Too Much Information!: The Need for Stronger Privacy Protection for the Online Activities of Employees and Applicants

Ralph Carter

Follow this and additional works at: https://scholarship.law.stjohns.edu/jcred

Part of the Internet Law Commons, and the Labor and Employment Law Commons
TOO MUCH INFORMATION!:
THE NEED FOR STRONGER PRIVACY
PROTECTION FOR THE
ONLINE ACTIVITIES OF EMPLOYEES AND
APPLICANTS

RALPH CARTER*

INTRODUCTION

Consider the following scenario: You have recently applied for a highly
 coveted position with a private employer. To make ends meet during the
current economic downturn, you have worked in a series of part-time jobs
that are decidedly outside of your desired career path. Luckily, you have
progressed quickly through several rounds of the interview process and a
battery of tests. The company’s human resources manager has informed
you that the company would like to extend you an offer of employment,
subject to the results of the company’s standard background investigation.

Imagine that as part of that company’s background investigation, the
human resources manager has requested that you provide the passwords to
your personal Gmail account and your social network accounts on
Facebook, Myspace, Google+, and LinkedIn.¹ You use those accounts
daily in your intimate personal interactions with family members, friends
and acquaintances. Your likely reaction would be one of shock at the

*J.D. 2014, St. John’s University School of Law (Evening Division). Executive Notes and Comments
Editor for the Journal of Civil Rights and Economic Development. Inaugural Winner of the Edwards,
Wildman, Palmer Prize for the Best Research Paper by a St. John’s Law Student in the 2013-2014
Academic Year on a Fair Employment Law Subject. Carter was also a Ronald H. Brown Scholar and
received the Robert J. Nobile Scholar for Excellence in Labor and Employment Law, the Junior Fellow
of the Center for Labor and Employment Law and the Dorothy Day Memorial Scholar for Excellence in
Labor and Employment Relations.

¹ Social networking sites may be defined as “web-based services that allow individuals to (1)
construct a public or semi-public profile within a bounded system, (2) articulate a list of other users
with whom they share a connection, and (3) view and traverse their list of connections and those made
by others within the system.” danah m. boyd & Nicole B. Ellison, Social Network Sites: Definition,
individuals . . . to express themselves online by posting opinions, information, images, photos, music,
and links to other users.” HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND
THE INTEGRITY OF SOCIAL LIFE 59 (STANFORD UNIV. PRESS 2010).
suggestion that such an utter intrusion into your personal life was a pre-
condition of employment with the company. You know, however, that if 
you follow your initial inclination and respectfully decline the employer’s 
request for your personal account passwords, it is all but certain that your 
application will be rejected. Given that there are no skeletons in your 
personal online closet, you reason that there is really no harm in providing 
your prospective employer with access to your protected personal accounts. 
Therefore, discretion being the better part of valor, you acquiesce and 
provide the human resource manager with your account passwords. After 
all, you have been on the job market for the last year and your 
unemployment compensation benefits and personal savings are rapidly 
dissipating. You are also keenly aware that the longer you remain on the 
job market, the less desirable you are as a candidate with other prospective 
employers.2

A week later when you inquire with the human resources manager, he 
tells you that you are no longer under consideration for the position, but 
declines to provide you with any details as to why. In racking your brain to 
figure out what could have caused such a reversal of fortune, you recall that 
some of your Facebook friends have posted on the private “wall” on your 
Facebook page. In the posts, your friends expressed certain controversial 
political views, and you lodged your support by “liking” the posts. Only 
then does it occur to you that the company may have decided that your 
political leanings are not in keeping with its corporate mission.

There have been a number of reported cases similar to the hypothetical 
situation above in which employers have demanded access to password-
protected content on the personal social media network accounts of 
employees and job applicants. In March 2012, the Associated Press 
reported that a New York statistician applying for a consulting position 
with a lobbying firm decided to withdraw his job application when the 
prospective employer requested during the job interview that the applicant 
provide his Facebook login.3 When asked in an ABC News interview why 
he declined to provide his Facebook password, the statistician responded 
that: “The most personal details of [his] life are contained on that social 
network.”4 Numerous similar incidents have received media attention over

---

2 Tami Luhby, Only 1 in 10 Long-Term Unemployed Find Work, CNNMONEY (June 14, 2012, 9:10 

3 Manuel Valdes, Job Seekers Getting Asked for Facebook Passwords, YAHOO! FINANCE (Mar. 20, 

4 Joanna Stern, Demanding Facebook Passwords May Break Law, Say Senators, ABC NEWS (Mar. 
26, 2012), http://abcnews.go.com/Technology/facebook-passwords-employers-schools-demand-access-
facebook-senators/story?id=16005565#.T3yzM_Dy-68.
the past several years.5

By seeking to rummage through the password-protected social network and other personal electronic accounts of applicants and employees, employers risk taking a troubling step past the more commonly used method of employing Internet searches to review publicly available online information pertaining to employees and applicants. For instance, according to a 2011 survey of more than 300 hiring professionals conducted by social media monitoring service, Reppler, “more than 90% of recruiters and hiring managers have visited a potential candidate’s profile on a social network as part of the screening process” and “69% of recruiters have rejected a candidate based on content found on his or her social networking profiles...”6 According to another survey, “two thirds of HR managers will browse unprotected social media profiles of candidates.”7 The results of a 2010 survey commissioned by Microsoft show that “[o]f the U.S. recruiters and HR professionals surveyed, 75% report that their companies have formal policies in place that require hiring personnel to research applicants online.”8 Notably, while the survey showed that 70% of

---

5 For example, in August 2009, a Georgia high school teacher was presented by her school superintendent with the Hobson’s choice of either resigning or facing suspension after an anonymous email complaint about the teacher’s purportedly inappropriate private Facebook postings. See LORI ANDREWS, I KNOW WHO YOU ARE AND I SAW WHAT YOU DID: SOCIAL NETWORKS AND THE DEATH OF PRIVACY 122-23 (FREE PRESS 2011). The offending posts amounted to a privately posted vacation photograph of the teacher drinking a glass of Guinness while visiting a brewery in Ireland, and what was arguably a mildly off-color private status update. Id. In another example, in March 2010, a former corrections officer with the Maryland’s Department of Public Safety and Correctional Services was required to provide his Facebook login and password as part of a recertification process after returning from a four-month leave of absence following his mother’s death. The department instituted the practice in order to screen its officers for gang affiliations. After the officer reported the incident to the American Civil Liberties Union, the department amended its policy to make disclosures voluntary. Id. at 123. In April 2011, a Michigan teacher’s aide privately posted a photo on her Facebook page depicting a co-worker’s pants around her ankles, and a pair of shoes. Emil Protalinski, Teacher’s Aide Fired for Refusing to Hand Over Facebook Password, ZDNET (Apr. 1, 2012, 6:15 PM), http://www.zdnet.com/blog/facebook/teachers-aide-fired-for-refusing-to-hand-over-facebook-password/11246. A parent who was a Facebook friend of the educator reported her to the school district superintendent, who repeatedly demanded access to the educator’s Facebook page. When she refused to provide access, the teacher’s aide was suspended. Id.


