The Global Business Law Review

Volume 7 | Issue 1 Note

7-1-2018

Workplace Privacy in the Age of Social Media

Tess Traylor-Notaro
Cleveland-Marshall College of Law

WORKPLACE PRIVACY IN THE AGE OF SOCIAL MEDIA

TESS TRAYLOR-NOTARO

ABSTRACT

This note addresses the lack of adequate protections in Ohio for social media privacy laws in the workplace and compares proposed legislation in Ohio to legislation that has passed in other states. It examines the provision of the SCA including the definition of "user" and whether social media sites fall under its umbrella. It also looks at the safeguards and limitations of the SCA and how it is used to protect a private employee's social media account. It analyzes the state statutory laws in Arkansas, Illinois, and California passed specifically to prevent employers from requesting passwords to personal Internet accounts. The note then analyzes Canada's approach to workplace privacy. Finally, based on this analysis, it looks at the proposed House Bill in Ohio and argues that Ohio should pass a bill prohibiting employers from requesting access to employees' social media accounts, and offers suggestions on what this bill should include.

I. INTRODUCTION

In 2010, during an interview with the Maryland Department of Public Safety and Correctional Services, Robert Collins was directed by the interviewee to provide his username and password for Facebook, even though he maintained his account privately.[1] After leaving the interview, Collins contacted the American Civil Liberties Union, who drafted a letter to the Department on his behalf, calling the practice an "invasion of privacy."[2] Eventually, Collins was rehired, the Department suspended its practice, and a lawsuit was avoided. In response to Collins's situation, Maryland became the first state to pass a bill prohibiting employers from requesting employees or job applicants to disclose their social media passwords.[3]

The increasing use of social media sites continues to generate issues of employee rights to privacy in the workplace.[4] Fortunately for Collins, public employees have greater privacy protections in the workplace than private employees. Unlike employees in the private sector, public employees can assert Constitutional rights to due process under the Fourteenth Amendment[5] and the right to be free from unreasonable searches and seizures under the Fourth Amendment.[6] Additionally, public employees may be able to recover on the theory that their First Amendment rights have been infringed.[7]

Although public employees enjoy greater protection from invasion of privacy in the workplace, some private employees are protected by statutes that regulate private employers' conduct.[8] As of 2017, twenty-five states have enacted legislation that restricts employers from requesting access to an employee's private social media account.[9] Currently, Ohio is not one of

---

[1] Lisa Sween & Jessica Luke, *2012 Emerging Issues 6788, California AB 1844: Limiting Employers' Access to Employees' Social Media*, MATTHEW BENDER & COMPANY, INC. (Nov. 28, 2012), https://www.lexisnexis.com/ legalnewsroom/workers-compensation/b/recent-cases-news-trends-developments/archive/2012/12/12/california-enacts-law-limiting-employers-access-to-employees-social-media.aspx

[2] *Id.*

[3] *See id.*; *see also* MD LAB. & EMP. CODE § 3-712 (2013) (prohibiting specified employers from requiring an employee or applicant for employment to provide the employer with access to specified Internet sites or electronic accounts through specified electronic devices).

[4] Sween & Luke, *supra* note 1; *see also* Manuel Valdes & Shannon McFarland, *Employers Ask Job Seekers for Facebook Password*, SEATTLE TIMES (March 20, 2012, 6:27 PM) *available at* http://www.seattletimes.com/nation- world/employers-ask-job-seekers-for-facebook-passwords/. When Justin Bassett of New York interviewed for a new job, the interviewer turned to her computer to search for his Facebook page, but could not see his private profile. She then asked him to hand over his login information. Bassett refused and withdrew his application, saying he did not want to work for a company that would seek such personal information. For those who are in desperate need of a job, however, saying "no" may not always be an option. *Id.*

[5] U.S. CONST. amend. XIV, § 1.

[6] U.S. CONST. amend. IV, § 1; Jackson v. Metropolitan Edison Co., 95 S. Ct. 449, 455-57 (1974); *see also* 13A SHARON P. STILLER, EMPLOYMENT LAW IN NEW YORK § 6:2 (2d ed. 2015).

[7] U.S. CONST. amend. I; Rankin v. McPherson, 107 S. Ct. 2891 (1987).

[8] *See generally* Pam Greenberg, *State Social Media Privacy Laws*, NAT'L CONF. ST. LEGIS. (last updated July 6, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx#stat.

these states, although a bill has been proposed in the House.[10] Lack of legislation does not mean that private employees in Ohio are completely without recourse when their employer asks to access their private social media account. Depending on the situation, an employee may be able to claim a violation under the Stored Communications Act (SCA) to protect his job, his secured social network site, and in turn, his privacy.[11] However, the SCA is limited in its protection of employees' and applicants' private social media sites.[12]

This note addresses the lack of adequate protections in Ohio for workplace social media privacy laws and compares its proposed legislation to legislation that has passed in other states. Section II will discuss privacy risks raised by the prevalence of social media. It will then examine the relevant provisions of the SCA, including the definition of "user" and whether social media sites, such as Facebook, fall under its umbrella. This section ends by looking at the safeguards and limitations of the SCA and whether it can be applied to protect a private employee's social media account. Section III will analyze the state statutory laws in Arkansas,[13] Illinois,[14] and California[15] —three of the 25 states that provide protections to employees and applicants. This section also looks at how Canada approaches workplace privacy and compares its law to state law in the United States. Finally, section III concludes by examining the proposed Ohio House Bill and argues that Ohio should pass a bill prohibiting employers from requesting access to employees' social media accounts, and offers suggestions on what this bill should include.[16]

II. BACKGROUND

A. Growing Online Usage of Social Media Sites by Adults

As of 2014, Facebook had 1.2 billion monthly active users around the world, with American and Canadian users making up less than a sixth of Facebook's total user base.[17] However, Americans and Canadians are some of the most active users.[18] According to company data, on any given day in December, 73% of Facebook's American and Canadian users visited the site, used its messenger app, or shared content with Facebook friends via an affiliated third

---

[9] *Id.*

[10] *See* H.B. 424, 130th Gen. Assemb., Reg. Sess. (Ohio 2014).

[11] 18 U.S.C.A. § 2701(a) (Current through Pub. L. 114-38).

[12] *See generally* Ehling v. Monmouth-Ocean Hosp. Service Corp., 961 F. Supp. 2d 659 (2013).

[13] ARK. CODE ANN. § 11-2-124 (2014).

[14] 820 ILL. COMP. STAT. 55 (2013).

[15] CALIF. LAB. CODE § 980 (2012).

[16] H.B. 424, 130th Gen. Assemb., Reg. Sess. (Ohio 2014).

[17] Drew Desilver, *Overseas Users Power Facebook's Growth: More Going Mobile Only*, PEW RES. CTR. (Feb. 4, 2014), http://www.pewresearch.org/fact-tank/2014/02/04/overseas-users-power-facebooks-growth-more-going-mobile-only/.

