition of employer, nor do the pending bills in Hawaii,[17] Massachusetts,[18] Minnesota,[19] Nevada,[20] New Hampshire,[21] Ohio,[22] Oregon,[23] and Texas,[24] nor two of the pending bills in Missouri[25] and one of the pending bills in New York,[26] nor one of the pending bills amending Illinois's

statute.[27] It is typical for the definition of employer to include agents, representatives, or designees of the employer,[28] though not all do.[29]

Applicant and Employee

Many of the statutes and proposed laws define an applicant simply as an applicant for employment.[30] Employee is defined by only a few of the proposed laws, either as an individual who provides services or labor for wages or other remuneration for an employer,[31] or as a person engaged in service to an employer in a business of the employer;[32] though Maine and Missouri include independent contractors in their definitions of employee.[33]

Social Media and Other Personal Online Accounts

The principal prohibition contained within the enacted statutes and proposed laws relates to employers requesting or requiring from employees and job applicants username and password information to access the employees' and job applicants' social media or personal online accounts. Certain states define "social media" generally as "an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, e-mail, online services or accounts, or Internet website profiles or locations."[34] However, many of the statutes and bills instead refer to and define "social networking websites" as:

> an Internet-based service that allows individuals to: (a) construct a public or semi-public profile within a bounded system created by the service; (b) create a list of other users with whom they share a connection within the system; and (c) view and navigate their list of connections and those made by others within the system.[35]

Four states expressly *exclude* e-mail from coverage,[36] while Maine includes a definition of "[p]ersonal e-mail account."[37]

Some states take a different approach by applying the prohibitions to electronic communications devices, which are defined in most instances as "any device that uses electronic signals to create, transmit, and receive information and includes computers, telephones, personal digital assistants, and other similar devices."[38] Other statutes and bills use a variety of "personal account" definitions:

- "Personal Internet account" means an account created via a bounded system established by an Internet-based service that requires a user to input or store access information via an electronic device to view, create, utilize, or edit the user's account information, profile, display, communications, or stored data;[39]
- "Personal (Internet) account" means an account, service, or profile on a social network website used by a current or prospective employee exclusively for personal communications unrelated to any business purpose of the employer, and does not apply to any account, service, or profile created, maintained, used, or accessed by a current or prospective employee for business purposes of the employer or to engage in business-related communications;[40]
- "Personal account or service" means an account, service or profile on an email, social networking or any other website that is used by a person for personal communications unrelated to the business purposes of the employer;[41]
- "Personal online account" means an online account that is used by an individual primarily or exclusively for personal communication;[42] and
- "Private electronic account" means a collection of electronically stored private information regarding an individual, including such collections stored on social media internet web sites, in electronic mail, and on electronic devices.[43]

And finally, some bills are completely unique. For example, in the House of Representatives' bill, ''social networking website'' means:

> any Internet service, platform, or website that provides a user with a distinct account—(A) whereby the user can access such account by way of a distinct user name, password, or other means distinct for that user; and (B) that is primarily intended for the user to upload, store, and manage user-generated personal content on the service, platform, or website.[44]

Arkansas's newly enacted statute first defines a "social media" account as: "a personal account with an electronic medium or service where users may create, share, or view user-generated content, including without limitation: (i) Videos; (ii) Photographs; (iii) Blogs; (iv) Podcasts; (v) Messages; (vi) Emails; or (vii) Website profiles or locations."[45] The statute then specifies that a social media account *does not* include an account:

> (i) Opened by an employee at the request of an employer; (ii) Provided to an employee by an employer such as a company email account or other software program owned or operated exclusively by an employer; (iii) Setup by an employee on behalf of an employer; or (iv) Setup by an employee to impersonate an employer through the use of the employer's name, logos, or trademarks.[46]

The statute then notes that "'Social media account' includes without limitation an account established with Facebook, Twitter, LinkedIn, MySpace, or Instagram."[47]

Additional Definitions

There are a few additional definitions that appear in only one or a few statutes or bills. These include:

- "Access information" means user name, password, login information, or other security information that protects access to a personal Internet account;[48]
- "Login information" means a user name and password, a password, or other means of authentication that protects access to a personal social networking account;[49]
- "Personal electronic content" means electronically stored content of an individual including, but not limited to, pictures, videos, emails and other data files;[50] and
- "Publically accessible communication" means information that may be obtained without required access information or that is available in the public domain.[51]

Prohibitions

The principal prohibition contained in the enacted and proposed legislation relates to an employer requiring or requesting an employee or job applicant to disclose his or her username and password to his or her social media account.[52] As can be discerned from the various definitions, the prohibition against requesting or requiring a user name or password can apply to the employee's or job applicant's personal social media account, social networking website, personal/private Internet/online account or service, personal electronic content, or private e-mail account. Principal variations on the central prohibition include also requiring or requesting other related account information,[53] other means of accessing,[54] demanding access in any manner,[55] or limiting the access through an electronic communications device.[56] A few enacted and proposed laws also prohibit an employer from requiring or requesting that an employee or applicant access his or her personal social media account in the presence of the employer or allow observation by the employer.[57] Kansas's and New Jersey's proposed laws would also prohibit employers from requesting or requiring employees to disclose the existence of any personal account or service, as well as to divulge any its content.[58]

There are additional variations on the principal prohibition. For example, some states also would prohibit the employer from: compelling an employee or applicant to add an employee, supervisor, or administrator to the list or contacts associated with his or her social media account; or requesting, requiring, suggesting, or causing an employee or applicant to change the privacy setting associated with his or her social media account.[59] Nebraska's and North Carolina's proposed laws would also prohibit employers from accessing an employee's or job applicant's social networking profile or account indirectly through any other person who is a social networking contact of the employee or applicant.[60] Nebraska, New Jersey, and North Dakota would also prohibit an employer from requiring an employee or applicant to waive his or her protection under the proposed law.[61] In contrast, one of Texas's proposed laws would allow an employee to consent through contract to the disclosure of a username, password, or other means of accessing a personal account of the employee through an electronic communication device.[62]

Most, but not all, enacted and proposed laws also prohibit employers from taking an adverse action against an employee or job applicant—such as discharging, threatening to discharge, refusing to hire, or otherwise penalizing—for refusing a request that violates the particular state's law.[63] A few also prohibit employers from taking adverse action against employees or job applicants arising from their filing a complaint, causing or instituting a proceeding, or testifying in any proceeding related to the law.[64] The states which do not include any "adverse action" prohibition are California, Illinois (as enacted), New Mexico, Georgia, Minnesota, and Texas.

Finally, seven states prohibit, or would prohibit, employees from downloading without authorization an employer's proprietary information or financial data to the employee's personal website, an Internet website, a web-based account, or any similar account.[65]

Exemptions

The majority of newly-enacted statutes and proposed laws provide numerous exemptions from coverage—many actually provide more exemptions than prohibitions. There are a number of exemptions which appear frequently throughout the enacted and proposed legislation. These exemptions do not prohibit an employer from:

- Complying with the requirements of federal, state, or local laws, rules, or regulations or the rules or regulations of self-regulatory organizations;[66]
- Demanding access information from employees if the employee's social media account activity is reasonably believed to be relevant to a formal investigation or related proceeding by the employer of allegations of an employee's violation of federal, state, or local laws or regulations, or of the

employer's written policies or work-related employee misconduct, though the access information will be used only for the purpose of the formal investigation or a related proceeding;[67]

- Conducting an investigation to ensure compliance with securities or financial laws or other regulatory requirements based on information indicating an employee's use of a personal website, Internet website, web-based account, or a similar account for business purposes;[68]
- Promulgating and maintaining lawful workplace policies governing the use of the employer's electronic equipment, including policies regarding Internet use, social networking site use, and electronic mail use;[69]
- Monitoring usage of the employer's electronic equipment and the employer's electronic mail without requesting or requiring any employee or prospective employee to provide any password or other related account information in order to gain access to the employee's or prospective employee's account or profile on a social networking website;[70]
- Monitoring, reviewing, or accessing electronic data stored on an electronic communications device paid for in whole or in part by the employer, or traveling through or stored on an employer's network, in accordance with state and federal law;[71]
- Requiring or requesting an employee to disclose a username, password, or other method for the purpose of accessing an employer-issued electronic device, or nonpersonal accounts or services that provide access to the employer's internal computer or information systems;[72]
- Requesting or requiring an employee to disclose a username or password required only to gain access to an account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, and used for the employer's business purposes;[73]
- Investigating, disciplining, or discharging an employee for transferring the employer's proprietary or confidential or financial data to an employee's personal Internet account without the employer's authorization;[74]
- Viewing information about a current or prospective employee that is publicly available on the Internet or in the public domain;[75] and
- Terminating or otherwise taking an adverse action against an employee or applicant if otherwise permitted by laws.[76]

Limitations of Duties and Liability

A few statutes and proposed laws expressly state that they do not create a duty for an employer to search or monitor the activity of a personal Internet account,[77] nor is an employer liable for failure to request or require that an employee or applicant for employment grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant for employment's personal Internet account.[78] A few statutes and introduced bills provide that if an employer inadvertently receives an employee's username, password, or other login information to the employee's social media account through the use of an electronic device provided to the employee by the employer or a program that monitors an employer's network, the employer is not liable for having the information but may not use the information to gain access to an employee's social media account.[79]

Remedies

A majority of the enacted statutes and proposed laws do not expressly provide for a remedy in the event an employer violates the enacted or proposed law.[80] Those laws that do provide a remedy—roughly one-third—may allow an aggrieved employee or applicant to bring a civil suit, providing various damage limitations, injunctive relief, and an award of attorney fees and costs.[81] Other laws may provide for fines of varying amounts.[82]

IS THIS LEGISLATION EVEN NEEDED?

Not only does the employee password protection legislation vary widely in exactly what is prohibited and what is exempted, the legislation may not even be needed. First, there is little evidence of widespread requests or requirements by employers for employees' and job applicants' personal online account access information. Second, in those instances where employers have improperly accessed personal accounts or need access to those accounts, existing law appears to already provide a remedy.