7 Francis Bea, What You Should Know About How Job Recruiters Use Social Media to Hunt You Down, DIGITAL TRENDS (Dec. 27, 2012), http://www.digitaltrends.com/lifestyle/how-hr-uses-social-media/#ixzz22LtBWq3. But see SOC’Y FOR HUMAN RESOURCE MGMT., SHRM SURVEY FINDINGS: THE USE OF SOCIAL NETWORKING WEBSITES & ONLINE SEARCH ENGINES IN SCREENING JOB CANDIDATES (Aug. 25, 2011), available at http://www.shrm.org/research/surveyfindings/articles/pages/thesuseofsocialnetworkingwebsitesandonlin esearchenginesinscreeningjobcandidates.aspx (“Only 18% of organizations indicated using social networking websites to screen job candidates during the hiring process; conversely, more than two-thirds of organizations (71%) have never used these websites to screen job candidates or used them in the past but no longer do.”).

8 CROSS-TAB, ONLINE REPUTATION IN A CONNECTED WORLD 8 (2010), available at
U.S. recruiters had rejected candidates on the basis of online information, only 7% of U.S. consumers believed that their online information was used in making hiring determinations. However, a more recent survey of social media users between the ages of 18 and 34 revealed that 29% of respondents feared adverse employment repercussions could result from their public postings on social media sites such as Facebook, Twitter, Instagram, Pinterest, and Tumblr; 21% of those surveyed reported that they had removed potentially damning content from their social media accounts in order to avoid such a consequence.

Because the information accessed by employers under such circumstances is, by its nature, publicly available, there is not the same level of concern that individuals' privacy has been invaded by these inquiries. By contrast, employers that seek unfettered access into the private online communications of current and prospective employees do a grave disservice to these individuals' privacy rights. In each of these reported incidents, the employees and applicants availed themselves of the privacy settings on their social networking accounts. In doing so, the individuals indicated that the matters discussed within that sphere were considered private. This is so without regard to the number of individuals with whom that employee or applicant saw fit to share her content online. "In sum, the fact that 'an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information.'"

When employers delve improperly into individuals' private online accounts, there is also the looming specter that the information gleaned as a
result may be used to take illegal employment actions on the basis of current or prospective employees’ protected class status, such as race, ethnicity, marital status, age, sexual orientation, pregnancy, religion, or disability.\textsuperscript{13} There is an infinite array of personal interests, proclivities, and characteristics that may be ascertained by an employer by viewing a job candidate or employee’s social media profile—public or private depending on the individual user’s security settings. Much of that information likely has limited value in assessing a particular employee or candidate’s suitability for a particular job. The information thus acquired by a prospective or current employer may be said in some instances to provide a richer picture of an individual and aid in the employer’s determination as to whether a particular employee or candidate is a proper “fit” for the organization. However, such social network information may also introduce subjective criteria and reinforce subtle biases based on information that may have little to no utility in assessing a particular employee or candidate’s suitability for a job.\textsuperscript{14} Permitting employers to riffle through the password-protected segments of candidates’ and employees’ social network accounts would seem only to increase the likelihood that employment decisions taken based on such information...
would be infected by implicit bias and other improper criteria.  

By accessing employees’ and applicants’ private online information, employers may also increase their exposure to potential liability for negligent retention and hiring claims. That is because once the private online content is accessible to the employer, it may be inferred that it would be negligent for a current or prospective employer to have failed to review and take appropriate action based on such information. Consequently, the net effect of restricting the employer’s access to private online content would be to protect employers from themselves.

To counter the spate of employers’ intrusions into private virtual domains of job applicants and employees, federal legislation was introduced in the 112th Congress that would bar employers from requiring employees or job applicants to provide user login or passwords to their social media and email accounts as a condition of employment. On April 27, 2012, Representatives Eliot Engel and Janice Schakowsky introduced the Social Networking Online Protection Act [referred to hereinafter as “SNOPA”] in the U.S. House of Representatives. On May 9, 2012, Senators Richard Blumenthal, Chuck Schumer, Ron Wyden, Jeanne Shaheen, and Amy Klobuchar introduced the Password Protection Act of 2012 [referred to hereinafter as “PPA”] in the U.S. Senate. These recent legislative efforts have been prompted in part by what has been characterized by some commentators as the inadequate or uncertain protections afforded by existing federal law. Neither of the federal bills

15 Cf. id. at 258 (“The social networking check allows the actor’s implicit bias to unwittingly affect the earliest stage of the hiring process. . . .”).

16 Katherine A. Peebles, Negligent Hiring and the Information Age: How State Legislatures Can Save Employers From Inevitable Liability, 53 WM. & MARY L. REV. 1397, 1416 (2012) (“noting that “some commentators and attorneys have warned hiring officials that failing to screen potential employees via the Internet may expose them to negligent hiring liability”). See id. (“Because running a

Google search is even simpler than conducting a traditional background investigation, courts will almost certainly rule that employers should have known about any Internet-based information that

speaks to an applicant’s dangerous proclivities.”).


19 On March 25, 2012, Senators Blumenthal and Schumer, co-sponsors of the PPA, wrote letters to U.S. Attorney General Eric Holder and Jacqueline A. Berrien, the Chair of the U.S. Equal Employment Opportunity Commission (“EEOC”) asking that they investigate whether “requiring job applicants to provide their usernames and passwords to social networking sites like Facebook as part of the hiring process” might violate existing federal law. Press Release, Blumenthal & Schumer, Employer Demands For Facebook And Email Passwords As Precondition For Job Interviews May Be A Violation Of Federal Law; Senators Ask Feds To Investigate (Mar. 25, 2012), available at 

THE NEED FOR STRONGER PRIVACY PROTECTION

progressed past the committee stage in the 112th Congress. On February 6, 2013 and August 1, 2013, respectively, SNOPA and PPA were reintroduced in the 113th Congress.20

Several states have also enacted or proposed legislation intended to protect job applicants’ and employees’ private online information.21 In May 2012, Maryland became the first state to enact a password-protection statute.22 Since that time, another ten states have enacted password-protection statutes, and provisions are under consideration in some twenty other states.23

The state statutes vary widely as to their scope in a number of key areas including: (1) what conduct is proscribed; (2) whether only social media accounts are protected, or other online accounts such as electronic mail, are also covered; (3) whether employees and applicants are afforded a private right of action; (4) what remedies are available; and (5) whether there are statutory exceptions for instances in which employers seek access to password-protected personal information in furtherance of legitimate business purposes, such as workplace harassment investigations or compliance with legal or regulatory requirements.24 The relentless profusion of varying state provisions is an expanding mosaic of uncertainty for employers, employees and applicants.25

This Note posits that a comprehensive federal statute is needed to provide employees and applicants with the means to protect their private online information from unwarranted scrutiny by employers. The Note’s model federal statute, the Personal Electronic Account Privacy Protection

senators observed that the practice could provide employers with “access to private, protected information that may be impermissible to consider when making hiring decisions,” such as “personal communications, religious views, national origin, family history, gender, marital status, and age.” Id.20


24 Id.24

25 At least one commentator has proposed federal preemption as a means to address the hodgepodge of state laws. See id. (arguing that “the only cure for the tangle of state law restrictions on access to social media content would be a federal law that preempts all of the state laws”). This Note suggests that rather than pursuing such a draconian intrusion on state police power, a more measured approach is warranted — i.e., a federal law that contains an election-of-remedies provision such that resort to the federal law would relinquish a state law claim for the same underlying conduct. See infra pp. 9 & note 27.
Act [referred to hereinafter as the "PEAPPA"], would protect employee and applicant private online information by setting a nationwide standard that is certain and manageable.