[18] *Id.*

party.[19]

As of October 2016, Twitter had 313 million monthly active users[20] and Instagram had 500 million monthly active users.[21] All these sites include customizable privacy settings that allow users to restrict access to their content. For example, on Facebook, access can be limited to a user's Facebook friends, to particular groups or individuals, or to just the user. Facebook provides users with ways of communicating with others privately.[22] According to one study done in 2012, 15% of Facebook users, 7% of LinkedIn users, and 5% of Twitter users modified privacy settings specifically with work in mind.[23]

Despite these privacy settings, growing use of social media sites has caused the separation between workers' private and professional lives to become more blurred; social media is not a luxury or lifestyle choice, but a part of the reality of the modern world.[24] In a 2014 survey, 20% of the American adults interviewed (employed full-time or part-time) stated they use social media on the job to get information that helps them solve work problems.[25] Seventeen percent stated they use social media to strengthen personal relationships with coworkers. Other reasons for using social media at work included asking work-related questions inside and outside the organization and taking time to mentally recharge at work.[26]

As noted, 17% of workers say they use social media to build or strengthen personal relationships at work – but the transparency that social media facilitates comes with costs as well as benefits. Some 14% of workers have found information on social media that has *improved* their professional opinion of a colleague; at the same time, a similar share (16%) have found information on social media that has *lowered* their professional opinion of a colleague.[27]

Because of its common use and popularity, there exists a potential for misuse and misinterpretation of information, especially at the hands of employers and, "[B]oth the dignity

---

[19] *Id*.

[20] TWITTER, https://about.twitter.com/company (last visited Oct. 24, 2016).

[21] INSTAGRAM, https://www.instagram.com/press/ (last visited Oct. 24, 2016).

[22] *Ehling*, 961 F. Supp. 2d at 669-70.

[23] Philip Gordon et al., *Social Media Password Protection and Privacy: The Patchwork of State Laws and How It Affects Employers*, LITTLER WORKPLACE POL'Y INST. (May 31, 2013), http://www.littler.com/files/press/pdf/WPI- Social-Media-Password-Protection-Privacy-May-2013.pdf.

[24] Alissa Del Reigo et al.*, Your Password or Your Paycheck?: A Job Applicant's Murky Right to Social Media Privacy*, J. INTERNET L., Sept. 2012, 17, 23; *see also* Lindsay Noyce, *Private Ordering of Employee Privacy: Protecting Employees' Expectations of Privacy with Implied-in-Fact Contract Rights*, AM. U. LAB. & EMP. L. F., Winter 2011, at 27, 29 ("There is an innate tension between an employee intentionally making information public and feeling that her information is private. Yet, with the expansion of social networking, growing use of technology in the workplace, and feeble boundaries between work and home, employees' electronic privacy is a pressing legal issue.").

[25] Kenneth Olmstead et al., *Social Media and the Workplace*, PEW RES. CTR. (June 22, 2016), http://www.pewinternet.org/2016/06/22/social-media-and-the-workplace/.

[26] *Id.*

[27] *Id.*

and the livelihood of individuals are at risk when employers request unfettered access to their employees' private lives, contacts, and habits."[28]

B. An Exploration of The Stored Communications Act

Courts have been faced with the issue of whether an employer's accessing an employee's or applicant's social media account constitutes a violation under the SCA. The SCA was enacted in 1986 as Title II of the Electronic Communications Privacy Act.[29] Section 2701 of the Act states:

> Except as provided in subsection (c) of this section, whoever 1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or 2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.[30]

The Act's legislative history suggests that Congress wanted to protect electronic communications that are configured to be private.[31] The SCA addresses the problem of unauthorized persons deliberately gaining access to electronic communications that are not intended to be available to the public.[32] Additionally, the SCA was enacted because the advent of the Internet presented a host of possible privacy breaches that the Fourth Amendment did not address.[33]

The statutory basis under which many employees' online privacy-based claims arise is the SCA.[34] Some employers say that access to personal social media accounts of employees is needed to protect the employer's proprietary information or trade secrets, to comply with certain federal financial regulations, or to prevent the employer from being exposed to legal liabilities.[35]

---

[28] Reigo et al., *supra* note 24, at 19.

[29] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002).

[30] 18 U.S.C.A. § 2701(a) (Current through Pub. L. 114-38).

[31] *Konop*, 302 F.3d at 875.

[32] *Id.*

[33] Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 971 (C.D. Cal 2010). Where the Fourth Amendment protects one's spatial privacy, i.e., the right of a person to be secure in his house against unreasonable searches and seizures, up until 1986, there was nothing to protect people's online and electronic privacy. This is where the SCA came in. It can be argued that today (2017) protection of one's online privacy may be just as important, if not more important, as one's spatial privacy and therefore, should be treated by state and federal government accordingly. Banking information, financial documents, and even private diaries and messages are just a few examples of what people store online. *Id.*

[34] Reigo et al., *supra* note 24, at 20.

[35] Greenberg, *supra* note 8. Keeping proprietary information secret is a legitimate concern for any business. Employers should always clearly explain and reiterate to each employee (through an employee handbook or clear

However, many policymakers view the practice as a clear violation of privacy.[36] After Collins's story made headlines, U.S. Senators Chuck Schumer and Richard Blumenthal requested that the Department of Justice conduct an investigation into the "new disturbing trend of employers demanding job applicants to turn over their usernames and passwords for social networking [sites]."[37] The two Senators pointedly asked whether employers who request or otherwise obtain access to applicants' social media profiles violated the SCA.[38]

Collins was fortunate enough to avoid a lawsuit altogether. However, his representative from the ACLU of Maryland wrote a letter to the Department of Correctional Services stating that their policy was illegal under the SCA, arguing that "[t]he [SCA] was enacted to ensure the confidentiality of electronic communications, [making] it illegal for an employer or anyone else to access stored electronic communications without valid authorization."[39] Could Collins actually claim an offense under the SCA since he was the user of the service *and* authorized the conduct? Additionally, what if someone who knew and used Collins' Facebook credentials provided it to the interviewer? Questions like these arise when claims are made under the SCA regarding wrongful access to social media sites. The SCA was enacted before the World Wide Web and well before the first social media site came into existence.[40] Networking technology has substantially changed since 1986, but the language of the SCA has remained static.[41]

Thus, the task of adapting the language of the Act to modern technology has fallen largely to the courts.[42] One main issue the courts have encountered is who qualifies as a "user" under the SCA. Furthermore, courts have had to analyze whether the SCA even covers social media sites such as Facebook. Finally, courts have had to address what it means for someone to have "authorization" under the SCA and interpret the exceptions within the SCA.

i. Defining "User" Under the SCA in the Age of Social Media

In *Konop v. Hawaiian Airlines, Inc.*, Plaintiff Robert Konop maintained a secured website where he posted bulletins criticizing his employers.[43] Konop controlled access, but gave certain coworkers access to the site with a username and password that he provided to them. The

---

workplace policies) what is considered private work information. More importantly, employers themselves should practice responsible social media usage so as to set an example for the rest of the company.

[36] Reigo et al., *supra* note 24, at 19.

[37] *Id.*

[38] *Id.*

[39] Letter from Deborah A. Jeon, Legal Dir., ACLU, to Gary D. Maynard, Sec'y, Md. Dep't of Pub. Safety & Corr. Servs. (Jan. 25, 2011) (on file with ACLU), *available at* http://www.aclu-md.org/uploaded_files/0000/004/ letter _collins_final.pdf.