To What Extent Are Employers Requesting Access?

According to the media, employers have recently been demanding Facebook passwords from job applicants and employees. This meme appears to have begun with a March 2012 AP article.[83] Subsequently a number of media outlets reported a "trend" in employers requesting social media account access from job applicants.[84] Yet a close reading of the articles reveals that when it comes to reporting actual incidents of an employer demanding access to an employee's or job applicant's social media account, it appears there are only seven documented incidents, including the two reported in the Introduction to this paper.[85] And while anecdotal evidence indicates that some college undergraduate and graduate students have been asked to login to their Facebook account in front of a recruiter, all the related incidents appear to have happened to a "friend of a friend"—the classic indicator of an urban legend.[86]

The few surveys that have asked the question directly reflect that, particularly in the private sector,[87] employers are not routinely asking for access to job applicants' social media accounts. For example, Littler Mendelson, a large labor and employment law firm, asked nearly 1,000 C-suite executives, corporate counsel, and human resources professionals from corporations throughout the United States and ranging in market capitalization from less than $1 billion to more than $4 billion the following question: "Has your organization requested social media logins as part of the hiring or onboarding process?"[88] The response: 99% of respondents answered the question in the negative.[89] In March 2013, an Ohio employment law attorney conducted an admittedly unscientific poll among his blog readers. Based on "hundreds" of responses, he reported the following results:

> Has your company ever asked a job applicant or employee to provide the login or password to a social media or other online account? No: 90%, Yes, an employee: 5%; Yes, an applicant: 3%; Yes, both: 1%. Have you ever been asked by an employer to provide the login or password to a social media or other online account? No: 95%; Yes: 5%. Has your company ever denied employment, or fired an employee, because an individual refused to disclose the login or password of a social media or other online site? No: 98%; Yes: 2%.[90]

And while there have been a very few reported cases involving employers requesting access to employees' Facebook or other social networking accounts,[91] as discussed below, they haven't necessarily involved the exact scenarios envisioned by the employee password protection legislation.

It is not surprising that Maryland—home to the first widely publicized request for a job applicant's social media access information—was the first state to enact protective legislation. Michigan—home to the only widely publicized request for an employee's social media access information—became the fourth state to enact protective legislation eight months later. It is also not surprising that most of the documented incidents arise from law enforcement-type government agencies attempting to perform extensive background checks on applicants.[92]

Why the interest in enacting protective legislation in so many states, as well as the U.S. Congress? It appears that publicity surrounding the two incidents reported at the beginning of this paper and a few additional incidents sparked a concern over employee and job applicant privacy, and coupled with the fact that a few states had begun enacting and considering protective legislation, legislators felt compelled to address the issue.[93] So, if there is minimal need for this type of legislation from a practical level, is it even necessary from a legal perspective—in other words, do laws already exist to protect employees and job applicants from the conduct outlawed in the newly enacted and proposed employee password protection legislation?

Do Existing Laws Already Protect Employees and Job Applicants from Prying Employers?

While Brian Pietrylo worked at a Hillstone Restaurant Group-owned Houston's restaurant as a server, he created an access-controlled MySpace page called the "Spec-Tator" for invited employees to "vent about any BS we deal with at work without any outside eyes spying in on us."[94] Pietrylo invited other past and present Houston's employees to join the group, including Karen St. Jean, a greeter at Houston's, who became an authorized participant in the MySpace group. At some point, Robert Anton, a Houston's manager, asked St. Jean to provide him the password to access the Spec-Tator, which she did. Although St. Jean stated that she was never explicitly threatened with any adverse employment action, she stated she gave her password to a member of management solely because he was a member of management and she thought she might get in some sort of trouble if she didn't.[95] Anton used the password provided by St. Jean to access the Spec-Tator from St. Jean's MySpace page. Houston's managers considered the posts on Spec-Tator to be offensive and Pietrylo and another employee, Doreen Marino, were fired.[96] Pietrylo and Marino then sued Hillstone Restaurant Group for, inter alia, violation of the Stored Communications Act[97] and common law invasion of privacy.[98]

The Stored Communications Act (SCA) prohibits unauthorized access to electronic communications while in electronic storage.[99] However, there is no violation of the SCA if access is authorized by a user of the service storing the electronic communications "with respect to a communication of or intended for that user."[100] The District Court for the District of New Jersey upheld the jury's verdict that the restaurant manager had violated the SCA because St. Jean's purported authorization was coerced.[101] This unreported decision supports the argument that an employer who coerces or compels an employee to turn over social media access information can possibly violate the SCA.[102] One could certainly argue

that just as an employee may be coerced into providing social media access information out of fear of losing her job, a job applicant may be just as coerced out of fear of being disqualified for a job.[103]

In June 2009, Deborah Ehling, a registered nurse employed by the Monmouth-Ocean Hospital Service Corporation ("MONOC") since 2004, posted a comment on Facebook regarding a shooting that took place at the Holocaust Museum in Washington, DC, stating:

> An 88 yr old sociopath white supremacist opened fire in the Wash D.C. Holocaust Museum this morning and killed an innocent guard (leaving children). Other guards opened fire. The 88 yr old was shot. He survived. I blame the DC paramedics. I want to say 2 things to the DC medics. 1. WHAT WERE YOU THINKING? and 2. This was your opportunity to really make a difference! WTF!!!! And to the other guards ....go to target practice.[104]

Only Ehling's Facebook Friends could view the post and Ehling had not "Friended" any of MONOC's management. Ehling alleged that MONOC management became aware of the posting through a supervisor "coercing, strong-arming, and/or threatening [an] employee [who was a Facebook Friend with Ehling] into accessing his Facebook account on the work computer in the supervisor's presence."[105] The District Court for the District of New Jersey refused to dismiss Ehling's common law privacy claim against MONOC, concluding that she "may have had a reasonable expectation that her Facebook posting would remain private, considering that she actively took steps to protect her Facebook page from public viewing."[106]

Ehling provides some precedent that coercing an employee to access a Facebook account could potentially violate the employee's common law right of privacy.[107] The problem with applying *Pietrylo* and *Ehling* to the current and proposed employee password protection legislation is that in both *Pietrylo* and *Ehling*, the employer did not demand access from the plaintiff-employee. The employers did not request access directly to Pietrylo's and Ehling's personal accounts—which is what is prohibited in the employee password protection legislation—they merely viewed communications stored on those accounts through other employees' authorized access. A plain reading of a majority of the enacted and proposed legislation—prohibiting employers from requesting usernames and passwords and other means of access to employees' and job applicants' own social media accounts, and, in most cases, prohibiting employers from taking adverse action against employees or refusing to hire applicants who do not comply—does not appear to address the scenarios presented by *Pietrylo* and *Ehling*.[108] In *Pietrylo* and *Ehling*, the employees who were disciplined or fired were never themselves requested to provide access information.

There have been two reported cases in which an employer has accessed a former employee's personal e-mail account, not by requesting or requiring a username and password, but because the username and password were automatically saved for login. In *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp*, the employer accessed a former employee's personal Hotmail account which the employee had accessed using the employer's computer equipment.[109] The employee's username and password were pre-saved on the employer's computer.[110] The court concluded that the former employee had a reasonable expectation of privacy in his "personal e-mail accounts, stored on third-party computer systems, protected (albeit ineffectively) by passwords."[111] The court also concluded that the employer violated the SCA by accessing the former employee's personal e-mail accounts—rejecting the employer's argument the employee had given "implied consent" to access by leaving the username and password saved on the employer's computer.[112]

In a similar case, an employer accessed a personal AOL e-mail account used by a former employee for both personal and business communications, again using login information pre-saved on the employer's computer.[113] In this case, the former employee had originally installed access to her personal AOL account on her employer's computer while the employer was transitioning to a new e-mail system. The former employee used her AOL account for some business communications during the transition, but later used her employer's new e-mail account exclusively for business communications and her own AOL account exclusively for personal communications—including communications with her attorney when she was considering a sexual harassment action against the employer.[114] The Illinois Appellate Court reversed the trial court's granting of the employer's motion to dismiss the former employee's SCA and common law privacy claims.[115] In general, courts have recognized privacy rights in personal online accounts versus accounts provided by the employer.[116]

One might argue that these two scenarios fall within the language of a large proportion of the employee password protection legislation that prohibits an employer from requesting or requiring disclosure of the username, password, "or other means of accessing" the employee's or job applicant's personal online account.[117] However, since the phrase is modified by a request or requirement by the employer to disclose that other means of accessing, there is a strong argument that the two scenarios above would not actually be covered by the legislation.

As discussed above, the newly enacted and proposed employee password protection legislation contains not only prohibitions against certain employer conduct, but also provides numerous exemptions from coverage. One exemption is observing information that is in the public domain.[118] This appears to be a rather unnecessary provision, as it has been well-established there is no privacy protection for information open to public viewing.[119] Most of the remaining exemptions appear to merely emphasize that the prohibitions do not supersede already existing employer rights to supervise, monitor, and maintain its information systems, as well as comply with various laws and regulations regarding employee online conduct.

But can this legislation actually establish new rights? Many companies hire employees to maintain an online presence for the employer and disputes later arise as to who is entitled to access to those online accounts. As discussed above, liability may rest on whether the employer exceeded its authority in violation of the SCA by accessing employee-controlled

accounts.[120] Some of the new and proposed laws exclude accounts created by employees for business purposes of the employer or apply only to accounts used exclusively for personal communications unrelated to the business purposes of the employer.[121] With the growing business presence in online social media, coupled with the comingling of workplace and personal use of—sometimes employer-provided—online accounts and communications devices,[122] it is inevitable that disputes will arise as to who exactly has rights of access and content control. If these laws do not prohibit an employer from requesting or requiring access information for accounts used, at least to some degree, for the employer's business, would that constitute an implied authorization on the part of the employee to access those accounts sufficient to satisfy the SCA?