In particular, the PEAPPA would explicitly provide for the following:

- Private right of action for employees and applicants against employers for violations of the Act;

- Private right of action for employees and applicants against providers of social network sites and other online service providers who fail to provide users a minimum thirty days' advance written notice and an opportunity to opt out of the subject service prior to making changes to privacy policies, terms of service, or taking other actions which have the effect of disclosing users' private account information;

- Private right of action for dissemination of private information by employer, except where necessary to comply with law or to report a good-faith belief that the employee or applicant has violated a federal, state or local law or ordinance;

- Compensatory, statutory and punitive damages;

- Injunctive and declaratory relief;

- Exceptions for certain legitimate employer inquiries, and compliance with legal and regulatory requirements;

- Election-of-remedies provision such that the commencement of an action under PEAPPA would constitute a waiver of the rights and remedies available to an applicant or employee under any other Federal or State law, rule or regulation, or the common law based on the same conduct, while preserving statutory and common-law claims distinct from the PEAPPA claim.27

26 See infra pp. 29–32.

Part II of this Note details the challenges presented by the existing federal framework by the use of the Stored Communications Act28 [hereinafter, the “SCA”] and the Computer Fraud and Abuse Act29 [hereinafter, the “CFAA”] in the protection of employees’ and applicants’ personal online social media and email accounts from scrutiny by employers. Part III of this Note addresses the limited efficacy of the common-law tort for invasion of privacy as a means to protect individuals’ private social media and email account information from unwarranted intrusion by their employers. Part IV of this Note outlines the approach of the model statute, the PEAPPA, and demonstrates how its salient provisions would address significant shortcomings in the federal proposals and myriad state statutes.

II. EXISTING FEDERAL STATUTORY FRAMEWORK

A. The Stored Communications Act

In several cases involving allegations of inappropriate access to employees’ online account information, parties have resorted to the SCA to seek redress.30 “The SCA makes it an offense to ‘intentionally access[] without authorization a facility through which an electronic communication service is provided . . . and thereby obtain[] . . . access to a wire or electronic communication while it is in electronic storage in such system.’”31 Because the SCA was enacted in 1986, it has been noted that “[c]ourts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfactory results.”32 In Crispin v. Christian Audigier Inc., for example, the court

30 See, e.g., Konop v. Hawaiian Airlines, 302 F.3d 868 (9th Cir. 2002) (company violated SCA by improperly accessing employee’s password-protected restricted access website using co-worker’s credentials); Pietrylo v. Hillstone Rest. Group, No. 06-5754 (FSH), 2009 U.S. Dist. LEXIS 88702, at *9 (D.N.J. Sept. 25, 2009) (declining to overturn jury award in plaintiffs’ favor under SCA where it was reasonable for jury to infer that company supervisor coerced plaintiffs’ co-worker into accessing password-protected Myspace chat room in her presence); Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 587 F. Supp. 2d 548 (S.D.N.Y. 2008) (holding that company employees violated SCA by accessing co-worker’s personal Hotmail account to establish that he intended to start a competing business; the employees accessed the co-worker’s personal email by using his password that had been saved on his company computer). See also Crispin v. Christian Audigier Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010) (holding that private Facebook and Myspace posts are covered by the SCA).
32 Konop, 302 F.3d at 874.
noted that “the difficulty is compounded by the fact that the [SCA] was written prior to the advent of the Internet and the World Wide Web [and] as a result, the existing statutory framework is ill-suited to address modern forms of communication.”

1. Pietrylo v. Hillstone Restaurant Group

In Pietrylo v. Hillstone Restaurant Group, plaintiffs alleged that their employer violated the SCA when a restaurant manager accessed a secure password-protected Myspace chat room, Spec-Tator, which was used by plaintiffs and their co-workers as a forum for employees to complain about the employer. The manager instructed one of the plaintiffs’ co-workers to access the site so that the manager could read the chat room posts. Based on the company’s determination that the Spec-Tator posts were offensive and violated company policy, the company fired the plaintiffs.

The plaintiffs brought suit in New Jersey federal court asserting statutory and common-law claims. After dismissal of certain claims by pretrial motions and stipulation, the parties proceeded to trial on the remaining claims for violation of the SCA and the analogous New Jersey statute, common-law invasion of privacy and wrongful termination in violation of public policy. After a jury found in favor of plaintiffs on their SCA and New Jersey statutory claims, the defendant moved for a new trial on the basis that there was insufficient evidence adduced at trial to establish that the manager’s access to Spec-Tator was without authorization because she was allowed to view the chat room by an authorized user. The trial court denied the motion, holding that “the jury could reasonably infer . . . that [the co-worker’s] purported ‘authorization’ was coerced or provided under pressure.” Consequently, the trial court upheld the jury’s finding against defendants on the SCA claim.

Although the Pietrylo court found in plaintiffs’ favor on their SCA claim, it is noteworthy that the issue of liability turned on the fact-specific question of whether defendants were authorized to access the password-protected Myspace chat room. Given the asymmetry of bargaining power in the typical employer-employee relationship—which is even more so in the

---

33 717 F. Supp. 2d at 983 (quoting Konop, 302 F.3d 868 at 874).
35 Id.
36 Id. The jury found in defendants’ favor on the common-law invasion of privacy claim and as a result, the parties agreed that the jury did not need to deliberate on the plaintiffs’ claim for wrongful termination in violation of public policy. Id. n.1.
37 Id.
THE NEED FOR STRONGER PRIVACY PROTECTION

case between prospective employer and applicant—it is not clear that an employee’s authorization to access private online information could be deemed freely given. Rather, when an employer requests or demands access to an applicant’s or employee’s private online information, the inherent inequality in the relationship renders such consent of dubious weight.

As discussed in Part IV infra, the provisions of the PEAPPA model statute would protect employees and applicants by setting a definitive bright line, making clear that requiring or requesting an employee or applicant to provide access to his or a co-worker’s private online information is impermissible unless an enumerated exception applies.38

2. Increasing Uncertainty As to Applicability of SCA to Online Account Information

Notwithstanding that some courts have found the SCA to apply in cases involving unauthorized access to employees’ personal online accounts,39 there is growing uncertainty among the courts as to whether the statute applies in such circumstances. The SCA prohibits “intentionally accessing without authorization a facility through which an electronic communication service is provided,” and thereby obtaining access to an “electronic communication while it is in electronic storage.”40

The question of whether a particular electronic communication is in “electronic storage” for purposes of the SCA is one that is unsettled by the courts.41 In the email context, the question of whether a communication is in electronic storage can turn on whether an email in the intended recipient’s in-box has been read or not.42 This conundrum is due in part to the fact that “[w]hen the SCA was enacted in 1986, computers were expensive and primarily used for storing and processing information” and that “E-mail providers only maintained a user’s information temporarily in ‘electronic storage’ before the information was delivered to the recipient.”43

38 See PEAPPA § 3, infra pp. 29–30.
39 See supra note 30.
41 See Rene, 817 F. Supp. 2d at 1095–96 (collecting cases).
42 Id. (“It is unclear whether opened email messages are in electronic storage.”) (collecting cases).
In Rene, the court declined to reach the issue of whether the email communications in question were in electronic storage, holding that although the plaintiff’s complaint did not state “whether the email messages accessed by the Defendants had already been opened by her, [plaintiff] Rene [was] not required to allege such details at [the motion to dismiss] stage. Id. at 1097.
43 Lindsay S. Feuer, Who Is Poking Around Your Facebook Profile?: The Need to Reform the
Adding to the uncertainty as to the reach of the SCA, in October 2012, the South Carolina Supreme Court issued its decision in *Jennings v. Jennings*,44 a case involving allegations that plaintiff’s Yahoo! email account was hacked by his daughter-in-law, who guessed his security questions in order to access incriminating emails between the plaintiff and his mistress.45 The daughter-in-law allegedly provided copies of plaintiff’s emails to his estranged wife’s divorce attorney and private investigator.46 The plaintiff-husband filed suit, alleging that his daughter-in-law’s unauthorized access to his Yahoo! email account violated the SCA.