[40] *Ehling*, 961 F. Supp. 2d at 666.

[41] *Id.*

[42] *Id.*

[43] *Konop*, 302 F.3d at 875.

site was considered a Bulletin Board Service (BBS)[44] allowing eligible users to post comments while prohibiting non-users, including anyone in management, from viewing the site.[45] Despite this restriction, the Vice President of Hawaiian Airline Inc. was able to log into the site by asking an authorized user for permission to use his login credentials.[46] Konop proceeded to file suit, alleging claims under the SCA.[47]

Although the SCA makes it an offense to intentionally access an unauthorized facility through which an electronic communication service is provided, it does have exceptions. Section (c) of the SCA provides that "Subsection (a) of this section does not apply with respect to conduct authorized: 1) by the person or entity providing a wire or electronic communication service; 2) by a user of that service with respect to a communication of or intended for that user…"[48] The court, looking at the plain language of § 2701(c)(2), concluded that only a "user" of the service can authorize a third party's access to the communication.[49] The statute defines "user" as one who 1) *uses* the service and 2) is duly authorized to do so. The court stated, "The statute does not define the word "use," so we apply the ordinary definition, which is 'to put into action or service, avail oneself of, employ.'"[50] Based on this definition, the court concluded that although the coworker was an eligible user of the website, he never accessed the site himself, therefore the coworker was not a "user" at the time he authorized the Vice President to view it. The Ninth Circuit Court therefore reversed the lower court's grant of summary judgment based on Konop's SCA claim.[51]

The *Konop* court reasoned that Congress wanted to protect communications that are configured to be private such as email and private electronic bulletin boards.[52] This reasoning laid much of the groundwork for future cases involving an employee's protection under the SCA. Several years later, social media sites—services the *Konop* court did not address—have become increasingly more popular and have begun to change the legal landscape of employee privacy rights.[53]

---

[44] A bulletin board server or bulletin board system is a computer or an application dedicated to the sharing or exchange of messages or other files on a network. *See* WHATIS.COM (last visited Oct. 23, 2016 at 1:00PM), http://whatis.techtarget.com/definition/bulletin-board-system-BBS.

[45] *Konop*, 302 F.3d at 872-73.

[46] *Id.*

[47] *Id.*

[48] 18 U.S.C.A. § 2701(a) (Current through Pub. L. 114-38).

[49] *Konop*, 302 F.3d at 880.

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] Sween & Luke, s*upra* note 1.

ii. Whether Social Media Sites Fall Under the Protection of the SCA

In 2010, in *Crispin v. Christian Audigier, Inc.*, the court addressed the issue of whether private communications through social media sites are covered under the SCA, noting that no other court had addressed this issue before.[54] Plaintiff Buckley Crispin was served subpoenas on his social media sites by Defendant Christian Audigier, Inc. Crispin moved to quash the subpoenas, making a claim under the SCA.[55]

Determining what information is and is not covered by the SCA is often complex, due in part to a split of authority among jurisdictions over the classification of certain types of messages, and whether a single service provider should be classified as either an electronic communication provider (ECS) or a remote computing service (RCS) or both an ECS and an RCS.[56] Section 2702 of the SCA prohibits:

> 1) a person or entity providing an electronic communication service from knowingly divulging to any person the contents of a communication while in electronic storage by that service; and 2) a person or entity providing remote computing service from knowingly divulging to any person or entity the contents of any communication which is carried or maintained on that service.[57]

The court in *Crispin* had to distinguish between ECS providers and RCS providers to determine whether social media sites fall under either.[58] The court found that "[g]iven the court's conclusion that the BBS communication in *Konop* could not have been temporary, intermediate storage, it appears that the passive action of failing to delete a BBS post, which is in all material

---

[54] *Crispin*, 717 F. Supp. 2d at 977.

[55] *Id.* at 969.

[56] NEIL MERKL & ROBERT HAIG, N.Y. PRAC., COM. LITIG. IN NEW YORK STATE COURTS § 113:15, 4th ed. (Sept. 2016).

[57] 18 U.S.C.A. § 2702(a) (Current through Pub. L. 114-38). Internet Service Providers (ISPs) such as Comcast and Time Warner are considered entities within the meaning of the SCA. Mailbox providers such as Yahoo, Gmail and Microsoft Outlook may also be considered entities. *See generally* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal 2010).

[58] *Crispin*, 717 F. Supp. 2d at 972-81. The court in *Crispin* noted that the SCA prohibits an ECS provider from knowingly divulging to any person or entity "the contents of a communication while in electronic storage by that service." *Id.* at 972. Electronic storage is (1) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (2) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. *Id.* at 973. In citing *Konop*, the court recognized that social media sites are virtually the same as bulletin board services (BBSs). *Id.* at 981. Since the sites provide private messaging, they constitute as an ECS provider; Facebook wall postings and MySpace comments are not strictly "public" but are accessible only to those users plaintiff selects. *Id.* at 982. Therefore, the SCA clearly applies to information stored on an electronic bulletin board system. *Id.* at 981. By contrast, RCS is "the provision to the public of computer storage or processing services by means of electronic communications system" and in turn defines an electronic communication system as "any wire, radio, electromagnetic…facilities for the transmission of wire or electronic communication." *Id.* at 973. The SCA prohibits an RCS provider from "knowingly divulging to any person or entity the contents of communication that is carried or maintained on that service." *Id.* Courts have held that Facebook and MySpace are RCS providers with respect to walls postings and comments, since they provide storage service for the user. *Id.* at 990.

ways analogous to a Facebook wall posting or a Myspace comment, also results in that post being stored for backup purposes."[59] The court concluded that Facebook and Myspace can be construed as both ECS and RCS providers and can therefore be covered under the SCA no matter how many people access a page. However, a completely public social media page with no privacy protections configured does not necessarily merit protection under the SCA. To access a communication in such a public system constitutes no violation of the Act, since the general public has been "authorized" to do so.[60]

Whereas *Konop* defined a "user" under the SCA, *Crispin* established that social media sites fall under the protections of the SCA in certain circumstances. However, the exceptions to the Act found in subsection (c)[61] pose problems to employees or applicants who want to claim that an employer wrongfully accessed their private social media account under the SCA.

iii. "Authorization" versus "Coercion" Under the SCA

Court decisions interpreting what it means for authorization to be freely given under the SCA are scarce. Courts that have rendered decisions are inconsistent. Thus, the point turns on the sometimes subtle distinction between whether the employee or prospective employee granted access freely or felt compelled to do so.

In 2013, the Third Circuit Court had to interpret what "authorization" meant under the SCA in *Ehling v. Monmouth-Ocean Hosp. Service Corp.* The court upheld the conclusion in *Crispin,* finding that the plaintiff's non-public Facebook posts are protected under the SCA.[62] However, based on its reading of "authorization," the court did not think the plaintiff, Deborah Ehling, had a valid claim under the SCA. Ehling maintained a private Facebook account but was "connected" with coworkers on the site. One of these coworkers took screenshots of Ehling's Facebook wall posts and sent them to a hospital manager who deemed them "inappropriate."[63] After being temporarily suspended because of the posts, Ehling filed a claim under the SCA.