In *Maremont v. Susan Fredman Design Grp., Ltd.*, the defendant, an interior design firm, hired the plaintiff as its Director of Marketing, Public Relations, and E-commerce.[123] In fulfilling her duties, the defendant established a Twitter following within the design community, created a blog hosted on the employer's website, and created a Facebook account for the employer—all of which were interlinked.[124] The plaintiff also maintained her own Facebook page and the Twitter account was evidently her own personal account. She also stored access information for all the accounts within the defendant's computer system.[125] After being struck by an automobile, the plaintiff ultimately stopped working for the plaintiff, but while she was hospitalized, the plaintiff alleges the defendant updated content on the plaintiff's personal Twitter and Facebook accounts.[126] The court refused to dismiss the plaintiff's SCA claim against the defendant, concluding there were disputed issues of material fact as to whether the defendant exceeded its "authority in obtaining access to Maremont's personal Twitter and Facebook accounts."[127] Although the court noted that it was "undisputed that Maremont's personal Twitter and Facebook accounts were not for the benefit of" her employer, Maremont did promote her employer's business on those accounts, particularly the Twitter account.[128]

In contrast, in *Ardis Health, LLC v. Nankivell*, there was minimal commingling of personal and work-related accounts and the court had no difficulty declaring employer access rights.[129] In *Ardis Health*, the defendant had been hired as a as Video and Social Media Producer to produce videos and maintain websites, blogs, and social media pages in connection with the online marketing of the plaintiffs' products.[130] The defendant was fired in June 2011 but refused to turn over access information to the plaintiffs' online accounts, leaving the plaintiffs unable to access a number of their online accounts and websites to update them as needed for their marketing purposes.[131] The District Court for the Southern District of New York ordered the defendant to turn over the access information, noting the plaintiffs "depend heavily on their online presence to advertise their businesses, which requires the ability to continuously update their profiles and pages and react to online trends."[132] The court even suggested that the defendant's unauthorized retention of the access information could form the basis of a claim of conversion.[133] However, the plaintiffs had to show they were suffering irreparable harm by not having access to their online accounts.[134] The court was willing to order the defendant to turn over the access information for online accounts that were vital to the plaintiffs' business,[135] but would a court be so willing if the accounts were "merely" important? At least within the jurisdictions that have enacted or may enact legislation which does not prohibit employers to require disclosure of access information to accounts associated with the employer's business, the employer would not have a high burden to establish the right to that information. It is therefore arguable that employee password protection legislation which includes an exemption for employers requesting access information to accounts used in part for the employer's business can legitimately obtain that information, without having to first show any harm to the business, and use it without violating the SCA.

However, *Ardis Health* also involved issues beyond the scope of employee password protection legislation, such as whether the former employee had the right to display selected portions of the plaintiffs' trademarked and copyrighted material within her personal online portfolio.[136] Similarly, *Maremont* involved claims beyond unauthorized access, including trademark, right of publicity, and common right to privacy claims.[137] Additional cases involving disputed ownership over "comingled" online accounts do not involve access claims per se, instead raising claims beyond the scope of the password protection laws, such as unauthorized use of name, misappropriation of identity, misappropriation of publicity, conversion, tortious interference with contract, intentional and negligent interference with prospective economic advantage, and misappropriation of trade secrets.[138]

CONCLUDING ANALYSIS: CAUSING MORE HARM THAN GOOD?

A privacy advocate would naturally applaud the growing number of states who are enacting employee password protection legislation—now eight, with bills working their way through the legislative process in an additional twenty-eight states and the U.S. Congress. It is too soon to tell whether it is a "good" thing that this legislation, as Gordon et al. argue, overturns decades of common law jurisprudence:

> The underlying premise of these laws is that an employer invades an applicant's or employee's privacy by viewing content on a restricted access social media account without the voluntary consent of the account holder. Digging one step deeper, these laws, at their core, assume that the content of a restricted access social media account is private no matter how many people the user invites to view that content and regardless of the relationship between the user and the viewer. Put more plainly, these laws are based on the belief that, for example, a Facebook user who has more than 500 "Friends," including current and

> former supervisors and other executives at his current employer, can establish the "privacy" of his content by using Facebook's privacy settings to restrict access to "Friends Only."
>
> No court has ever construed the tort of invasion of privacy by intrusion upon seclusion so broadly.[139]

Perhaps Gordon et al. miss the point, which is that the focus of the legislation is not how many Friends an employee or job applicant has, but that the employer, except in specific instances,[140] has no business—meant in a literal sense—prying into communications that have been clearly restricted to individuals which do not include the employer.

A review of the enacted and proposed employee password protection legislation reveals similarities among them in a very broad sense, but significant inconsistencies in how they may be applied in different situations from state to state. For example, Abril et al. have published recent empirical data suggesting that while college-aged employees are generally ambivalent regarding employer access to their online social media profiles,[141] only approximately one-third of survey respondents included their immediate supervisor as an online Friend.[142] In addition, fifty-four percent of survey respondents strongly or somewhat agreed that "work life is completely separate from personal life, and what you do in one should not affect the other."[143] However, eighteen percent "of respondents reported a senior executive requested to [be] (and was) added as a friend or connection to an [online social network] profile."[144] Yet, "[e]ighty-one percent of respondents considered it inappropriate for employees to be required to invite their supervisor to their [online social network] profile."[145] Abril et al. conclude that "it is likely a considerable number of employers may already have access to their employees' information on an" online social network.[146]

Only nine of the enacted and proposed laws address employees "Friending" their employer.[147] Two of the states, Arkansas and North Carolina, prohibit an employer from requiring or requesting that it be added as an employee's or job applicant's online social network Friend, while seven states—Colorado, Maine, Massachusetts, New Hampshire, Oregon, Rhode Island, Washington—merely prohibit an employer from "compelling" an employee or job applicant to do so. Abril et al.'s survey respondents reported requests by employers, not requirements, and the respondents complied because "it is clear that respondents were not willing to forgo participation in social networks to achieve privacy or separation of work and personal life. They displayed a strong desire to socialize, to interact, and to share truthful information about themselves on social networks."[148] If many young employees generally accept that supervisors, and even executives, expect to be made Friends with employees within their online social network worlds, is the employer engaging in overly-intrusive monitoring or merely just finding another way for workers, along the chain of command, to connect with each other? In either event, employers asking to become employee's online Friends, to the extent it is occurring, is apparently now illegal in only Arkansas and perhaps in the future in North Carolina.[149]

While it was argued earlier that the employee password protection legislation does not directly apply to scenarios such as those presented in *Pietrylo* and *Ehling* where employers have viewed private online communications by "coercing" another employee to provide the employer access to those communications,[150] only two states, Nebraska and North Carolina, include that exact scenario within their proposed legislation.[151] In contrast, *Maremont* applied Illinois law,[152] but Illinois's "Right to Privacy in the Workplace Act"[153] does not expressly allow employers to request access information for accounts used in whole or in part for the employer's business, so it would be of no help to the employer in that case. And would the enacted and proposed legislation in Illinois, Minnesota, Missouri, and North Dakota, which expressly excludes personal e-mail accounts,[154] overrule cases such as *Pure Power Boot Camp*[155] and *Borchers*,[156] both of which found that a former employer had improperly accessed an employee's personal e-mail account?[157]

Recall that one of Texas's proposed laws would allow an employee to enter an agreement with the employer consenting to the disclosure of the employee's personal account access information.[158] This would completely negate the purpose of the proposed legislation. The European Union, for example, recognizes the impracticality of true consent by an employee due to the power imbalance between the employer and the employee.[159] While U.S. jurisprudence does not formally adopt this approach, the EU's approach does point out the reality that when presented with such a consent agreement, most employees will feel compelled to sign it. Recall also that, in contrast, three states would prohibit an employer from requiring an employee or applicant to waive his or her protection under the proposed law.[160] This raises an interesting conundrum. Does that fact that three states believe there is a need to include a "no-waiver" provision mean that employers in states without one would be allowed to request applicants and employees to waive their rights to any enacted employee password protection legislation? Again, employment realities suggest applicants and employees would feel compelled to agree to such a waiver.[161]

It could be argued that except in Arkansas and possibly North Carolina,[162] the enacted and proposed employee password privacy protection will have minimal practical effect for four reasons: (1) the conduct proscribed does not appear to be actually happening to any meaningful extent;[163] (2) six of the enacted and proposed laws merely prohibit requesting or requiring access information to employee's and job applicant's personal online accounts, they do not prohibit employers from taking adverse action against an employee or job applicant who does not comply;[164] (3) only approximately one-third of the enacted and proposed legislation actually provides a remedy or penalty in the event the law is violated, and many of those fines are minimal—as low as a few hundred dollars per incident;[165] and (4) an argument can be made that employers may be able to request that employees waive their rights under the legislation.[166]

In one sense, going forward employers can continue with the status quo: not requesting access information to employee's and job applicant's personal online accounts, except in specific instances. But it is those specific instances which may cause the most trouble for employers. As noted previously, it appears most of the exemptions in the enacted and proposed employee password protection legislation are included merely to re-affirm that the prohibitions do not supersede already existing rights, such as supervising, monitoring, and maintaining the employer's information systems, or complying with various laws and regulations regarding employee online conduct. [167] But as a review of the enacted and proposed legislation reveals, there are significant inconstancies among the various laws regarding what conduct is exempted. Could it be argued that when and whichever exemptions exist prescribe the only circumstances in which an employer can require disclosure of an employee's personal online account access information? Could it then be argued that where an exemption does not exist, the employer would not have the access right, even if it might have existed without the legislation? Could it be argued that if a state omits an exemption, while other states include it, the former state's legislature intended that it not be a right of the employer?

As noted previously,[168] the primary motivation underlying the employee password protection legislation is to protect employees' and job applicants' personal online communications from the prying eyes of (prospective) employers—in other words, to protect one aspect of individual privacy.[169] "A statute should represent 'timely responsiveness'; that is, it should be responsive to the needs of the people—it should be protective of their interests. . . ."[170] But this legislation appears to be responsive not to the needs of the people—employees, current and prospective, and employers alike—but to a media meme that had very little factual basis and a "me-to" attitude among the states that if other states are passing this legislation then they ought to too. While the enacted and proposed employee password protection legislation appears to be an answer in search of a problem,[171] all the legislation really does is raise more questions than it answers.