The South Carolina Supreme Court held that the plaintiff-husband’s emails on the Yahoo! server were not in “electronic storage” because they were not “stored for ‘purposes of backup protection.’”47 In effect, the majority reasoned that for the emails in plaintiff’s Yahoo! account to be considered backups, plaintiff would have had to keep copies of those messages elsewhere. Consequently, the court held that the intentional hacking into plaintiff’s email account did not violate the SCA.48

Whether a private Facebook wall posting or other electronic communication sent to an employee’s social networking account would fall within the purview of the SCA under the narrow definition of “electronic storage” enunciated in *Jennings* is uncertain at best. Following the rationale of *Jennings*, a court could hold that communications saved within a social networking site such as Facebook are not in electronic storage under the SCA unless a user saves another copy of the communications elsewhere.

For instance, applying *Jennings’* holding to the facts in *Pietrylo*, an argument could be made that communications in the Spec-Tator Myspace chat room were not backups unless the messages were


45 Id. at 243.
46 Id.
47 Id. at 245 ("We decline to hold that retaining an opened e-mail constitutes storing it for backup protection under the [SCA]."). In ruling that the ordinary meaning of the term “backup” required the existence of another copy of the emails in question, to which the copies on the Yahoo! server would serve as a “substitute or support,” the *Jennings* court explicitly rejected the reasoning of the United States Court of Appeals for the Ninth Circuit in *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004), which held that “e-mails which had been received and read, and then left on the server instead of being deleted, could be characterized as being stored ‘for purposes of backup protection’ and therefore kept in electronic storage under subsection (B).” 736 S.E.2d at 244–45.
48 Id. In a concurring opinion, the court observed that “[m]uch of the difficulty in applying the SCA to cases such as this arises because of the discrepancy between the current technology and the technology available in 1986 when the SCA was first enacted” and that “[t]he SCA is ill-fitted to address many modern day issues . . .” Id. at 248 (Beatty, J., concurring).
downloaded by plaintiffs, so could not be deemed in electronic storage for purposes of the SCA. As a result, the Pietrylo plaintiffs' SCA claim would likely not have made it to the jury.49

In light of the challenges in applying the SCA to modern technologies, and also the limitations of its reach to instances in which access is unauthorized, there is a need for a statutory scheme in the form of the model statute proposed in Part IV that would provide certain and specific protections to employees' and applicants' private online communications from improper access by employers. In addition, the expansive language of the PEAPPA would avoid constricted interpretations of covered technologies that would unduly limit its intended coverage.50

B. Computer Fraud and Abuse Act

Under the CFAA, a 1986 anti-hacking statute with criminal and civil provisions, a civil plaintiff may recover upon a showing that the defendant "intentionally access[ed] a computer without authorization or exceed[ed] authorized access, and thereby obtain[ed]... information from any protected computer; [or] ... "intentionally access[ed] a protected computer without authorization, and as a result of such conduct, cause[d] damage and loss."51 Under the CFAA's broad definition, a "protected computer" includes a computer that is used in interstate or foreign commerce.52 Consequently, the CFAA's broad scope has been held to cover the computers of the social networking site Myspace.53

49 By contrast, in Crispin, the court held that the Facebook wall posts and Myspacecomments were protected under the SCA. 717 F. Supp. 2d at 989 ("Given the court's conclusion that the BBS communication in Konop could not have been in temporary, intermediate storage, it appears that the passive action of failing to delete a BBS post, which is in all material ways analogous to a Facebook wall posting or a Myspacecomment, also results in that post being stored for backup purposes."). The court reasoned by analogy based on the Ninth Circuit's decision in Konop that, "[b]ecause Facebook wall postings and Myspacecomments, on the one hand, and bulletin postings on a website such as Konop's, on the other, cannot be considered to be in temporary, intermediate storage, the court interprets Konop as holding that the postings, once made, are stored for backup purposes." Id.

50 See PEAPPA § 2(c), infra p. 29 (defining a "personal electronic account" as "an electronic service, account, or electronic content created via a bounded system, that requires the employee or applicant for employment to input or store access information via an electronic device to view, create, utilize, or edit the employee or applicant's account information, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations, profile, display, communications, or other stored data").


53 See United States v. Drew, 259 F.R.D. 449, 458 (C.D. Cal. 2009) (holding that the "protected computer" requirement was met in criminal case involving improper use of Myspace in excess of its terms of use; the requirement "is satisfied whenever a person using a computer contacts an Internet
However, there are several obstacles to the use of the statute to protect employee and applicant private online information. The CFAA requires an employee to show that an employer accessed the employee's information intentionally and without authorization. As with the SCA, this requirement would likely be subject to repeated challenge in the employment context, as employers could be expected to counter CFAA claims by claiming that they were authorized by the employee or applicant to access their private online accounts, notwithstanding that the unequal bargaining position between the parties in most cases would tend to negate any claim that such access authorization could be freely given.

An additional challenge exists in the context of a CFAA civil action alleging unauthorized access to an employee's social media or email account. To maintain a private action under the CFAA, a party must also satisfy the "requirements of § 1030(g), which provides in relevant part [that] [a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 54

The requirement that a party demonstrates loss or economic damage under the CFAA is a significant hurdle to recovery in connection with cases involving unauthorized access to employees' password-protected social networking account information. As to loss under the CFAA, courts generally require that "the alleged 'loss' must be related to the impairment or damage to a computer or computer system." 55 It would be the rare case in which an employer's unauthorized access to an employer or applicant's online account could be shown to cause actual damage to an employee or applicant's computer. Rather, the nature of the injury in such cases in terms of violation of personal privacy is generally of a more inchoate nature.

As a result, a CFAA claim involving unauthorized or exceeded access to an employee or applicant's private online account information would likely lie only under 18 U.S.C. § 1030(c)(4)(i)(I), for which claims damages "are limited to economic damages." 56 The economic damages requirement of

55 Id. at *8 (internal citation omitted).
56 18 U.S.C. § 1030(g) (2006). The remaining clauses of the subsection provide for a civil action in the following instances, none of which would be present for unauthorized access to a user's social network account: "(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (III) physical injury to any person; (IV) a threat to public health or safety; [or] (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security." 18 U.S.C. § 1030(c)(4)(A)(I) (2006).
the CFAA limits the ability of employees and applicants to seek recovery for violations of their privacy rights resulting from employers’ intrusions into their private online accounts.