The court applied the SCA's statutory exceptions, specifically (c)(2), in finding that the plaintiff's posts were authorized by a Facebook user with respect to a communication intended for that user. In reaching its decision, the court noted that first, the coworker voluntarily provided the plaintiff's post to management without any coercion or pressure; second, access to the plaintiff's Facebook wall post was authorized "by a user of that service;" and third, the plaintiff's wall post was intended for that user.[64] Therefore, the authorized user exceptions applied and the defendants were not liable under the SCA.[65]

---

[59] *Id.* The distinction between ECS and RCS is complicated and has even caused confusion for the courts. At this point, it may not even be necessary to distinguish the two since modern electronic communications combine both services. For example, email transmission (ECS) and long-term storage of that same email (RCS) can be provided by a single network operator, such as AT&T or Verizon.

[60] *Id.* at 990.

[61] 18 U.S.C.A. § 2701(a) (Current through Pub. L. 114-38).

[62] *Ehling*, 961 F. Supp. 2d at 668-69.

[63] *Id.* at 663.

[64] *Id.* 669-70.

[65] *Id.* at 771.

Conversely, prior to *Ehling*, the court had found that the plaintiffs did have a valid claim under the SCA in *Pietrylo v. Hillstone Restaurant Group*.[66] Plaintiffs, who were employees of a restaurant, created a MySpace group for coworkers to vent about work. Restaurant management gained access to the page and fired two of the employees, who then sued, alleging a violation of the SCA.[67] The defendant employer argued that it had obtained authorization from one of its employees in the group. However, the district court learned through the testimony of this employee that access to the group was given to management because she felt coerced into doing so.[68] The district court concluded as a matter of law that the allegedly coerced authorization was not enough to relieve the employer's liability under the SCA.[69]

iv. Limitations of the SCA

The complex provisions of the SCA have left the courts to interpret who qualifies as a "user" under the SCA, whether the SCA covers social media sites and what it means for someone to have "authorization" under the SCA. Until Congress brings the law in line with modern technology, protection of the Internet and websites will remain an uncertain area of law.[70] The Act was not built around clear principles that are intended to easily accommodate future changes in technology; instead, Congress drafted a convoluted statute based on the operation of early computer networks, making it difficult for courts to apply the Act to modern computing.[71] The SCA forbids the intentional and unauthorized access of social media accounts and prohibits employers from coercing applicants and employees into giving access to their accounts. However, it excludes from liability those who have been given access by a user of the service who is either the source of the communication or the intended recipient of the communication.[72] Applying this exception to social media, it appears that if someone willingly gives a potential or current employer access to her account, she must forfeit a claim or defense under SCA.[73]

Overall, the ability of the SCA to resolve social media abuse problems is questionable since the Act primarily concerns how and by whom a message, email, or other communication is intercepted or stored and not how a user's online privacy is protected.[74] This concern is dated in

---

[66] Pietrylo v. Hillstone Restaurant Group, WL 6085437 *1, *4 (D.N.J. July 25, 2008).

[67] *Id.* at *3

[68] *Id.* at *4.

[69] *Id*. What constitutes coercion to one court, may be considered authorization by another. This creates another complexity to the SCA.

[70] Michelle Scheinman, *Cyberfrontier: New Guidelines for Employers Regarding Employee Social Media*, 44 MCGEORGE L. REV. 731, 737 (2013).

[71] William J. Robinson, *Free at What Cost? Cloud Computing Privacy under the Stored Communication Act*, 98 GEO. L.J. 1195, 1204-05 (2010).

[72] Reigo et al., *supra* note 24, at 20.

[73] *Id.*

[74] Roberta Studwell, *The Notion and Practice of Reputation and Professional Identity in Social Networking: From K-12 through Law School,* 25 KAN. J.L. & PUB. POL'Y 225, 234 (2016).

part because the SCA was written when older technologies, such as floppy disks and cassette tapes, were used to store information.[75] The intent of the Act appears to be to protect email and similar electronic communications, but it does not expressly state that it applies to an electronic communication that is accessible to portions of the general public, making it inadequate to control access to information—even private information—provided on social media sites.[76]

III. ANALYSIS OF CURRENT SOCIAL MEDIA PRIVACY LAWS

A. An Exploration of State Approaches to Protect Employees' Private Social Media Accounts from Employers

Today, there are no federal laws that specifically prohibit an employer from requiring an employee or applicant to give access to their social media accounts.[77] After Collins's story went public,[78] state lawmakers, fearing delayed action at the federal level, began introducing legislation to prevent employers from requesting prospective or current employees' passwords to personal Internet accounts to get or keep a job. As of 2017, 25 states have enacted laws that apply to employers.[79] "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."[80]

Many of these state password protection laws overlap in a variety of ways. First, most of the laws enacted prohibit employers from seeking applicants' and employees' social media login information.[81] For example, California's Labor Code § 980 states, "An employer shall not require or request an employee or applicant for employment to…1) Disclose username or password for the purpose of accessing personal social media."[82] The other 24 state laws include the same or similar language to that of California.[83]

A second similarity between the state laws enacted is that they include exceptions to their prohibitions in cases of employer investigations. California Labor Code § 980 states, "Nothing in

---

[75] *Id.*

[76] *Id.*

[77] *Social Networking & Computer Privacy*, WORKPLACE FAIRNESS (last visited Oct. 12, 2016), https://www.workplacefairness.org/social-network-computer-privacy-workplace#4.

[78] *See* Meredith Curtis, *Want a Job? Password, Please!* ACLU MD (Feb. 18, 2011, 2:04 PM), https://www.aclu.org/blog/speakeasy/want-job-password-please; *see also* Alexis C. Madrigal, *Should Employers Be Allowed to Ask for Your Facebook Login?* THE ATLANTIC (Feb. 22, 2011, 5:11 PM), http://www.theatlantic.com/technology/archive/2011/02/should-employers-be-allowed-to-ask-for-your-facebook-login/71480/.

[79] Greenberg, *supra* note 8.

[80] *Id.*

[81] Gordon et al., *supra* note 23.

[82] CALIF. LAB. CODE § 980(b) (2012).