Footnotes

* J.D., M.B.A. Associate Professor, University of Wyoming College of Business Department of Management & Marketing.

[1] *See* Letter from Deborah A. Jeon, Legal Dir., ACLU of Md., to Sec'y Gary D. Maynard, Md. Dep't of Pub. Safety & Corr. Servs. (Jan. 25, 2011), *available at* http://www.aclu-md.org/uploaded_files/0000/0041/letter-_collins_final.pdf.

[2] *Id.*

[3] *Id.* Collins was told interviewees were required to provide social media login information as a standard part of the Department of Correction's process for hiring and recertification to enable the Department to review wall postings, e-mail 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. *Id.*

[4] Emil Protalinski, *Teacher's Aid Fired for Refusing to Hand over Facebook Password*, ZDNET (April 1, 2012, 18:15), http://www.zdnet.com/blog/facebook/teachers-aide-fired-for-refusing-to-hand-over-facebook-password/11246.

[5] *Id.*

[6] *Id.*

[7] California: CAL. LAB. CODE § 980 (enacted Sept. 27, 2012; effective Jan. 1, 2013); Illinois: 820 ILL. COMP. STAT. 55/10 §10 (enacted Aug. 1, 2012; effective Jan. 1, 2013); Maryland: MD. CODE ANN., LAB. & EMPL. § 3-712 (enacted May 2, 2012; effective Oct. 1, 2012); Michigan: MICH. COMP. LAWS §§ 37.272–.278 (enacted Dec. 27, 2012; effective Dec. 28, 2012); In addition, two states, Delaware (Del. Code Ann. tit. 14, §§ 8101-8105 (2012)) and New Jersey (N.J. STAT. ANN. §§ 18A:3-29–32 (2012)), enacted legislation banning schools from requesting students' personal online account access information.

[8] Act 1480 (enacted Apr. 22, 2013) (to be codified at ARK. CODE ANN. § 11-2-124 (2013)).

[9] H.B. 13-1046 (enacted May 11, 2013) (to be codified at COLO. REV. STAT. § 8-2-127 (2013)).

[10] S.B. 371 (enacted Apr. 5, 2013).

[11] H.B. 100 (enacted Mar. 26, 2013; effective May 14, 2013) (to be codified at UTAH CODE ANN. §§ 34-48-101–301 (West 2013)).

[12] See *Employer Access to Social Media Usernames and Passwords 2013*, NAT'L CONFERENCE STATE LEGISLATURES, http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords-2013.aspx (last updated May 7, 2013), for a list of pending and enacted state bills. Montana's proposed legislation, S.B. 195, died in committee April 24, 2013. Mississippi's proposed legislation, H.B. 165, died in committee Feb. 5, 2013. Vermont's proposed legislation, S.B. 7, was amended to form a committee "to study how to create statutory language to prohibit employers from requiring employees or applicants for employment to disclose a means of accessing the employee's or applicant's social network account." Unless otherwise noted, all citations to proposed legislation are for the 2013 legislative session.

[13] Only eleven of the proposed and enacted laws contain formal names, which vary— "Right to Privacy in the Workplace Act" (Illinois: 820 ILL. COMP. STAT. 55/10 §10 (2012)); "Internet Privacy Protection Act" (Michigan: MICH. COMP. LAWS §§ 37.272–.278 (2012)); "Social Networking Online Protection Act" (U.S. Congress: H.R. 537); "Personal Online Account Privacy Protection Act" (Louisiana: H.B. 314); "Password Privacy Protection Act" (Missouri: H.B. 706, S.B. 164); "Workplace Privacy Act" (Nebraska: L.B. 58); "Job and Education Privacy Act" (North Carolina: H.B. 846); "Social

Network Privacy Protection Act" (Oregon: S.B. 499); "Social Media Privacy Protection Act" (Pennsylvania: H.B. 1130); "Internet Privacy Protection Act" (West Virginia: H.B. 2966)—and can be quite convoluted. For example, Arkansas's statute, Act 1480 (to be codified at ARK. CODE ANN. § 11-2-124), is entitled: "An act to prohibit an employer from requiring or requesting a current or prospective employee from disclosing his or her username or password for a social media account or to provide access to the content of his or her social media account; and for other purposes" and is subtitled: "To prohibit an employer from requiring or requesting a current or prospective employee from disclosing his or her username or password for a social media account." For convenience, the legislation, enacted and proposed, discussed in this paper will often be generically referred to as "employee password privacy" legislation.

[14] S.B. 371.

[15] While New Jersey's proposed legislation defines an employer as including an employer's agent, representative, or designee, it does not include public employers. A.B. 2878. In fact, the latest version of the bill expressly excludes the Department of Corrections, State Parole Board, county corrections departments, or any State or local law enforcement agency. *Id*. This is arguably in response to the original controversy involving Maryland Department of Corrections applicant Robert Collins, as discussed in the opening paragraph of this paper. *See supra* notes 1-3 and accompanying text. Maryland's Attorney General had defended the screening practice of the Department of Corrections as necessary to ferret out possible gang affiliations of applicants. *See* Neal Augenstein, *Md. AG: Requiring Employees' Personal Passwords Is Legal*, WTOP.COM (Feb. 23, 2011, 7:15 PM), http://wtop.com/?nid=46&sid=2282721. Similar to New Jersey, North Dakota's proposed legislation does not include public employers. H.B. 1455.

[16] One of Illinois's proposed amendments to its statute does define employer, which includes both private and public entities, as well as the employer's agents, representatives, or designees. H.B. 1047(b)(7)(B).

[17] H.B. 713, S.B. 207.

[18] While Massachusetts's S.B. 872 does not include a definition of employer, it proposes to amend Section 4 of Chapter 151B of the commonwealth's General Laws, which, in its definition of employer, primarily defines what is not an employer, but also states that it includes "the commonwealth and all political subdivisions, boards, departments and commissions thereof." MASS. GEN. LAWS ch. 151B, § 1(5) (2010). Another of Massachusetts's pending bills, S.B. 852, also does not include a definition of employer, but proposes to amend Chapter 149 of the commonwealth's General Laws, which does define employer, including "any person acting in the interest of an employer directly or indirectly." MASS. GEN. LAWS ch. 149, § 1 (2010). The definition does not, however, include public entities. *Id*. Massachusetts's third pending bill, H.B. 1707, defines an employer simply as including "any agent, representative, or designee of the employer."

[19] H.F. 293, H.F. 611, S.F. 484, S.F. 596.

[20] Nevada's bill, A.B. 181, proposes to amend its state's Chapter 613 relating to employment practices. The bill does not state where within Chapter 613 its contents would be incorporated; however, within the sections addressing equal opportunities for employment, employee is defined as a person who has fifteen or more employees. NEV. REV. STAT. § 613.310(2) (Westlaw current through 2011 76th Reg. Sess.). Therefore, Nevada's proposed legislation may apply only to private employers with fifteen or more employees.

[21] H.B. 414.

[22] While Ohio's proposed legislation, S.B. 45, does not define employer, it does amend the state's anti-discrimination chapter, which includes both public and private employers in its definition, though exempting private employers with less than four employees. OHIO REV. CODE ANN. § 4112.01(A)(2) (Westlaw, current through File 7 of the 130th Gen. Assemb. (2013-2014)).

[23] Oregon's proposed legislation, while not defining an employer, amends chapter 659A, the state's anti-discrimination law, which limits the definition of employer to only private entities. OR. REV. STAT. ANN. § 659A.001(4) (Westlaw current through Ch. 42 of the 2013 Reg. Sess.).

[24] Texas's bills (H.B. 318, H.B. 451, S.B. 118, S.B. 416) do not include a definition of employer, but amend Chapter 21 of the state's Labor Code, which includes both public and private employers in its definition, though exempting private employers with less than fifteen employees. TEX. LAB. CODE ANN. § 21.002(8) (Westlaw current through Chapter 4 of the 2013 Reg. Sess. of the 83rd Leg.).

[25] Two of the pending bills in Missouri, H.B. 286 and H.B. 1020, propose to amend Chapter 285 of Missouri's statutes relating to employers and employees generally. Chapter 285 contains two sections which define employer, but neither applies to the section proposed to be enacted: H.R. 286 proposes to add a section 285.605 and H.R. 1020 proposes to add a section 285.603; employer is defined in MO. REV. STAT. § 285.500 (Westlaw current through Mar. 29, 2013 of the 2013 First Reg. Sess. of the 97th Gen. Assemb.), but the definition applies only to §§ 285.500–.515; similarly employer is defined in MO. REV. STAT. § 285.525, but the definition applies only to §§ 285.525–.550.

[26] S.B. 1701.

[27] S.B. 2306.

[28] *See, e.g.*, Arkansas: Act 1480 (to be codified at ARK. CODE ANN. § 11-2-124(a)(2) (2013)); Maryland: MD. CODE ANN., LAB. & EMPL. § 3-712(a)(4)(ii) (2012); Michigan: MICH. COMP. LAWS §§ 37.272(c) (2012).

[29] Utah: H.B. 100 (to be codified at UTAH CODE ANN. § 34-48-102(2) (2013)); U.S. Congress: H.R. 537; Connecticut: C.B. 159; Georgia: H.B. 117, H.B. 149; Kansas: H.B. 2092, S.B. 53; Missouri H.B. 286, H.B. 706, S.B.164.

[30] Colorado: H.B. 13-1046 (to be codified at COLO. REV. STAT. § 8-2-127(1)(a) (2013)); Maryland: MD. CODE ANN., LAB. & EMPL. § 3-712(a)(2); Arizona: SB 1411; Connecticut: C.B. 159 ("'Applicant' means any person actively seeking employment from an employer."); Illinois: H.B. 1047 ("'Prospective employee' means an applicant for employment."); Maine: H.P. 838; Missouri: H.B. 115, H.B. 706, S.B. 164; Nebraska: L.B. 58 ("Applicant means a prospective employee applying for employment."); New York: A.B. 443, S.B. 1701, S.B. 2434; North Carolina: H.B. 846 ("Applicant—a prospective employee applying for employment with an employer."); North Dakota: H.B. 1455 ("'Applicant' means a prospective employee applying for employment."); Rhode Island: H.B. 5255, S.B. 493; Washington: S.B. 5211; West Virginia: H.B. 2966.