1. Eagle v. Morgan

The CFAA’s economic damages requirement proved fatal in a case involving allegations of improper access to a former employee’s social networking account. In Eagle, a former executive with Edcomm, an education banking company, brought suit under the CFAA alleging that her former employer improperly accessed her LinkedIn account without authorization and changed her password after terminating her employment.\(^{57}\) The company encouraged plaintiff to use her LinkedIn account as a marketing tool for the company. One of Edcomm’s employees assisted the plaintiff in maintaining her LinkedIn account and had access to her account password. When the company terminated plaintiff’s employment, Edcomm changed the password of the plaintiff’s LinkedIn account, thereby disabling her access. It also reset the profile to reflect the name and photograph of the company’s new interim CEO. Plaintiff alleged that as a result of these improper actions, her “business contacts or potential customers of [plaintiff’s], who were searching for her profile, [were] routed to a LinkedIn page featuring [the interim CEO’s] name and photograph, but [plaintiff’s] honors and awards, recommendations, and connections.”\(^{58}\)

The defendant-employer moved for summary judgment on plaintiff’s CFAA claim, arguing that she could not establish “a legally cognizable loss or damages [under 18 U.S.C. § 1030(g)] in the brief period in which her LinkedIn Account was accessed and controlled by Edcomm.”\(^{59}\) The court granted defendant’s motion, holding that her “claims that she was denied potential business opportunities as a result of Edcomm’s unauthorized access and control over her account . . . [were] simply not compensable under the CFAA.”\(^{60}\) The court also held that plaintiff’s alleged loss of goodwill and reputation due to her inability to respond to business contact during the time she was unable to access her LinkedIn account did not


\(^{58}\) Id. Plaintiff’s access to her LinkedIn account was disabled “from late June 20[1] through July 12, 2011. After filing suit, plaintiff contacted LinkedIn and was able to reestablish access to her account but “continued to be unable to receive messages on her account for a substantial period of time thereafter.”

\(^{59}\) Id.

\(^{60}\) Id.
amount to a cognizable loss under the CFAA.\textsuperscript{61}

The CFAA’s requirement that a party establish actual loss in the form of damage to a computer or economic loss is a bar to recovery for employees alleging improper access to their private online accounts. In most if not all cases, the damages that employees and applicants would suffer by being required to divulge their private online information would be difficult to quantify in terms of economic loss, and would not likely result in loss in the form of damage to a computer. Consequently, it would not seem that the CFAA provides sufficient protection for employees’ and applicants’ online privacy rights, which may not be readily quantified in terms of damage to computers or economic loss.\textsuperscript{62}

The PEAPPA would address this shortcoming by employing the damages framework of the SCA, which provides for recovery of actual or statutory damages, as well as reasonable attorney’s fees and punitive damages.\textsuperscript{63} These provisions will ensure that employees and applicants have adequate recourse against unwarranted invasions of their online personal accounts and that employers are prohibited from using their unequal bargaining power to coerce the disclosure of private online information as a condition of an offer of employment, or continued employment.

III. COMMON-LAW RIGHT TO PRIVACY

As noted by a recent decision addressing the scope of the common-law tort of invasion of privacy, “[p]rivacy in social networking is an emerging, but underdeveloped, area of case law.”\textsuperscript{64} In the formulation of the Restatement (Second) of Torts, “[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of...
his privacy, if the intrusion would be highly offensive to a reasonable person."\(^\text{65}\) The approach of the Restatement is predicated on the view that "'[t]he right protected by the action for the invasion of privacy is a personal right, peculiar to the individual whose privacy is invaded.'\(^\text{66}\)

Certain commentators have posited that the common-law approach is based on a conceptually restrictive view of the value of privacy, which is founded primarily on privacy's utility in terms of value to the individual, and to the exclusion of the broader societal value that privacy affords to the community as a whole.\(^\text{67}\) This view, it is suggested, overlooks that "[p]rivacy is valuable not only for our personal lives, but for our lives as citizens—our participation in public and community life. . . . [P]rivacy is more than a psychological need or desire; it is a profound dimension of social structure."\(^\text{68}\) As a result of this constricted view of the value of privacy, the common-law approach under the Restatement does not take proper account of these salutary societal benefits of privacy, which benefits also inure to the individual.\(^\text{69}\)

In recent cases applying the common-law tort of privacy in the social media context, this restrictive view of privacy has provided inadequate protection to the privacy rights of employees whose password-protected social media account information has been accessed by their employers.

A. Maremont v. Susan Fredman Designs Group, Ltd.

In Maremont v. Susan Fredman Designs Group, Ltd.,\(^\text{70}\) the plaintiff, a former marketing director for the defendant, brought suit in Illinois federal court, alleging that her former employer accessed and used her personal Twitter and Facebook accounts without her authorization to promote its

\(^{65}\) Restatement (Second) of Torts § 652B.

\(^{66}\) SOLOVE, supra note 62, at 89 (quoting Restatement (Second) of Torts § 652(1) cmt. a).

\(^{67}\) Id. ("The problem with framing privacy solely in individualistic terms is that privacy becomes undervalued. Often, privacy receives inadequate protection in the form of damages to compensate individual emotional or reputational harm; the effects of the loss of privacy on freedom, culture, creativity, innovation, and public life are not factored into the valuation.").

\(^{68}\) Id. at 93. See also Helen Nissenbaum, A Contextual Approach to Privacy Online, DJEDALUS, THE JOURNAL OF THE AMERICAN ACADEMY OF ARTS & SCIENCES (Fall 2011) ("Time spent on social networks, such as Facebook, is an amalgam of engagement with personal, social, intimate and home life, political association, and professional or work life.").

\(^{69}\) SOLOVE supra note 62, at 92 ("[P]rivacy harms affect the nature of society and impede individual activities that contribute to the greater social good."). See also id. at 91 ("When individualism is severed from the common good, the weighing of values is often skewed toward those equated with the common good, since the interests of society often outweigh the interests of particular individuals. When individualism is not considered at odds with the common good, we can better assess its values, contributions, and limitations.").

business while she was out of the office convalescing after a severe work-related automobile accident. 71 When plaintiff learned of her employer’s unauthorized use of her personal password-protected social network accounts, she asked that defendant and its employees cease using her Facebook and Twitter accounts while she was in the hospital. Defendant’s employees continued to use her personal online accounts to promote defendant’s business. 72

Based on the defendant’s unauthorized access to her personal Facebook and Twitter accounts, Ms. Maremont asserted claims for (1) false endorsement under the federal Lanham Act, (2) violation of the SCA, and (3) violation of her common-law right to privacy. The court dismissed her common-law right to privacy claim, holding that “the matters discussed in [plaintiff’s] Facebook and Twitter posts were not private and that [plaintiff] did not try to keep any such facts private.” Notably, the Maremont court reached this conclusion despite finding that “Facebook posts are accessible only to those whom the user selects, and thus they are not strictly public.” 73

What the Maremont court’s ruling overlooks is that, by posting information online to a select group of individuals on a social network, a user has not effectively ceded any privacy right. To argue otherwise would conflate privacy with secrecy. 74 For information to be treated as private, it need not be completely secret. 75 Rather, “[t]he mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be seen by everyone.” 76