[83] *See, e.g.*, Internet Privacy Protection Act, MCL § 37.271-37.278 (2012) (prohibiting employers from requiring certain individuals to disclose information that allows access to certain social media accounts); Personal Online Account Privacy Protection Act, LA. REV. STAT. § 51:1951 (2014) (prohibiting employers from requesting or requiring individuals to disclose information that allows access to or observation of personal online accounts).

this section shall affect an employer's existing rights and obligations to request an employee to divulge personal social media reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations…."[84] Most other states include language that explicitly states that the prohibition does not affect an employer's existing rights and obligations in the context of workplace investigation. If the employer is put on notice of conduct that may violate its harassment policies, for instance, the employer may be obligated to investigate the situation by requesting that an employee divulge social media information relevant to the investigation.[85]

The state password protection laws also diverge in important ways. Many of the states go beyond their original stated purpose to prohibit requiring an employee or applicant to allow access to his social media account.[86] At face value, Arkansas, California and Illinois all share similar laws, but each state includes something extra that goes a step further toward protecting private accounts.

i. Arkansas: The Privacy of Personal Electronic Mediums or Services

Arkansas's social media password protection law was enacted in 2013, and like other state statutes, it provides restrictions to employers seeking applicants' and employees' social media log-in information. However, the legislators, realizing that there are other ways around this restriction, explicitly included that no employer may "add another employee…to the list of contacts associated with the individual's social media account or change the privacy settings associated with his or her social media account."[87] Further, the law not only protects social media accounts, but also protects any electronic personal account of an employee where "users may create, share, or view user-generated content" such as blogs, podcasts, and videos.[88]

Under the Arkansas law, an employee is not obligated to accept a friend request from his employer, a situation that can be uncomfortable for many. Additionally, an employee does not have to make his private page public, a move that would cause an employee to forfeit any rights under the SCA. Finally, with so many different ways of communicating electronically, Arkansas makes clear (and broadly defines) what type of personal electronic account is protected under the law, leaving little room for confusion.

ii. California: Employer Use of Social Media and Privacy Rights for California Minors in the Digital World

California was the third state to enact a law that prohibits employers from requesting social media account information from applicants or employees. California's law is unique in that it prohibits employers from requiring an employee to "access social media in the presence of

[84] CALIF. LAB. CODE § 980(d) (2012).

[85] Sween & Luke, s*upra* note 1.

[86] Gordon et al., *supra* note 23.

[87] ARK. CODE ANN. § 11-2-124(b)(1) (2014).

[88] ARK. CODE ANN. § 11-2-124(a)(3)(A) (2014).

an employer."[89] This prohibited practice is known as "shoulder surfing", and means that an employee or applicant goes online while the employer examines a website over the applicant's shoulder.[90] If an employer asks an employee to pull up his private Facebook page while the employer is sitting next to him, the employee, if he complies, will have a difficult time making a claim under the SCA. In such a case, the employer technically becomes an authorized "user" of the site since he *uses* the service and is duly authorized to do so.[91]

California also became the leader in strengthening online privacy protection for minors who will one day be applying for jobs.[92] In 2013, the Governor signed into law an amendment to California's Online Privacy Protection Act,[93] the first measure in the United States giving minors under the age of 18 the legal right to "erase" information they post to websites.[94] The law went into effect in January 2015 and requires "website and mobile app operators to provide anyone under 18 with (i) the ability to remove or request removal of content that the minor posted on the website or mobile app; (ii) notice and clear instruction on how to do so; and (iii) notice that such removal may not remove all traces of such posting."[95] This law was implemented to help minors remove old (and oftentimes inappropriate) posts and comments made on message boards and news websites so as to prevent future employers from searching these sites for teenage indiscretions.[96]

iii. Illinois: Right to Privacy in the Workplace Act

While most state social media privacy laws prohibit an employer from requesting access to an employee's or applicant's private social media page, many laws are silent on whether an employer can use private social media information voluntarily given by an existing employee who is "friends" with the applicant or employee.[97] The Illinois Right to Privacy in the Workplace

---

[89] CALIF. LAB. CODE § 980(b)(2) (2012).

[90] Katrina Grider, *Employment Law Update*, 70 THE ADVOC. (TEXAS) 138, 218 (2015).

[91] *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 880 (9th Cir. 2002) (defining "user").

[92] Judith Delaney, *What is California's "Erase" Law for Minors on Social Media,* MELISSA AGNES CRISIS MGMT. STRATEGIST (Oct. 8, 2013), http://melissaagnes.com/what-is-californias-erase-law-for-minors-on-social-media/.

[93] Privacy Rights for California Minors in the Digital World, CA SB 568 § 22580-22582 (2013).

[94] Delaney, *supra* note 92.

[95] Privacy Rights for California Minors in the Digital World, CA SB 568 § 22580-22582 (2013). *See also* Eric Ball, *Eraser Laws: Forgetting a Minors Past to Save His Future*, FENWICK & WEST, LLP (May 5, 2015), https://www.fenwick.com/FenwickDocuments/EraserLaw.pdf.

[96] *Id.* The intent of the Eraser Law is admirable, but seemingly impossible to accomplish. When someone under the age of 18 posts something on social media, it is possible for the original post to be removed. However, this minor's "friend" or "connection" can share this post, and in turn, another person (possibly someone who is unknown to the minor who originally wrote the post) can go in and share the "friend" or "connection's" post. The process of sharing and re-sharing on the Internet makes it very difficult to delete all traces of the original post. Both minors and adults alike may run into this issue when using social media platforms.

[97] Sween & Luke, s*upra* note 1.

Act attempts to address this issue by making it unlawful for an employer to "demand access in any manner to an employee's or prospective employee's account or profile on a social networking website."[98] This language prohibits employer requests for an employee to print screen shots of a coworker's social media post,[99] the situation that occurred and was deemed legal under the SCA in *Ehling.*[100] As *Ehling* demonstrated, instances in which an employee shared a coworkers' social media content has happened in the past.[101]

This situation could very well happen to job applicants, too. For example, "if an existing employee gets word that the employer is looking to hire their 'frenemy' from college, and decides to print out Facebook of said frenemy doing a keg standing…can the employer legitimately use this information to deny employment?"[102] Although Illinois law does not completely prevent this action from occurring, it limits indirect requests to access private social media pages.

B. The Canadian Approach to Protect Employees' Private Social Media Accounts from Employers

i. A Brief Overview of Canada's Views on Privacy in the Workplace

The United States is not alone in its efforts to find a balance between employers' interests and employees' and applicants' privacy in emerging technologies.[103] However, reports of employers' requesting access to their employees' online social media accounts have largely been concentrated in the United States.[104] One explanation for this disparity is that U.S. laws focus on privacy that is based on control and physical space, as opposed to dignity.[105] Similar to the United States, there is no explicit constitutional protection of privacy in Canada.[106] However, some argue that Canadian privacy protection does more to protect the dignity, integrity, and autonomy of its citizens in the workplace.[107]

---

[98] 820 ILL. COMP. STAT. 55(b)(1) (2013).

[99] *Id.*; *see also* Gordon et al., *supra* note 23.

[100] *Ehling*, 961 F.Supp.2d at 662-63.

[101] *Id.*

[102] Sween & Luke, *supra* note 1.

[103] Reigo et al., *supra* note 24, at 22.

[104] *Id.*

[105] *Id.* In the United States, there are some boundaries even for private employees, but they usually include physical possessions such as purses or briefcases. An employee may bring these personal items into their place of work, usually without worrying that they will be searched. However, anything the employee says or does while using a company computer, the company server, or the company Wi-Fi may be considered fair game for the employer to search since it is technically company property. *See generally* City of Ontario v. Quon, 560 U.S. 746 (2010); U.S. v. Ziegler, 474 F.3d 1184 (9th Cir. 2007); Mintz v. Bartelstein & Assoc., Inc., 885 F. Supp. 2d 987 (C.D. Cal. 2012).