[31] Arkansas: Act 1480; Rhode Island: H.B. 5255, S.B. 493.

[32] Connecticut: C.B. 159; Georgia: H.B. 117, H.B. 149.

[33] Maine: H.P. 838; Missouri: H.B. 706, S.B. 164.

[34] California: CAL. LAB. CODE § 980 (2013); Georgia: H.B. 117, H.B. 149; Maine: H.P. 838 (excluding "an account opened at an employer's behest, or provided by an employer, that is intended to be used solely on behalf of the employer"); Massachusetts: H.B. 1707, S.B. 852; Nevada: A.B. 181; New Hampshire: H.B. 414 (containing similar language); Oregon: H.B. 2654, S.B. 499; Rhode Island: H.B. 5255, S.B. 493 (excluding "an account opened at an employer's behest, or provided by an employer, that is intended to be used primarily on behalf of the employer"). Pennsylvania uses a much more narrow definition of "social media" as including, but not limited to, "social networking internet websites and any other forms of media that involve any means of creating, sharing and viewing user generated information through an account, service or internet website." H.B. 1130.

[35] Illinois: 820 ILL. COMP. STAT. 55/10 §10(b)(4) (2013); New Mexico: S.B. 371 (enacted Apr. 5, 2013); Illinois: S.B. 2306; Kansas: H.B. 2092, S.B. 53 (defining the Internet website as privacy-protected); Minnesota: H.F. 293, H.F. 611, S.F. 484, S.F. 596; Missouri: H.B. 286; New Jersey: A.B. 2878; Ohio: S.B. 45 (calling it a "Social media internet web site"). North Carolina and North Dakota use a more extensive definition of a "Social networking site":

> An Internet-based, personalized, privacy-protected Web site or application whether free or commercial that allows users to construct a private or semiprivate profile site within a bounded system, create a list of other system users who are granted reciprocal access to the individual's profile site, send and receive e-mail, and share personal content, communications, and contacts.

North Carolina: H.B. 846; North Dakota: H.B. 1455.

[36] Illinois: 820 ILL. COMP. STAT. 55/10 §10(b)(4), S.B. 2306; Minnesota: H.F. 293, H.F. 611, S.F. 484, S.F. 596; Missouri: H.B. 286, H.B. 1020; North Dakota: H.B. 1455.

[37] H.P. 838 ("'Personal e-mail account' means an account with an electronic medium or service through which users may send or receive e-mail delivered by transmission over the Internet. 'Personal e-mail account' does not include an account opened at an employer's behest, or provided by an employer, that is intended to be used solely on behalf of the employer.").

[38] Colorado: H.B. 13-1046 (to be codified at COLO. REV. STAT. § 8-2-127(2)(a) (2013)); Maryland: MD. CODE ANN., LAB. & EMPL. § 3-712(a)(3) (2012); Arizona: S.B. 1411; Georgia: H.B. 117, H.B. 149; Iowa: H.F. 272; Missouri: H.B. 115, H.B. 706, S.B. 164; New Jersey: A.B. 2878; New York: A.B. 443, S.B. 1701, S.B. 2434; North Carolina: H.B. 846; North Dakota: H.B. 1455; Texas: H.B. 318, H.B. 451, S.B. 118, S.B. 416; Washington: S.B. 5211; West Virginia: H.B. 2966. Nebraska uses a more expansive definition of "electronic communication device": "a cellular telephone, personal digital assistant, electronic device with mobile data access, laptop computer, pager, broadband personal communication device, two-way messaging device, electronic game, or portable computing device[.]" L.B. 58.

[39] Michigan: MICH. COMP. LAWS §§ 37.272(d) (2012); Illinois: H.B. 1047 (excluding an account provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or used for the employer's business purposes); Iowa: H.F. 127.

[40] Utah: H.B. 100 (to be codified at UTAH CODE ANN. §§ 34-48-102(4) (2013)); Connecticut: C.B. 159 (including e-mail, social media and retail-based Internet websites); Hawaii: H.B. 713, S.B. 207; Illinois: S.B. 2306 (applying only the first half of the definition); Missouri: H.B. 706, S.B. 164 (naming it a "Personal online account;" defining also a "Personal online service" with identical language, substituting account for service); New Hampshire: H.B.414; New Jersey: A.B. 2878; North Carolina: H.B. 846 (containing similar language).

[41] Kansas: H.B. 2092, S.B. 53.

[42] Louisiana: H.B. 314.

[43] Ohio: S.B. 45.

[44] H.R. 537, § 5(2).

[45] Act 1480 (to be codified at ARK. CODE ANN. § 11-2-124(a)(3)(A) (2013)).

[46] *Id.* at § 11-2-124(a)(3)(B).

[47] *Id.* at § 11-2-124(a)(3)(C).

[48] Michigan: MICH. COMP. LAWS §§ 37.272(a) (2012); Iowa: H.F.127.

[49] Washington: S.B. 5211 (though the proposed legislation does not define "social networking account").

[50] Kansas: H.B. 2092, S.B. 53.

[51] North Carolina: H.B. 846.

[52] Recall that New Mexico's prohibition applies only to job applicants and not employees. S.B. 371 (enacted Apr. 5, 2013).

[53] Illinois: 820 ILL. COMP. STAT. 55/10 §10(b)(1) (2013).

[54] Colorado: H.B. 13-1046 (to be codified at COLO. REV. STAT. § 8-2-127(2)(a) (2013)); Maryland: MD. CODE ANN., LAB. & EMPL. § 3-712(b)(1) (2012); U.S. Congress: H.R. 537; Arizona: S.B. 1411; Connecticut: C.B. 159 (prohibiting other authentication means of accessing); Georgia: H.B. 117; Illinois: H.B. 1047 (prohibiting other means of authentication); Iowa: H.F. 272; Louisiana: H.B. 314 (prohibiting other authentication information); Maine: H.P. 838; Massachusetts: H.B. 1707, S.B. 852; Missouri: H.B. 115, H.B. 706, S.B. 164 (prohibiting other authentication means); New York: A.B. 443, S.B. 1701, S.B. 2434; Oregon: H.B. 2654, S.B. 499; Pennsylvania: H.B. 1130; Rhode Island: H.B. 5255, S.B. 493; Texas: H.B. 318, H.B. 451, S.B. 118, S.B. 416; West Virginia: H.B. 2966.

[55] Illinois: 820 ILL. COMP. STAT. 55/10 §10(b)(1); New Mexico: S.B. 371.

[56] Colorado: H.B. 13-1046 (to be codified at COLO. REV. STAT. § 8-2-127(2)(a)); Maryland: MD. CODE ANN., LAB. & EMPL. § 3-712(b)(1); Arizona: S.B. 1411; Georgia: H.B. 117; Iowa: H.G. 272; Massachusetts: S.B. 872; Nebraska: L.B. 58; New Hampshire: H.B. 414; New Jersey: A.B. 2878; New York: A.B. 443, S.B. 1701, S.B. 2434; North Carolina: H.B. 846; North Dakota: H.B. 1455; Texas: H.B. 318, H.B. 451, S.B. 118, S.B. 416.

[57] California: CAL. LAB. CODE § 980(b)(2) (2013) (prohibiting also a request to divulge any personal social media); Michigan: MICH. COMP. LAWS §§ 37.273(a) (2012); Georgia: H.B. 149, H.B. 117; Hawaii: H.B. 713, S.B. 207; Iowa: H.F. 127; Nebraska: L.B. 58; North Carolina: H.B. 846; North Dakota: H.B. 1455; Washington: S.B. 5211.

[58] Kansas: H.B. 2092, S.B. 53; New Jersey: A.B. 2878. Rhode Island would also prohibit employers from requesting or requiring that employees or job applicants divulge any personal social media information except when reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations; provided, that the social media account is used solely for purposes of that investigation or a related proceeding. S.B. 493.

[59] Arkansas: Act 1480 (to be codified at ARK. CODE ANN. § 11-2-124(b) (2013)) (prohibiting requiring, requesting, suggesting, or causing, rather than compelling); Colorado: H.B. 13-1046 (to be codified at COLO. REV. STAT. § 8-2-127(2)(a)); Maine: H.P. 838 (including also an employee's or applicant's e-mail account); Massachusetts: H.B. 1707, S.B. 852 (excluding the prohibition regarding changing privacy settings); New Hampshire: H.B. 414; North Carolina: H.B. 846 (prohibiting requesting or requiring, rather than compelling; excluding the prohibition regarding changing privacy settings); Oregon: H.B. 2654, S.B. 499 (excluding the prohibition regarding changing privacy settings); Rhode Island: H.B. 5255, S.B. 493; Washington: S.B. 5211 (prohibiting employers from requesting, requiring, or causing an employee or applicant to alter the settings on his or her personal social networking account that affect a third party's ability to view the contents of the account).

[60] Nebraska: L.B. 58; North Carolina: H.B. 846.

[61] Nebraska: L.B. 58; New Jersey: A.B. 2878; North Dakota: H.B. 1455.

[62] H.B. 318

[63] Arkansas: Act 1480 (to be codified at ARK. CODE ANN. § 11-2-124(c); California: CAL. LAB. CODE § 980(e) (2013); Colorado: H.B. 13-1046 (enacted May 11, 2013) (to be codified at COLO. REV. STAT. § 8-2-127(3)); Maryland: MD. CODE ANN., LAB. & EMPL. § 3-712(c) (2012); Michigan: MICH. COMP. LAWS §§ 37.273(b) (2012); Utah: H.B. 100 (to be codified at UTAH CODE ANN. § 34-48-201(2) (2013)); U.S. Congress: H.R. 537; Arizona: S.B. 1411; Connecticut: C.B. 159; Georgia: H.B. 149; Hawaii: H.B. 713, S.B. 207; Illinois: H.B. 1047; Iowa: H.F. 127, H.F. 272; Kansas: H.B. 2092, S.B. 53; Louisiana: H.B. 314; Maine: H.P. 838; Massachusetts: H.B. 1707, S.B. 852; Missouri: H.B. 115, H.B. 706, S.B. 164; Nebraska: L.B. 58; Nevada: A.B. 181; New Hampshire: H.B. 414; New Jersey: A.B. 2878; New York: A.B. 443, S.B. 1701, S.B. 2434; North Carolina: H.B. 846; North Dakota: H.B. 1455; Ohio: S.B. 45; Oregon: H.B. 2654, S.B. 499; Pennsylvania: H.B. 1130; Rhode Island: H.B. 5255, S.B. 493; Washington: SB. 5211; West Virginia: H.B. 2966.