71 Id. at *6.
72 Id. at *7.
73 Id. at n.2 (emphasis added).
74 See DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 178 (Yale Univ. Press 2007) (observing that in social networking context, “[t]here is no magic number” and that “[i]nstead of counting how many other people know certain information, we should focus on the social circles in which information travels.”), available at http://docs.law.gwu.edu/facweb/dsolove/Future-of-Reputation/text.htm; Carly Brandenburg, The Newest Way to Screen Job Applicants: A Social Networker’s Nightmare, 60 FED. COMM. L.J. 597, 598 (2011) (“The fact that a Facebook user could permit hundreds, or even thousands, of people to view her profile may not be the only indication of whether the social networker has a reasonable expectation of privacy where unwelcome viewers are involved. It seems plausible that ‘if you are using privacy features that you believe restrict access to very few specific people completely within your control, and an employer somehow hacks past such a privacy barrier, you may have a strong privacy claim.’”).
75 See M.G. v. Time Warner, Inc., 89 Cal. App. 4th 623, 632 (Cal. App. 4th Dist. 2001) (“[T]he claim of a right of privacy is not ‘so much one of total secrecy as it is of the right to define one’s circle of intimacy—to choose who shall see beneath the quotidien mask.’ Information disclosed to a few people may remain private.”). See also Connie Davis Powell, Privacy for Social Networking, 34 U. ARK. L. REV. 689, 702 (2012) (discussing cases which “suggest that even if an individual discloses information about himself to dozens of people without legal or contractual constraints on those people’s ability to disseminate the information further, the information can remain ‘private’ for the purposes of privacy tort law.”).
76 Powell, supra note 75, at 702-03 (quoting Sanders v. American Broad. Cos., 978 P.2d 67, 72
The court's decision is also silent as to whether any consideration was given to the viability of the common-law privacy claim based on the defendant-employer's unauthorized access to the non-public portions of the plaintiff's personal password-protected Facebook and Twitter accounts that would have been required to issue public Facebook postings and Tweets from her accounts. The fact that certain communications made from her password-protected accounts were made to the public did not amount to license for her employer to use her passwords without authorization to root through her personal accounts for its own benefit.

Under the proposed PEAPPA, courts would be relieved of the need to engage in such unnecessary inquiries as to whether a user reasonably believed that its password-protected communications were private. Nor would there be a need for a factual finding that such an intrusion is "highly offensive."\(77\) Rather, the PEAPPA effectively engrafts a blanket presumption that it is highly offensive for an employer to access a current or prospective employee's personal online account information, unless a valid exception applies.\(78\)

**B. Pietrylo v. Hillstone Restaurant Group**

As noted above in Part II.A.1, in *Pietrylo*, the plaintiffs alleged that their manager accessed a secure password-protected Myspace chat room, Spec-Tator, which was used by plaintiffs and their co-workers as a forum for employees to complain about the employer. The jury found that the employer's conduct violated the SCA;\(79\) the jury, however, found against plaintiffs on their common-law invasion of privacy claim.\(80\) It is noteworthy that the court held that, as with their SCA claim, "the ability of Plaintiffs to recover on [the common-law claim] for invasion of privacy turn[ed] on the disputed issue of whether or not [the co-worker] gave 'consent' for Defendant to view the Spec-Tator."\(81\)

However, in a seemingly inconsistent finding, the jury found in the affirmative on the question of whether the plaintiffs' password-protected Myspace chat room was "a place of solitude and seclusion which was designed to protect the Plaintiffs' private affairs," but held nonetheless that plaintiffs did not have a reasonable expectation of privacy in the Spectator

---

77 Restatement (Second) of Torts § 652B.
79 See supra pp. 10–11.
81 Id.
chat room. In effect, the jury determined that the company improperly accessed the Myspace page without consent as to the SCA claim, but that it was not reasonable for plaintiffs to expect that their consent would be required to access their "place of solitude and seclusion which was designed to protect [their] private affairs and concerns" as to the common-law privacy claim.

Other courts have also reached similarly discordant results in attempting to apply the common-law of privacy to social networking sites. In light of holdings in these cases, it is evident that the fact-specific nature of inquiries as to whether and when a reasonable expectation of privacy exists for password-protected online activity leaves employees and applicants with limited protection at common law in instances in which their password-protected online information has been improperly compromised.

C. The Mistaken Notion That Users Do Not Expect Privacy in Their Online Interactions

There is the view professed in certain quarters that privacy is a dead letter in the online agora, pointing to the alacrity with which users of social networks share their personal information in such fora. For instance, in January 2010, Facebook CEO Mark Zuckerberg, remarked that there has been something of a paradigm shift as relates to users' online privacy expectations: "[P]eople have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time."

While it may be that some people have become more comfortable with sharing information online, what Mr. Zuckerberg's statement overlooks is the extent to which social network users have a more particularized or context-specific view as to the appropriate flow of their online

---

83 Id.
84 See Ehling, 2012 U.S. Dist. LEXIS 74558, at *12 (observing that "Courts . . . have not yet developed a coherent approach" and "differ dramatically" as to whether a reasonable expectation of privacy exists in password-protected online communications that are shared with others) (collecting cases).
85 NISSENAUM, supra note 1, at 221 (noting "the apparent abandon with which participants confide their inner thoughts and post personal information and photographs of themselves and others to their profiles," which "leads many people . . . to assert that 'the youth of today' do not care about privacy.").
86 Marshall Kirkpatrick, Facebook's Zuckerberg Says the Age of Privacy is Over, READWRITE (Jan. 9, 2010), http://readwrite.com/2010/01/09/facebook_zuckerberg_says_the_age_of_privacy_is_over.
communications. That is, employees and applicants expect that their information is used within the online context as they intended it to be used and for no other reasons. Studies suggest that users of social networks are becoming increasingly concerned about the protection accorded to their online personas and are more often availing themselves of the sites’ privacy settings. By so doing, users are effectively registering their intent that their online content be treated as private.

To demonstrate the extent to which users of social media are concerned with the privacy of their online communications one need only look to the backlash that ensued as a result of unilateral changes by social network providers to their terms of service as relates to the privacy of users’ account information. For instance, in December 2012, a user revolt erupted when Instagram, an online photo-sharing site owned by Facebook, reported that it intended to change its terms of service in a manner that was widely interpreted as suggesting that Instagram intended to “begin selling its user photos to advertisers without users’ consent.” As a result of public uproar, the company agreed to revert to its prior terms of service with respect to advertising. The vehemence of the user response to...

87 NISSENBAUM, supra note 1, at 127.

A right to privacy is neither a right to secrecy nor a right to control, but a right to appropriate flow of information. Privacy may still be posited as an important human right or value worth protecting through law and other means, but what this amounts to is a right to contextual integrity and what this amounts to varies from context to context.

Id.; See also Patricia Sánchez Abril, Avner Levin & Alissa Del Riego, Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee, 49 AM. BUS. L.J. 63, 124 (2012) (concluding that, although millennials are comfortable sharing private information in online fora, they maintain an expectation of “network privacy,” or “audience segregation” and as such are uncomfortable with being “forced to share with unintended audiences and objected to being judged across contexts.”).

88 MARY MADDEN & AARON SMITH, PEWRESEARCHCENTER, REPUTATION MANAGEMENT AND SOCIAL MEDIA 29 (May 26, 2010), available at http://pewinternet.org/~/media//Files/Reports/2010/PIP_Reputation_Mangement_with_topline.pdf (noting that “71% of social networking users ages 18-29 have changed the privacy settings on their profile to limit what they share with others online” and “55% of SNS users ages 50-64 have changed the default settings”).

89 See Adam Pabarcus, Contemporary Issues in Cyberlaw: Are “Private” Spaces on Social Networking Websites Truly Private? The Extension of Intrusion Upon Seclusion, 38 WM. MITCHELL L. REV. 397 (2011) (advocating change to common-law privacy tort such that “[w]hen social network users create a private profile or group, it is as if they are closing the virtual door behind them. Everyone, including people off of Facebook, can no longer see their profile or groups. Any unauthorized monitoring or viewing of the private virtual space would constitute an intrusion.”).