[106] Bryce Clayton Newell, *Rethinking Reasonable Expectation of Privacy in Online Social Networks*, RICH. J.L. & TECH, Spring 2011, at 1, 40.

[107] *Id.*

In the landmark case *R. v. Cole*, the Supreme Court of Canada confirmed that a person has a reasonable expectation of privacy in his personal computer, even if it is owned by his employer.[108] In *Cole,* a high-school teacher was charged with unauthorized use of a computer.[109] The teacher used his work computer to save inappropriate photographs of female students.[110] During a check-up of the computer, a school technician notified the principal of the images. The principal seized the laptop and handed it over to police.[111] During the subsequent trial of the school teacher, The Supreme Court of Canada stated:

> Computers that are reasonably used for personal purposes—whether found in the workplace or the home—contain information that is meaningful, intimate, and touching on the user's biographical core. Canadians may therefore reasonably expect privacy in the information contained on these computers, at least where personal use is permitted or reasonably expected…. Workplace policies are not determinative of a person's reasonable expectation of privacy. [O]ne must consider the totality of the circumstances in order to determine whether privacy is a reasonable expectation in the particular situation. While workplace policies and practices may diminish an individual's expectation of privacy...these sorts of operational realities do not in themselves remove the expectation entirely. A reasonable though diminished expectation of privacy is nonetheless a reasonable expectation of privacy.[112]

The *Cole* court's focus on the individual's dignity and integrity is reflective of privacy law in Canada that is more protective of the individual than in the United States.[113]

ii. Canada's Personal Information Protection and Electronic Document Act

The Canadian federal and Provincial Privacy Commissioners, the country's data protection regulators, have issued guidelines for social media background checks wherein they caution employers from relying on the consent of job applicants and clarify that personal information collected from social media sites are subject to Canada's personal information protection laws.[114]

The established personal information protection law in Canada is the Federal Personal Information Protection and Electronic Document Act (PIPEDA). The PIPEDA and related provincial legislation applies to collection of private employee information in various industries

---

[108] R. v. Cole, [2012] 53 S.C.R. 34 (Can.), http://www.canlii.org/en/ca/scc/doc/2012/2012scc53/2012scc53.html.

[109] *Id.*

[110] *Id.*

[111] *Id.*

[112] *Id.* at 36.

[113] Reigo et al., *supra* note 24, at 22.

[114] *Id.*

and businesses.[115] The legislation, enacted in 2000, seeks to strike a balance between employer's need to know and employee's right to privacy, generally requiring that the employer obtain the consent of the employee to collect, use and disclose personal information only for purposes specifically outlined.[116] Along with consent, there must be a reasonable purpose for the collection of employees' or applicants' social media information.[117] The law states that its purpose is

> [t]o establish, in an era [when] technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use[,] and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use[,] or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.[118]

PIPEDA sets the minimum standards for privacy in the workplace. The provinces and territories within the country that have enacted substantially similar privacy laws are not bound by PIPEDA. For example, prior to the enactment of PIPEDA, Quebec had already introduced its Act Respecting the Protection of Personal Information in the Private Sector—the first legislation of its kind in North America—which was a direct response to the EU's directive on data protection. Also enacted were The British Columbia Personal Information Protection Act and the more recent Manitoba private sector privacy legislation.[119] The PIPEDA was intended to apply to every private sector employer that collects, uses, and discloses personal information in the course of a commercial activity.[120] It is generally accepted that a commercial activity must have a transaction-based component, meaning it includes not only activities conducted in the normal character of business, but also any transaction or conduct that has a commercial character.[121]

The PIPEDA essentially prohibits personal information from being used without an individual's consent, including social media information and passwords.[122] Under the PIPEDA, consent means that the employee has knowledge and gives consent, which assumes that the employee is informed not only of the nature of the information being used, collected or

---

[115] Natalie MacDonald & Stuart Rudner, *The Law, Surveillance and Employee Privacy*, THE GLOBE AND MAIL (last updated June 10, 2014 at 9:26AM), http://www.theglobeandmail.com/report-on-business/careers/career-advice/ experts/what-privacy-rights-to-do-you-have-at-work/article19079506/.

[116] *Id.*

[117] *Id.*

[118] Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5, s. 3, (Can.). *available at* http://laws-lois.justice.gc.ca.

[119] Patrick L. Benaroche, *Canada, in* SOCIAL MEDIA AND EMPLOYMENT LAW: AN INTERNATIONAL SURVEY, 55, 56 (Anders E. Reitz et al. eds., 2015).

[120] *Id.* at 56.

[121] *Id* at 57. PIPEDA has limited or no application to non-commercial organization such as non-profits and charities.

[122] *Id.*

disclosed, but also of the objectives underlying the use, collection, or disclosure.[123] Furthermore, the PIPEDA requires that consent must be obtained every time information collected for one purpose is used for another purpose.[124] Additionally, asking for consent may come at a price for the employer, since a candidate or employee cannot face reprisals for refusing to consent to social media screening.[125] Therefore, employers have to justify their decisions not to hire (or to fire) someone who has withheld consent to social media screening, lest they be accused of retaliation. [126]

Under the PIPEDA, so as to not breach any privacy laws, employers must obtain express consent of candidates in order to collect any information on them through social media. The requirement applies to social media sites even when the employee's or applicant's social media page is public.[127] As stressed in subsection 5(3) of the PIPEDA, employers must also have a legitimate and reasonable purpose for collecting information about an applicant or employee through their social media networks.[128] Reasonableness refers to the non-procedural requirements relating to the information collection, such as (i) the accuracy of the information collected, (ii) the existence of a legitimate purpose to collect the information and the relevance of the information collected to this purpose and, (iii) use of the least intrusive means to collect information in light of the stated purpose.[129]

---

[123] *Id.* at 56. While PIPEDA was enacted in 2000, the SCA was enacted while the Internet was still in its infancy. This has made it difficult for U.S. courts to affirmatively say that the SCA applies to social media media sites. *See also* Studwell, *supra* note 74, at 234-35.

[124] Benaroche, *supra* note 119, at 61.

[125] *Id.* at 62.

[126] *Id.*

[127] *Id.* at 60.

[128] Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c.5, s.3, (Can.), *available at* http://laws-lois.justice.gc.ca; *see also Leading by Example: Key Developments in the First Seven Years of the Personal Information and Electronic Act*, OFF. PRIVACY COMM'R CAN. (May 2008), *available at* https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/lbe_080523/. This Act, too, differs substantially from the SCA. If a job applicant willingly gives a potential or current employer access to her account, she must forfeit a claim or defense under the SCA. *See also* Studwell, *supra* note 74, at 234-35. PIPEDA goes further than the SCA to protect employees and applicants. An employer may still be held liable under PIPEDA if there is no reasonable justification for obtaining the consent in the first place.