[64] U.S. Congress: H.R. 537; Connecticut: C.B. 159; Nebraska: L.B. 58; New Jersey: A.B. 2878; North Dakota: H.B. 1455.

[65] Maryland: MD. CODE ANN., LAB. & EMPL. § 3-712(d); Arizona: S.B. 1411; Iowa; H.F. 272; Missouri: H.B. 706, S.B. 164; Nebraska: L.B. 58; North Dakota: H.B. 1455; West Virginia: H.B. 2966.

[66] Arkansas: Act 1480 (to be codified at ARK. CODE ANN. § 11-2-124(e)(1)); Maryland: MD. CODE ANN., LAB. & EMPL. § 3-712(e)(1); Michigan: MICH. COMP. LAWS §§ 37.275(1)(c)(i); Utah: H.B. 100 (to be codified at UTAH CODE ANN. § 34-48-202(1)(c)(i)); Arizona S.B. 1411; Illinois: H.B. 1047; Louisiana: H.B. 314; Missouri: H.F. 706, S.B. 164; New Hampshire: H.B. 414; New Jersey: A.B. 2878; New York: A.B. 443, S.B. 2434; Oregon: H.B. 2654; Texas: H.B. 318; Washington: S.B. 5211.

[67] Arkansas: Act 1480 (to be codified at ARK. CODE ANN. § 11-2-124(e)(2)); California: CAL. LAB. CODE § 980(c); Georgia H.B. 117, H.B. 149; Hawaii: H.B. 713; Illinois: H.B. 1047; Iowa: H.F. 127; Kansas: H.B. 2092, S.B. 53; Louisiana:

H.B. 314; Missouri: H.B. 706, S.B. 164; New Jersey: A.B. 2878; New York: A.B. 443, S.B. 2434; North Carolina: H.B. 846; Oregon: H.B. 2654; Rhode Island: H.B. 5255, S.B. 493.

[68] Colorado: H.B. 13-1046 (to be codified at COLO. REV. STAT. § 8-2-127(4)(a)); Arizona: 1411; Hawaii: S.B. 207; Iowa: H.F. 272; Massachusetts: S.B. 872; New Hampshire: H.B. 414; West Virginia: H.B. 2966.

[69] Colorado: H.B. 13-1046 (to be codified at COLO. REV. STAT. § 8-2-127(6)); Illinois: 820 ILL. COMP. STAT. 55/10 §10(b)(2)(A) (2013); New Mexico: S.B. 371 (enacted Apr. 5, 2013); Arizona: 1411; Illinois: H.B. 1047, S.B. 2306; Massachusetts: H.B. 1707; Minnesota: H.F. 293, H.F. 611, S.F. 484, S.F. 596; Missouri: H.B. 1020; Nebraska: L.B. 58; New Hampshire: H.B. 414; New Jersey: A.B. 2878; North Carolina: H.B. 846; North Dakota: H.B. 1455; Pennsylvania: H.B. 1130.

[70] Illinois: 820 ILL. COMP. STAT. 55/10 §10(b)(2)(B); Michigan: MICH. COMP. LAWS §§ 37.275(1)(a)(i); New Mexico: S.B. 371 (enacted Apr. 5, 2013); Massachusetts: S.B. 872; Missouri: H.B. 1020; New Hampshire: H.B. 414; Ohio: S.B. 45; Pennsylvania: H.B. 1130; Texas: H.B. 318, H.B. 451, S.B. 118, S.B. 416.

[71] Michigan: MICH. COMP. LAWS §§ 37.275(1)(e); Hawaii: H.B. 713; Iowa: H.F. 127; Missouri: H.B. 706, S.B. 164; New York: A.B. 443, S.B. 2434.

[72] California: CAL. LAB. CODE § 980(d); Colorado: H.B. 13-1046 (to be codified at COLO. REV. STAT. § 8-2-127(2)(b)); Maryland: MD. CODE ANN., LAB. & EMPL. § 3-712(b)(2); Arizona: S.B. 1411; Georgia: H.B. 117; Hawaii: H.B. 713, S.B. 207; Iowa: H.F. 127, H.F. 272; Kansas: H.B. 2092, S.B. 53; Louisiana: H.B. 314; Missouri: H.B. 115, H.B. 706, S.B. 164; Nebraska: L.B. 58; Nevada: A.B. 181; New York: A.B. 443, S.B. 1701, S.B. 2434; North Carolina: H.B. 846; North Dakota: H.B. 1455; Oregon: H.B. 2654, S.B. 499; Texas: H.B. 318, H.B. 451, S.B. 118, S.B. 416; Washington: S.B. 5211.

[73] Utah: H.B. 100 (to be codified at UTAH CODE ANN. § 34-48-202(1)(a)(ii) (2013)); Illinois: H.B. 1047; Iowa: H.F. 127; Massachusetts: H.B. 1707, S.B. 852; Missouri: H.B. 706, S.B. 164; Nebraska: L.B. 58; Washington: S.B. 5211.

[74] Colorado: H.B. 13-1046 (to be codified at COLO. REV. STAT. § 8-2-127(4)(b)); Maryland: MD. CODE ANN., LAB. & EMPL. § 3-712(e)(2); Michigan: MICH. COMP. LAWS §§ 37.275(1)(b); Utah: H.B. 100 (to be codified at UTAH CODE ANN. § 34-48-202(1)(b)); Hawaii: S.B. 207; Illinois: H.B. 1047; Iowa: H.F. 127, H.F. 272; Louisiana: H.B. 314; Massachusetts: S.B. 872; Missouri: H.B. 706, S.B. 164; Nebraska: L.B. 58; New Jersey: A.B. 2878; New York: A.B. 443, S.B. 2434; North Dakota: H.B. 1455; Washington: S.B. 5211.

[75] Arkansas: Act 1480 (to be codified at ARK. CODE ANN. § 11-2-124(d) (2013)); Illinois: 820 ILL. COMP. STAT. 55/10 §10(b)(3); New Mexico: S.B. 371 (enacted Apr. 5, 2013); Utah: H.B. 100 (to be codified at UTAH CODE ANN. § 34-48-202(4)); Illinois: 1047, S.B. 2306; Iowa: H.F. 127, H.F. 272; Louisiana: H.B. 314; Maine: H.P. 838; Massachusetts: H.B. 1707, S.B. 852; Missouri: H.F. 706, H.B. 1020, S.B. 164; Nebraska: L.B. 58; New Hampshire: H.B. 414; New Jersey: A.B. 2878; New York: A.B. 443, S.B. 2434; North Carolina: H.B. 846; North Dakota: H.B. 1455; Oregon: H.B. 2654; Pennsylvania: H.B. 1130; Rhode Island: H.B. 5255, S.B. 493; Texas: H.B. 318, H.B. 451, S.B. 118, S.B. 416.

[76] California: CAL. LAB. CODE § 980(e); Georgia: H.B. 149; Hawaii: H.B. 713, S.B. 207.

[77] Michigan: MICH. COMP. LAWS § 37.277(1); Utah: H.B. 100 (to be codified at UTAH CODE ANN. § 34-48-203); Iowa: H.F. 127.

[78] Michigan: MICH. COMP. LAWS § 37.277(2);Utah: H.B. 100 (to be codified at UTAH CODE ANN. § 34-48-203); Hawaii: H.B. 713, S.B. 207; Illinois: H.B. 1047; Iowa: H.F. 127; Missouri: H.B. 706, S.B. 164; Oregon: H.B. 2654.

[79] Arkansas: Act 1480 (to be codified at ARK. CODE ANN. § 11-2-124(b)(2)); Michigan: MICH. COMP. LAWS § 37.275(3); Louisiana: H.B. 314; Oregon: H.B. 2654; Washington: S.B. 5211.

[80] As noted *supra* note 65, seven states prohibit, or would prohibit, employees from downloading without authorization an employer's proprietary information or financial data to the employee's personal website, an Internet website, a web-based account, or any similar account. Of those seven states, three provide for remedies—one of Iowa's bills, H.F. 127, limits remedies to only violations relating to employer prohibitions, but Nebraska's remedies in L.B. 58 and North Dakota's remedies in H.B. 1455 could also apply when the employer is the aggrieved party.

[81] Michigan: MICH. COMP. LAWS § 37.278(2) (providing for damages up to $1,000, injunctive relief, plus attorney fees and court costs); Utah: H.B. 100 (to be codified at UTAH CODE ANN. § 34-48-301) (providing for damages up to $500); Georgia: H.B. 149 (providing for compensatory and consequential damages, plus attorney fees and court costs); Iowa: H.F. 127 (providing for injunctive relief, damages up to $1,000, plus attorney fees and court costs); Maine: H.P. 838 (providing for an amount up to three times lost wages, reinstatement, civil damages up to $1,000, plus attorney fees and court costs); Nebraska: L.B. 58 (providing for actual damages, plus attorney fees and court costs); New Jersey: A.B. 2878 (providing for injunctive relief with possible reinstatement, compensatory & consequential damages, plus attorney fees and court costs); North Dakota: H.B. 1455 (providing for actual damages, plus attorney fees and court costs); Rhode Island: H.B. 5255, S.B. 493 (providing for injunctive relief, actual and punitive damages, plus attorney fees and court costs); Washington: S.B. 5211 (providing for actual damages plus a penalty of $500, attorney fees and court costs; providing also that an employer may be awarded attorney fees and expenses if a frivolous action is brought).