Instagram’s announced changes to its terms of service keenly demonstrates the extent to which users intend that the private information they post and share on such sites be shared no further than to those with whom they have intentionally communicated that information.

One commentator argues that the "bait and switch" tactics and opaque and prolix terms of service used by social networking sites have resulted in user confusion as to what information is accessible to the public, thus exposing them to unnecessary risk of harm." Although it has been estimated that a small number of users actually read the terms of service of the social network to which they belong—and even fewer actually comprehend them, this does not mean that users’ expectation that the information that they set as private should remain so is unreasonable. In the case of Facebook, the serial changes to its privacy policies have limited users’ ability to control the privacy of personal information on the social network. Indeed, certain changes to Facebook’s privacy settings have invited regulatory action by the Federal Trade Commission.

Moreover, notwithstanding the uncertain solace that social networks’ privacy settings and terms of service may offer, there are still valid reasons that users choose to share personal information online. In the employment context, a 2010 survey suggests a significant disconnect as relates to U.S. consumers’ expectation as compared with the reality of how their online information is accessible.

---

92 Connie Davis Powell, Social Networking and the Law: You Already Have Zero Privacy. Get Over It!, Would Warren and Brandeis Argue for Privacy for Social Networking?, 31 PACE L. REV. 146, 169 (2011) (observing the “troubling . . . change of privacy policies, which often occur after users have disclosed personal information”). See also SOLOVE supra note 62, at 73 (suggesting that “several factors can affect people’s decisions about privacy,” including, “limited bargaining power respecting privacy and inability to assess the privacy risks.”).

93 See James Grimmelmann, Saving Facebook, 94 IOWA L. REV. 1137, 1183 (2009) (citing a “2006 survey of Facebook users [which] found that seventy-seven percent had never read its privacy policy and that large majorities had mistaken beliefs about how Facebook collected and shared personal information”).

94 Kurt Opsahl, Facebook’s Eroding Privacy Policy: A Timeline, ELEC. FRONTIER FOUND. (Apr. 28, 2010), https://www.eff.org/deeplinks/2010/04/facebook-timeline/. See also Nick Bilton, Facebook Changes Privacy Settings, Again, N.Y. TIMES BITS (Dec. 12, 2012, 10:35 AM), http://bits.blogs.nytimes.com/2012/12/12/facebook-changes-privacy-settings-again/ (noting changes that, while improving certain privacy settings, also “eliminat[ed] the ability for people to hide themselves on Facebook’s search, a control, that until now, has existed in the privacy settings on the company’s Web site”).

95 See, e.g., Press Release, FTC Approves Final Settlement With Facebook, Facebook Must Obtain Consumers’ Consent Before Sharing Their Information Beyond Established Privacy Settings, available at http://ftc.gov/opa/2012/08/facebook.shtm. Under the terms of the settlement with the FTC, Facebook has agreed to “giv[e] consumers clear and prominent notice and obtaining their express consent before sharing their information beyond their privacy settings, . . . “maintain[] a comprehensive privacy program to protect consumers’ information, and . . . “obtain[] biennial privacy audits from an independent third party.” Id.

96 Id. at 73 (suggesting that “several factors can affect people’s decisions about privacy,” including, “limited bargaining power respecting privacy and inability to assess the privacy risks.”).
information is used in hiring decisions. According to the survey, 70% of U.S. recruiters and HR professionals surveyed rejected job candidates based on information found online, but “only 7% of U.S. consumers surveyed believe information about them online affected their job search.

There is, however, a growing awareness of the need to restrict online information flow in connection with one’s employment status within the U.S. workforce, particularly among younger users of social networking sites. A 2013 survey of social media users between the ages of 18 and 34 revealed that over a quarter of those surveyed were concerned that content they posted could negatively impact their employment. Of those surveyed, 21% reported that they had removed content from their social media accounts in order to avoid employer scrutiny and 82% said they “pay at least some attention to their privacy settings.” In light of this increasing recognition of the need of users to control the flow of information in their personal electronic accounts, appropriate federal protection in the form of the PEAPPA proposed herein is needed.

IV. PROPOSED MODEL STATUTE – THE PERSONAL ELECTRONIC ACCOUNT PRIVACY PROTECTION ACT

A. Key Provisions

The model Personal Electronic Account Privacy Protection Act ("PEAPPA") seeks to eliminate any ambiguity as to whether an individual’s personal online content is protected from access by a current or prospective employer. Simply stated, once an employee or applicant has set her social network or other electronic account so that access to online content is protected from public view, the inquiry is at an end. By so doing, the employee or applicant has established a reasonable expectation that his online content should be treated as private.

By dispensing with the need for a fact-specific common-law inquiry as to whether there is a personal privacy violation, the PEAPPA would send a clear message in favor of the broader societal value in protecting

97 Supra note 8.
98 Id. at 5.
99 See Wang, supra note 10. See also MARY MADDEN & AARON SMITH, PEWRESEARCHCENTER, REPUTATION MANAGEMENT AND SOCIAL MEDIA 29 (May 26, 2010), http://pewinternet.org/-/media//Files/Reports/2010/PIP_Reputation_Management_with_topline.pdf (noting that “71% of social networking users ages 18-29 have changed the privacy settings on their profile to limit what they share with others online” and “55% of SNS users ages 50-64 have changed the default settings”).

individuals' private online communications. The protected content would then not be accessible to the employer unless an appropriate exception warrants such disclosure. In the case of enumerated job classes, such as those involving national security, law enforcement, or certain regulated industries, the burden would shift to the employer to demonstrate that its need for the employee or applicant's private online information fell within a particular enumerated exception.

The PEAPPA would also reduce ambiguity as to whether an employee or applicant assented to the disclosure of his private online information. Rather, because employers would be barred from requesting such access to private online information, the PEAPPA would protect employees and applicants from any subtle coercive measure that might be argued to constitute authorized access. Further, unlike the CFAA, the PEAPPA would not require that a party show economic loss or damage to a computer as a result of the employer's violative access to private online information to establish entitlement to relief. This would serve to ensure that the individual and broader societal interest in privacy protection is afforded appropriate value.

1. Definitions

The proposed model statute would prohibit employers from requesting or requiring current or prospective employees to provide access to their "personal electronic accounts," which are defined as:

an electronic service, account, or electronic content created via a bounded system, that provides the employee or applicant for employment with the ability to input or store access information via an electronic device to view, create, utilize, or edit the employee or applicant's account information, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations, profile, display, communications, or other stored data.

The broad definition is intended to cover not only social network accounts, but also email accounts, and other electronic communication channels that may emerge in the future. In that way, the statutory text would avoid the challenges of applying the outmoded language of the SCA.
to new and emerging communications platforms.\textsuperscript{103}

2. Prohibited Conduct

a. Employers

Under the model PEAPPA, employers would be prohibited from requiring or requesting that an employee or applicant provide access, allow observation or disclose information to permit access to the employee’s or applicant’s personal electronic accounts. This provision would prevent both employers from requesting users’ passwords, as well as the practice of shoulder-surfing, in which the employer reads over the employee’s or applicant’s shoulder while she logs in to her private online accounts. In addition, the model statute would also prohibit conduct such as that at issue in Pietrylo in which the company supervisor watched the screen while the plaintiffs’ co-worker accessed the Spec-Tator chat room.\textsuperscript{104} Furthermore, the PEAPPA includes a provision prohibiting employers from otherwise accessing employee or applicant private social networking or other electronic content, to eliminate any ambiguity as to co-worker consent to obtain access a subject employee private online information.