[129] Benaroche, *supra* note 119, at 63. Viewing an employee's profile page may be considered a form of collection for the purpose of Canadian privacy legislation. An employer who reads and gathers inaccurate information on an employee's or applicant's Facebook profile page could be violating his obligation under Canadian privacy laws to only collect accurate information about others. Online information may be prone to error, and social media is no exception. The ease with which individuals can link images and information that has been collected from social media to a name increases the chances that the employer performing the check will collect inaccurate personal information. Even when consent is obtained and accurate information is collected for a legitimate purpose, the existence of less intrusive means to collect the information may still pose a hurdle to social media screening. Employers may have difficulty justifying the use of social media screening to obtain information that could be obtained through traditional vetting means. *Id.* at 64.

iii. Comparing the PIPEDA to Statutes in the United States

Overall, the PIPEDA is arguably stronger than the separate statutes enacted by Arkansas, Illinois, and California because it incorporates the protections found in each one. For example, similar to Illinois's Right to Privacy in the Workplace Act,[130] an employer in Canada is not permitted to use misrepresentation in order to screen an employee's social media profile.[131] An employer cannot create a fictitious Facebook profile in order to become Facebook friends with an employee.[132] Moreover, an employer that monitors an employee must be acting on the basis of legitimate concern or for a legitimate purpose, and cannot invoke a concern or purpose after the fact.[133]

In general, the password protection laws that states have enacted address privacy on social media sites as "fundamentally about protection from intrusion and information gathering by others."[134] "Privacy is [thus] protected when information is hidden" from public view, and invaded "when such information is revealed."[135] Canada takes this idea one step further since it generally does not distinguish, as a matter of principle, between public or private information. Without the consent of the job candidate or employee, social media posts, no matter how weak the privacy settings are, do not give the employer the right to access and use the posted information.[136]

The state laws declare that as long as access to a social media profile is restricted in some way, the information it contains is private.[137] Employers are prohibited from demanding access to private profiles because to do so constitutes an "unreasonable and unacceptable invasion of privacy."[138] As one state legislator asked, "[W]hy should [these entities] be able to ask [users] for their Facebook passwords and gain unwarranted access to a trove of private information about what [they] like, what messages [they] send to people, or who [they] are friends with?"[139] Canada also considers this question as it continues to develop and assess the PIPEDA, recognizing that there must be a balance between the employer's need to know and the employee's right to privacy.[140]

---

[130] 820 ILL. COMP. STAT. 55(b)(1) (2013).

[131] Benaroche, *supra* note 119, at 66.

[132] *Id.*

[133] *Id.*

[134] Sarah N. O'Donohue, "*Like" It or Not, Password Protection Law Could Protect Much More than Passwords*, 20 J.L. BUS. & ETH. 77, 110 (2014).

[135] *Id.*

[136] Benaroche, *supra* note 119, at 61.

[137] *Id.*

[138] *Id.*

[139] *Id.*

[140] MacDonald & Rudner, *supra* note 115.

Another key provision of the PIPEDA, comparable to that of Arkansas, California, and Illinois, is that collection of an employee's personal information does not require consent where it is justified by the employer's power to conduct disciplinary investigations under its management rights.[141] This exception provided in the PIPEDA plays a role when there is a threat that private company information is being stolen or compromised.[142] Additionally, employers have a right to take action against employees without consent in instances of cyberbullying between colleagues.[143]

The PIPEDA was enacted in part as a response to technological threat to privacy, but does not contain provisions that address particular types of technologies.[144] However, the Office of the Privacy Commissioner of Canada, which investigates privacy complaints and helps businesses improve their personal information handling practices, views the PIPEDA as a general regulatory instrument[145] that applies across all electronic and online sectors and activities, including social media.[146] At the early ages of social media, Canada realized that its citizens should not be forced to choose between their privacy rights and their right to participate in the interactive world.[147] This is an idea that some states in the United States have embraced, while others, such as Ohio, are still debating.

IV. ARGUMENT FOR SOCIAL MEDIA PRIVACY LAW IN OHIO

In 2013, Ohio introduced House Bill 424 to address the issue of employers requesting access to an employee's or applicant's private social media pages. However, as of 2017, the bill has yet to pass. Ohio needs to be proactive and pass the bill before a lawsuit emerges.[148]

---

[141] Benaroche, *supra* note 119, at 67.

[142] *Id.*

[143] *Id.* at 69.

[144] *Leading by Example*, *supra* note 128.

[145] Benaroche, *supra* note 119, at 56-57.

[146] *Leading by Example*, *supra* note 128.

[147] Pierre-Luc Dusseault, *Privacy and Social Media in the Age of Big Data: Report of the Standing Committee on Access to Information, Privacy and Ethics*, 41st Parliament, First Sess. (April 2013), *available at* http://www.parl.gc.ca/content/hoc/Committee/411/ETHI/Reports/RP6094136/ethirp05/ethirp05-e.pdf.

[148] Michigan is an example of state that waited for a lawsuit to emerge before passing its Internet Privacy Protection Act. In 2011, Kimberly Hester, a teacher aide at an Elementary School in Michigan, was asked by the Superintendent for access to her Facebook account and Hester refused. In response, the district's special education director wrote to her that "in the absence of you[r] voluntarily granting…administration access to you[r] Facebook page, we will assume the worst and act accordingly." Hester went on paid administrative leave and then was suspended. In response to this situation, the Michigan House of Representatives contacted Hester to include her story in a House Bill that would make it illegal for employers to request employees' login information for social media sites. *Kimberly Hester, Michigan Teacher's Aide, Files Lawsuit for Losing Job after Denying District Access to Facebook*, HUFFINGTON POST (last updated June 1, 2012), http://www.huffingtonpost.com/2012/04/01/kimberly-hester-michigan-_n_1394880.html; *see also* Rubino v. City of New York, 106 A.D.3d 439 (May 2013) (stating that penalty of termination for teacher's act of posting comments on social media website was shocking to one's sense of fairness and there was no indication in the record, nor in any finding, that her postings affected her ability to teach).

Although Ohio has not passed a social media privacy law, its proposed bill contains many of the elements of other state statutes as well as the PIPEDA, including the same general prohibitions and exceptions. Ohio's House Bill 424 prohibits "employers…from requiring an employee [or] applicant to provide access to [his] personal Internet-based account."[149] Furthermore, it prohibits "an employer from taking adverse action against those individuals for failing or refusing to grant access to, allow observation of, or provide access information to the individual's personal Internet-based account."[150] Additionally, comparable to Canada, California, Arkansas, and Illinois, the Ohio bill includes exceptions so that an employer may request that an employee disclose access information when a workplace investigation is being conducted.[151] For example, the bill does not prohibit an employer from

> conducting any investigation or requiring an employee to cooperate in an investigation in either of the following circumstances: The employer has specific information about activity on the employee's personal Internet-based account and must conduct the investigation to ensure compliance with the applicable laws, regulations, or other prohibitions against work-related employee misconduct. The employer has specific information about an unauthorized transfer of the employer's proprietary, confidential, or financial information to an employee's personal Internet-based account.[152]

Finally, the bill also prohibits an employer from asking an employee or an applicant to allow observation of an employee's or applicant's personal Internet-based account.[153] This wording, although somewhat ambiguous, hints at prohibiting "shoulder surfing," which is a strength of the proposed House Bill.