[82] Colorado: H.B. 13-1046 (to be codified at COLO. REV. STAT. § 8-2-127(5) (2013)) (authorizing the Department of Labor and Employment to promulgate rules regarding penalties that include fines of up to $1,000 for a first offense and up to

$5,000 for each subsequent offense); Michigan: MICH. COMP. LAWS § 37.278(1) (providing for a misdemeanor fine up to $1,000); U.S. Congress: H.R. 5050 (providing for a fine up to $10,000 plus injunctive relief); Connecticut: S.B. 149 (providing for a civil fine up to $10,000 plus other equitable relief as the court deems appropriate); Georgia: H.B. 117 (providing for a statutory fine between $200-$400), H.B. 149 (providing for a fine up to $1,000 per violation); Iowa: H.F. 127 (providing a misdemeanor punishable by a fine up to $1,000 per violation); Maine: H.P. 838 (providing for a civil penalty up to $1,000 and up to $2,000 for any subsequent offense, payable to the affected employee or applicant); New Jersey: A.B. 2878 (providing for civil fine up to $1,000 for the first violation and up to $2,500 for each subsequent violation); New Hampshire: H.B. 414 (providing for civil penalty imposed pursuant to N.H. REV. STAT. § 273:11-a, which provides a civil penalty up to $2,500); New York: S.B. 1701 (providing for injunctive relief, and civil fines up to $300 for the first violation and up to $500 for each subsequent violation); Ohio: S.B. 45 (providing for civil fines up to $1,000 for the first violation and up to $2,000 for each subsequent violation); Pennsylvania: H.B. 1130 (providing for a civil penalty up to $5,000).

[83] Manuel Valdes & Shannon McFarland, *Job Seekers Getting Asked for Facebook Passwords*, YAHOO! FINANCE (Mar. 20, 2012, 7:55 AM), http://finance.yahoo.com/news/job-seekers-getting-asked-facebook-passwords-071251682.html (recounting two incidents with named job applicants, including Robert Collins in Maryland (*see supra* notes 1-3 and accompanying text), and identifying three separate government entities that have currently or in the past asked for job applicant social media access). "In their efforts to vet applicants, some companies and government agencies are going beyond merely glancing at a person's social networking profiles and instead asking to log in as the user to have a look around." *Id.*

[84] *See, e.g.*, Sarah Shemkus, *Employers Asking for Facebook Passwords: Privacy Concern or Evolution of the Job Interview?*, SALARY.COM, http://www.salary.com/employers-asking-for-facebook-passwords-privacy-concern-or-evolution-of-the-job-interview/ (last visited May 17, 2013) (noting the "uproar" caused by Valdes's and McFarland's article that "reported on the trend of employers demanding access to applicants' Facebook accounts"); *see also* James Poulos, *Employers Demanding Facebook Passwords Aren't Making Any Friends*, FORBES (Mar. 22, 2012, 12:12 PM), http://www.forbes.com/sites/jamespoulos/2012/03/22/employers-demanding-facebook-passwords-arent-making-any-friends (suggesting that employers are "increasingly" requesting access to job applicants' Facebook pages as a condition of employment).

[85] *See supra* notes 1-6 and accompanying text; Tuan C. Nguyen, *Want to Get Hired? Please Provide Your Facebook Password*, SMARTPLANET (Dec. 21, 2011, 5:30 AM), http://www.smartplanet.com/blog/thinking-tech/want-to-get-hired-please-provide-your-facebook-password/9557 (reporting that a woman applying for work as a phone operator at a local police department in North Carolina was asked to provide usernames and passwords to her online social media accounts on the application form; providing also a picture of the application form); City of Bozeman, Montana, *Consent and Release to Conduct Criminal Background and Reference Checks*, ERBLAWG.COM, http://www.erblawg.com/wp-content/uploads/2009/06/erblawbozeman.pdf (last visited May 16, 2013) (displaying copy of Consent and Release to Conduct Criminal Background and Reference Checks form for job applicants to the City of Bozeman, Montana, reflecting a request for usernames and passwords to social media accounts); Matt Gouras, *City Drops Request for Internet Passwords*, NBCNEWS.COM (June 19, 2009, 8:42 PM), http://www.nbcnews.com/id/31446037/ns/technology_and_science-security/#.UZU1WkoSr7I (reporting that "[a] flood of criticism . . . prompted a Montana city [Bozeman] to drop its request that government job applicants turn over their user names and passwords to Internet social networking and Web groups"); Valdes & McFarland, *supra* note 83 (reporting that in addition to Robert Collins, Justin Bassett, a New York City statistician, had been asked to log into his Facebook account in the presence of a job interviewer, and that in addition to the city of Bozeman, Montana, the McLean County, Illinois and Spotsylvania County, Virginia sheriff's offices had routinely requested online access information). *But see infra* note 146 and accompanying text (presenting evidence that employers may be asking for access to employees' online social networks, though not by requesting usernames and passwords).

[86] *See* JAN HAROLD BRUNVAND, I ENCYCLOPEDIA OF URBAN LEGENDS, UPDATED AND EXPANDED EDITION 241 (2012) (noting that "friend of a friend"—often denoted by the acronym FOAF—is "the oft-mentioned supposed original source of the incidents described in urban legends"); Mary B. Nicolini, *Is There a FOAF in Your Future? Urban Folk Legends in Room 112*, 78 ENG. J. 81, 81 (1989) ("A necessary component of the folk legend is the FOAF: a friend of a friend, as in 'This didn't happen to me, but it happened to a friend of a friend of mine. . . .' This is designed to lend authenticity to the tale and the teller; while not a firsthand witness, the teller has it from very good sources.") (alteration in original).

[87] Although Valdes and McFarland do not identify the employer Justin Bassett, the New York statistician, was interviewing with, all other documented incidents have involved a governmental entity. *See* Valdes & McFarland, *supra* note 83; *supra* notes 1-6 and accompanying text.

[88] LITTLER MENDELSON, EXECUTIVE EMPLOYER SURVEY REPORT 15 (2012), *available at* http://www.littler.com/files/Littler%20Mendelson%20Executive%20Employer%20Survey%20Report%202012_06-25-12.pdf.

[89] *Id.*; *see also* PHILLIP L. GORDON ET AL., SOCIAL MEDIA PASSWORD PROTECTION AND PRIVACY—THE PATCHWORK OF STATE LAWS AND HOW IT AFFECTS EMPLOYERS 3 (2013), *available at* http://www.littler.com/files/press/pdf/LittlerReportSocialMediaPasswordProtectionaAndPrivacyThePatchworkOfStateLawsA

ndHowItAffectsEmployers.pdf ("Both the available anecdotal and empirical evidence, albeit limited, compel the conclusion that private employers are not asking applicants or employees for personal social media log-in credentials.").

[90] Jon Hyman, *The Results Are In: Social Media Password Survey*, OHIO EMPLOYER'S LAW BLOG (Apr. 4, 2013), http://www.ohioemployerlawblog.com/2013/04/the-results-are-in-social-media.html (concluding "this supposed practice is not much more than an answer in search of a problem").

[91] *But see infra* notes 146 & 148 and accompanying text (discussing that some supervisors and executives may be requesting employees "Friend" them and suggestions as to why employees comply).

[92] *See* Augenstein, *supra* note 15 (reporting that Maryland's Attorney General defended the social media screening practice of the Department of Corrections as necessary to ferret out possible gang affiliations of applicants); Valdes & McFarland, *supra* note 83 (reporting two sheriff's departments that use social media access to screen applicants). A few of the statutes and proposed laws exempt law enforcement agencies from coverage. *See, e.g.*, New Mexico: S.B. 371 (enacted Apr. 5, 2013); New Jersey: A.B. 2878 (excluding law enforcement agencies from the definition of employer); Texas: H.B. 318.

[93] *See, e.g.*, Shemcus, *supra* note 84 (reporting that in March 2012, Senators Richard Blumenthal (D-Conn.) and Charles E. Schumer (D-N.Y.) "sent letters to the U.S. Equal Employment Opportunity Commission and the U.S. Department of Justice asking the agencies to launch investigations into the legality of what they called 'the disturbing trend'" of employers requesting social media passwords); California A.B. 1844 Synopsis (2011-2012 Sess.) (codified at CAL. LAB. CODE § 980 (2013)) (noting that "[r]ecent media accounts have reported that some employers may have demanded access to the private social media accounts of employees and prospective employees, and these reports have naturally generated significant public concern across California and the entire nation about such potential encroachments on individual privacy. In response, several states including Maryland, Texas and Illinois are also considering similar legislation to prohibit this practice."); *LD 1194—Ought to Pass: Hearing on H.P. 838 [L.D. 1194] Before the Joint Standing Comm. on Judiciary*, 126th Leg., 1st Reg. Sess. (Me. 2013) (testimony of Shenna Bellows, ACLU Maine) (asserting that "[a] growing number of employers and schools are demanding that job applicants, employees, and students hand over the passwords to their private social media accounts such as Facebook" but identifying only one actual incident—Maryland's Robert Collins as described *supra* notes 1-3 and accompanying text); *Bus. & Labor Comm.*, 103rd Leg., 1st Sess. (Ne. 2013) (statement of Sen. Larson) (noting that "[s]ix other states including Michigan, Illinois, and California, have passed laws similar to [Nebraska's L.B. 58] with the intent to protect the privacy of employees and applicants on the Internet); New York A.B. 443 Justification ("Recently, there have been reports of employers demanding login information, including username and password information to popular social media websites such as Facebook, Twitter [sic] as well as login information to email accounts and other extremely personal accounts."); Washington S.B. 5211 (Comm. Rep) (noting that "six states enacted legislation in 2012 to prohibit employers or institutions of higher education from requiring an employee, applicant, or student to provide a username or password to a social media account" and that "Washington law does not address requests by an employer to access to an employee's or prospective employee's social networking accounts").

[94] Pietrylo v. Hillstone Rest. Grp., No. 06–5754, 2008 WL 6085437, at *1 (D. N.J. July 25, 2008) (internal quotation marks omitted). The MySpace page also stated, "This group is entirely private, and can only be joined by invitation." *Id.* (internal quotation marks omitted).

[95] *Id*.

[96] *Id.* at *2.

[97] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, Title II, ch. 121, 100 Stat. 1848, 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701–12 (2006)).

[98] *Pietrylo*, 2008 WL 6085437, at *2.

[99] 18 U.S.C. § 2701(a).

[100] *Id.* at § 2701(c)(2).

[101] Pietrylo v. Hillstone Rest. Grp., No. 06–5754, 2009 WL 3128420, at *3 (D. N.J. Sept. 25, 2009). The jury, however, rejected the plaintiffs' common law privacy claim. *Id.* at *1.

[102] *Cf.* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 880 (9th Cir. 2002) (holding that management's access to an employee's restricted-access website by requesting access information from authorized users violated the SCA because the users had never actually "used" the website in question and therefore were not technically "users" who could authorize access under 18 U.S.C. § 2701(c)(2)).

[103] "This practice is coercion if you need a job." Joshua Waldman, *What to Do if a Company Asks for Your Facebook Password in a Job Interview*, THE LADDER, http://www.theladders.com/career-advice/what-to-do-if-company-asks-for-facebook-password-in-job-interview (last visited May 17, 2013) (quoting Lori Andrews, IIT Chicago-Kent College of Law professor) (internal quotation marks omitted). Waldman presents a compelling scenario for coercion:

> Imagine you've been on the job market for about six months. You are paying your mortgage on your credit cards at this point. Your unemployment benefits are about to run out and your job prospects remain dismal, no matter what you seem to do.

> Finally, you land a killer opportunity, pass the phone screen and show up to an interview with a hiring manager. Just as you think you're about to close the deal, she spins her computer screen around and asks you to login to your Facebook account.

Id.

[104] Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 872 F. Supp. 2d 369, 370 (D. N.J. 2012).

[105] *Id.*

[106] *Id.* at 374.

[107] Ehling's SCA claim against MONOC was not addressed in *Ehling v. Monmouth-Ocean Hosp. Serv. Corp*. *See* Amended Complaint at 12, Ehling v. Monmouth-Ocean Hosp. Serv. Corp. (2007) (No. 2-11-CV-03305 (WJM)).

[108] *But see supra* note 60 and accompanying text (discussing two states which would prohibit employers from accessing an employee's or job applicant's social networking profile or account indirectly through any other person who is a social networking contact of the employee or applicant).

[109] 587 F. Supp. 2d 548, 552 (S.D.N.Y. 2008).

[110] *Id.* The employer was able to also access the former employee's personal Gmail account because the employee had e-mailed his Gmail username and password to his Hotmail account. *Id.* The employer also "guessed" the former employee's password for his e-mail account at the new, competing business he had opened. *Id.*

[111] *Id.* at 561.

[112] *Id.* at 562.

> There is no sound basis to argue that [the former employee], by inadvertently leaving his Hotmail password accessible, was thereby authorizing access to all of his Hotmail e-mails, no less the e-mails in his two other accounts. If he had left a key to his house on the front desk at [Pure Power Boot Camp], one could not reasonably argue that he was giving consent to whoever found the key, to use it to enter his house and rummage through his belongings. And, to take the analogy a step further, had the person rummaging through the belongings in [the employee's] house found the key to [his] country house, could that be taken as authorization to search his country house. We think not. The Court rejects the notion that carelessness equals consent.

Id. at 561.

[113] Borchers v. Franciscan Tertiary Province of Sacred Heart, Inc., 962 N.E.2d 29 (Ill. App. Ct. 2011).

[114] *Id*. at 689, 692.

[115] *Id.* at 697-98.

[116] *Compare* Stengart v. Loving Care Agency, 990 A.2d 650 (N.J. 2010) (holding that an employee had a privacy interest in e-mail messages stored on a personal online account), *with* Holmes v. Petrovich Dev. Co., 191 Cal. App. 4th 1047, 1051, 119 Cal. Rptr. 3d 878, 883 (Cal. App. 2011) (concluding that an employee had no privacy right in personal e-mail messages sent to her attorney through her employer's e-mail system; analogizing her e-mails "to consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by him").

[117] *See supra* note 54 and accompanying text.

[118] *See supra* note 75 and accompanying text.

[119] *See* Maremont v. Susan Fredman Design Grp., No. 10 C 7811, 2011 WL 6101949, at *7 (N.D. Ill Dec. 7, 2011); *see also* Sumien v. CareFlite, No. 02–12–00039–CV, 2012 WL 2579525, at *3 (Tex. App. July 5, 2012) (refusing to find a right of privacy in Facebook posts viewed by a friend-of-a-friend); Gill v. Hearst Publ'g Co., 253 P.2d 441, 444–45 (Cal. 1953) (holding that a couple photographed at a farmer's market had no cause of action against the photograph's publisher).

[120] *See supra* notes 99-103, 112, and 115, and accompanying text.

[121] *See supra* notes 40-42 and accompanying text.

[122] *See* Patricia Sánchez Abril et al., *Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee*, 49 AM. BUS. L.J. 63, 64 (2012) ("Employer-provided laptops and mobile devices do not discriminate between private and professional communications or locations. These 'boundary-crossing' technologies blur the already elusive line between the private and the public, the home and the workplace.").

[123] No. 10 C 7811, 2011 WL 6101949, at *2 (N.D. Ill. Dec. 7, 2011).

[124] *Id.*

[125] *Id.*

[126] *Id.* at *2-3.

[127] *Id.* at *5.

[128] *See id.* at *2.

[129] No. 11 Civ. 5013(NRB), 2011 WL 4965172 (S.D.N.Y. Oct. 19, 2011).

[130] *Id.* at *1.

[131] *Id.* at *2.

[132] *Id.*

[133] *Id*. at *3.
[134] *Id.* at *2.
[135] *Id.* ("The inability to [continuously update their profiles and pages and react to online trends] unquestionably has a negative effect on plaintiffs' reputation and ability to remain competitive, and the magnitude of that effect is difficult, if not impossible, to quantify in monetary terms. Such injury constitutes irreparable harm.")
[136] *Id.* at *4-5 (denying plaintiffs' motion requesting the defendant to remove the material).
[137] Maremont v. Susan Fredman Design Grp., Ltd., No. 10 C 7811, 2011 WL 6101949, at *4-5, 6-8 (N.D. Ill. Dec. 7, 2011).
[138] *See* Eagle v. Morgan, No. 11–4303, 2013 WL 943350 (E.D. Pa. Mar. 12, 2013); PhoneDog v. Kravitz, No. C 11–03474 MEJ, 2011 WL 5415612 (N.D. Cal. Nov. 8, 2011), 2012 WL 273323 (N.D. Cal. Jan. 30, 2012); Christou v. Beatport, LLC, 849 F. Supp. 2d 1055 (D. Colo. 2012); Zoe Argento, *Whose Social Network Account? A Trade Secret Approach to Allocating Rights*, 20 MICH. TELECOMM. & TECH. L. REV. (forthcoming 2013), *available at* http://ssrn.com/abstract=2187511 (arguing that these disputes are ultimately about the right to access the accounts' followers, necessitating a trade secrets approach to their resolution).
[139] GORDON ET AL., *supra* note 89, at 4.
[140] *See supra* pages 11-14 discussing employer exemptions.
[141] Abril et al., *supra* note 122, at 98.
[142] *Id.* at 102.
[143] *Id*. at 103.
[144] *Id.* at 107.
[145] *Id.*
[146] *Id.* at 107-08.
[147] *See supra* note 59 and accompanying text.
[148] Abril et al., *supra* note 122, at 109.
[149] This practice could arguably be illegal in the future in Nebraska and, again in North Carolina, via the employer indirectly accessing employee and job applicant online profiles through existing Friends, which could arguable include current or potential supervisors. *See supra* note 60 and accompanying text.
[150] *See supra* text following note 107.
[151] *See supra* note 60 and accompanying text (discussing Nebraska's and North Carolina's proposed laws which would prohibit employers from accessing an employee's or job applicant's social networking profile or account indirectly through any other person who is a social networking contact of the employee or applicant).
[152] *See supra* notes 123-128 and accompanying text.
[153] 820 ILL. COMP. STAT. 55/10 §10 (2013).
[154] *See supra* note 36 and accompanying text.
[155] *See supra* notes 109-112 and accompanying text.
[156] *See supra* notes 113-115 and accompanying text.
[157] *Pure Power Boot Camp* and *Borchers* raise an additional issue. Both cases involved former employees, so arguably their former employers would no longer be considered "employers" for purposes of applying the legislation. Or would "employer" status relate back to when the employee actually worked for the employer since the employer's access to the account arose from the original employment relationship?
[158] H.B. 318.
[159] *See* Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979, 1027-28 (2011) (discussing that employee consent is actually "involuntary" due to the typical balance of power in the employment relationship).
[160] Nebraska: L.B. 58; New Jersey: A.B. 2878; North Dakota: H.B. 1455.
[161] *See, e.g.*, Waldman, *supra* note 103 (describing a "coercion" scenario for a "typical" job applicant).
[162] *See supra* note 149 and accompanying text (discussing prohibitions against employers requiring or requesting that they be "Friended" by an employee or job applicant).
[163] *See supra* notes 88-90 and accompanying text.
[164] *See supra* notes 63-64 and accompanying text.
[165] *See supra* notes 81-82 and accompanying text.
[166] *See supra* notes 158-161 and accompanying text.
[167] *See supra* text following note 119.
[168] *See supra* note 93 and accompanying text.
[169] *Cf.* Kenneth N. Waltz, *Kant, Liberalism, and War*, 56 AM. POL. SCI. REV. 331, 332 (1956) ("The purpose of legislation is negative: to 'hinder hindrances' to freedom so that each may enjoy his antecedently existing rights unmolested.").
[170] Howard Newcomb Morse, *Theories of Legislation*, 14 DEPAUL L. REV. 51, 51 (1964).

[171] *See* Hyman, *supra* note 90.