Based on the other state statutes analyzed, however, Ohio House Bill 424 could be improved to provide stronger protections for applicants and employees in at least four ways. First, to limit confusion over what the bill covers, it should explicitly state what type of personal electronic accounts are protected, similar to Arkansas's law. Second, it should prohibit employers from using other means to access employees' or applicants' secured accounts; it should restrict employers from forcing an employee to "connect" on social media, or forcing an employee to change the privacy settings associated with his or her social media account. Finally, like the Illinois law and the PIPEDA, Ohio should make it unlawful for an employer to achieve access in alternative manners to an employee's or prospective employee's account. This restriction should include prohibiting an employer's request for an employee to print screen shots of a coworker's social media page as well as prohibiting requests to "shoulder surf" others with the purpose of viewing an applicant's or employee's private social media pages. Additionally, it should include prohibiting an employer from using misrepresentation in order to screen the social media profile of an employee.

---

[149] H.B. 424, 130th Gen. Assemb., Reg. Sess. (Ohio 2014).

[150] *Id.*

[151] *Id.*

[152] *Id.*

[153] *Id.*

Finally, similar to Canada's law, the Ohio bill should require more than simply obtaining an individual's express consent. Ohio employers should have a legitimate and reasonable purpose for collecting information about an applicant or employee through their social media networks. Employers should be required to state the legitimate purpose to collect the information and the relevance of the information collected for this purpose. Additionally, if there are less intrusive means to collect information in light of the stated purpose, the employer should resort to those techniques rather than social media screening.[154]

Although California's "Eraser" law seems like the proactive approach that Ohio might take to protect future applicants and employees, it raises a number of uncertainties that need to be considered. For example, it fails to define when a user can request removal. For example, does the employee or applicant have to be a minor, or can he make this request when he is 22 and on the job hunt?[155] Furthermore, major social media providers, such as Twitter and Facebook, already allow users to remove their content[156] and did not need a new law to require this existing business practice.[157] At this point, a similar law seems unnecessary for Ohio to enact, although it may be an added layer of protection and worth considering in the future as social media continues to change and grow.

At first, an Ohio law may seem like an unnecessary restriction on an employer's ability to manage its workforce. In reality, however, the law protects the employers from themselves.[158] First, the exceptions included in H.B. 424 would still provide the employer with the ability to access an employee's social media account when it is deemed absolutely necessary, such as during a workplace investigation. Additionally, as *Collins* proved, it is usually not a good idea to access an employee's personal social media account, even if the employee offered his password voluntarily.[159] For example, an employee's Facebook wall may show that she is pregnant. If an employer takes an adverse action against her, even for something not involving her pregnancy, the employee may well file a discrimination suit claiming that the action was taken because of the pregnancy.[160] Thus, social media screening can reveal information that might constitute illicit discriminatory grounds unrelated to the aptitudes required for employment, and use of such information in the hiring process to disqualify a candidate could lead to employment discrimination claims.[161]

The very act of online screening may be discriminatory: An employer might conduct pre-hiring social media screening solely for a sub-set of candidates on the basis of discriminatory

---

[154] Benaroche, *supra* note 119, at 63. Examples of less intrusive means include questionnaires, surveys, or a simple discussion with the applicant or employee.

[155] Ball, *supra* note 95.

[156] *Id.*

[157] *Id.*

[158] Sara Sakagami, *New Law Protects Employees' Social Media Privacy,* VA. EMP. L. LETTER, June 2015, at 1.

[159] *Id.*

[160] *Id.*

[161] *Id.*

grounds, such as racial origin.[162] Furthermore, if an employer views applicants' social media postings to determine whom to interview, and in the process discovers a Facebook posting indicating protected status, such as an applicant who is a devout Catholic, a native of China, or being treated for severe depression, that employer could then be left to argue in a discrimination lawsuit that although it had knowledge of the applicant's characteristics, it did not take such information into account when declining to invite the applicant to interview.[163]

Because it can be deemed unlawful for an employer to view an applicant's social media page and then refuse to hire the individual on the basis of the applicant's race, sex, color, national origin, religion, disability, age, genetic information, or in some states, sexual orientation, why would an employer want to risk having knowledge of an applicant's protected status in the first place?[164] It can be argued that "seeking out information about the personal lives of employees can only get an employer in hot water and make them the target of a lawsuit."[165] Therefore, an Ohio law will not only protect applicants and employees, but will also protect employers.[166]

V. CONCLUSION

In her letter to the Division of Corrections on behalf of Robert Collins, Deborah Jeon stated, "While we appreciate the DOC's need to ensure that applicants and employees are not engaged in illicit activity, here there is no basis whatsoever for the Department to suspect Officer Collins of gang involvement or illegal activity of any kind. As such, an intrusion upon his private, off-duty communications in this manner is unjustified and unacceptable."[167] Jeon claimed that the DOC policy was illegal under the SCA,[168] but based on case law, the Act's history, and the limits of the SCA, it is unclear whether Collins would have had a valid argument under the SCA since he authorized the interviewer to view his private page.

Authorized access does not necessarily violate the SCA, so employers may take the route of getting the employees' consent in order to view their private social media pages.[169] However, state legislatures are viewing this practice as an invasion of privacy "akin to requiring someone's house keys."[170]

With the increased use of privacy settings on social media websites, some employers are asking for login credentials, requesting "friendship" status, or "shoulder surfing" to gain access

---

[162] Eric Bentley, *The Pitfalls of Using Social Media for Job Applications*, 29 A.B.A. J. LAB. & EMP. L., Fall 2013, at 1, 2.

[163] *Id.*

[164] *Id.*

[165] Sakagami, *supra* note 158, at 1.

[166] *Id.*

[167] Letter from Jeon, *supra* note 39.

[168] *Id.*

[169] Reigo et al., *supra* note 24, at 20.

[170] Valdes & McFarland, *supra* note 4.

to applicants' or employees' social media pages.[171] Other employers are creating fake profile pages so as to "connect" with employees and applicants.[172] The outcry over stories like Collins's has led state legislators to quickly take action to fill any gaps in federal law (i.e., the SCA), which allows employers to request access to employees' accounts on social media websites.[173]

Unless and until an employer's request for social media credentials becomes illegal under U.S. federal law, much like it is in Canada, employees and applicants in Ohio are without recourse. However, the Ohio legislature can follow 25 other states by passing the proposed H.B. 424.[174] Additionally, the legislature can mirror what other states have done, specifically Arkansas, California, and Illinois, in providing "a preemptive measure that will provide [employers] with critical guidelines to the accessibility of private information behind the 'social media wall.'"[175]

[171] *See generally* Greenberg, *supra* note 8.

[172] Benaroche, *supra* note 119, at 66. In Canada, an employer's Facebook evidence is inadmissible in court when it is gathered using misrepresentation. In one such case, the employer created a fake Facebook profile specifically tailored to the likes and interests of the employee and was able to become Facebook friends with this employee. The court determined that this evidence could not be used against the employee.

[173] *See generally* Gordon, *supra* note 23.

[174] H.B. 424, 130th Gen. Assemb., Reg. Sess. (Ohio 2014).

[175] Scheinman, *supra* note 70, at 733.