The PEAPPA also contains broad anti-retaliation provisions, which cover both instances in which employees and applicants refuse to provide password-protected personal electronic account information, as well as where they participate in proceedings under the Act.\textsuperscript{105} These provisions ensure that employees and applicants can vindicate their rights under the PEAPPA without fear of retribution.\textsuperscript{106}

b. “Personal Electronic Account Service Providers”

The PEAPPA would also create a private right of action against providers of personal electronic accounts that fail to provide, with a minimum of thirty days’ advance written notice to users, and an opportunity to opt out of the subject service prior to making changes to

\textsuperscript{103} See supra Part II.A.

\textsuperscript{104} See PEAPPA § 3(a)(1), infra p. 30 (prohibiting employers from requiring or requesting employee or applicant to “allow observation of” their personal electronic account).

\textsuperscript{105} Id. § 2(a)(2).

\textsuperscript{106} The PEAPPA’s anti-retaliation provision would permit for recovery for retaliation where the current or prospective employee shows that the denial to provide access to a personal electronic account was a “motivating factor,” as opposed to the “but for” cause of the retaliatory action by an employer. PEAPPA § 3(a)(3)(C). Cf. Univ. of Tex. S.W. Med. Ctr. v. Nassar, 133 S. Ct. 2517, 2534 (2013) (“The text, structure, and history of Title VII demonstrate that a plaintiff making a retaliation claim under § 2000e-3(a) must establish that his or her protected activity was a but-for cause of the alleged adverse action by the employer”).
privacy settings, terms of service, or taking other actions that would have the “effect of publicly disclosing personal electronic account information.” This provision is intended to give additional force to the employer prohibitions against requesting or requiring the disclosure of personal electronic account information. It does so by ensuring that employees and applicants have some level of comfort that their online account privacy settings will not be changed precipitously by online service providers to their detriment.

3. Exceptions

The PEAPPA incorporates a number of the exceptions intended to permit employer inquiries into otherwise protected personal electronic account information in connection with certain positions, such as those involving working directly with minors, and those within the financial services industry who are required by law or rule to monitor online communications of certain registered individuals. In such instances, the Act puts the onus on the employer to ensure that such private information is not improperly disseminated.

The PEAPPA gives additional protection to employers by explicitly providing that it does not create a duty for employers to search personal electronic accounts, which ensures that claims of negligent retention or hiring would not result from employers’ compliance with the Act’s prohibitions. These provisions are intended to strike an appropriate balance to allow employers latitude to conduct legitimate, good-faith investigations in the course of their business.

4. Remedies

The PEAPPA would provide a private right of action, equitable and declaratory relief, as well as compensatory, statutory and punitive damages. These remedial provisions are intended to ensure that the Act provides a sufficient bulwark against improper transgressions by employers or personal electronic account service providers in their handling of employees’ and applicants’ private online information. It is submitted that

107 Id. § 2(b)(1).
109 Id. § 5.
110 See Pure Power Boot Camp, 587 F. Supp. 2d 548. But see Van Alstyne v. Electronic Scriptorium, Ltd., 560 F.3d 199, 201–02 (4th Cir. 2009) (holding that a plaintiff must prove actual damages in order to recover statutory damages under the SCA, but may recover punitive damages, attorney fees and costs without showing actual damages).
without these measures, employees and applicants would be without adequate means to protect their personal privacy interests as companies would have less incentive to comply without the threat of civil litigation and liability.

CONCLUSION

“Privacy . . . has a social value—it shapes the communities in which we live, and it provides necessary protection of individuals against various types of harms and disruptions. . . . We establish privacy protections because of their profound effects on the structure of power and freedom within society as a whole. The protection of privacy shields us from disruption to activities important to both individuals and society.”\(^{111}\)

Efforts to protect employees’ and applicants’ online private information under the existing framework of the SCA, CFAA and the common law have resulted in inconsistent and inequitable outcomes for employees and applicants. A model federal statute in the form of the PEAPPA would serve to eliminate confusion and uncertainty created by varying standards under the SCA, CFAA and the common law. By eliminating the requirement under the SCA and CFAA that an employee or applicant show that an employer’s access to protected content was not authorized, the model statute would provide greater clarity and protections to employees, applicants and employers as to the private online information that is presumed to be off limits. This would level the playing field given the decidedly unequal bargaining power between most employees’ and applicants’ and current and prospective employers.

By also providing employees and applicants with a private cause of action against electronic account service providers where those companies acts or omissions cause the unwarranted disclosure of private information, the model statute would also serve to incent service providers to hew to the spirit and letter of the privacy policies and terms of service and to take care that changes in such policies are undertaken in a manner that protects the private content of employees and applicants.

\(^{111}\) SOLOVE supra note 62, at 92.
PERSONAL ELECTRONIC ACCOUNT PRIVACY PROTECTION ACT

Sec. 1. Title
This Act shall be known and may be cited as the “Personal Electronic Account Privacy Protection Act.”

Sec. 2. Definitions
As used in this Act:
(a) “Access information” means user name, password, login information, or other security information that protects access to a personal electronic account.
(b) “Employer” means a person, including a unit of federal, state or local government, engaged in a business, industry, profession, trade, or other enterprise and includes an agent, representative, or designee of the employer, acting directly or indirectly in the interest of an employer in relation to an employee or an applicant for employment;
(c) “Personal electronic account” means an electronic service, account, or electronic content created via a bounded system, that requires the employee or applicant for employment to input or store access information via an electronic device to view, create, utilize, or edit the employee or applicant’s account information, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations, profile, display, communications, or other stored data;
(d) “Personal electronic account service provider” means a person, engaged in the business, industry, profession, trade, or enterprise of providing personal electronic account services, and includes an agent, representative, or designee of the personal electronic account service provider, acting directly or indirectly in the interest of an personal electronic account service provider.

Sec. 3. Prohibited Conduct
(a) It shall be unlawful for any employer—
(1) to require or request that an employee or applicant for employment provide access to, allow observation of, or disclose information that allows access to or observation of an employee’s or applicant’s personal electronic account; or
(2) to otherwise access or observe the content contained on an employee’s or applicant’s personal electronic account that would require access information to access or observe; or
to discharge, discipline, discriminate against in any manner, or deny employment or promotion to, or threaten to take any such action against, any employee or applicant for employment because—

(A) the employee or applicant for employment refuses or declines to provide access to, allow observation of, or disclose information that allows access to or observation of the employee’s or applicant’s personal electronic account; or

(B) such employee or applicant for employment has filed any complaint or instituted or caused to be instituted any proceeding under or related to this Act or has testified or is about to testify in any such proceeding.

(C) A violation is established under subsection (a)(3)(A) or (a)(3)(A) when the employee or applicant party demonstrates that their denial of access to a personal electronic account was a motivating factor for any practice prohibited under subsection (a)(3), even though other factors also motivated the practice.

(b) It shall be unlawful for any personal electronic account service provider—

(1) To fail to provide users of a personal electronic account a minimum thirty days’ advance written notice prior to making changes to privacy policies, terms of service, or taking other actions which have the effect of disclosing users’ private account information that have the effect of publicly disclosing personal electronic account information.

Sec. 4. Exceptions

(a) This Act does not prohibit an employer from doing any of the following:

(1) Conducting an investigation or requiring an employee to cooperate in an investigation in any of the following circumstances:

(A) If there is specific information about activity on the employee’s or applicant’s personal electronic account, for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct.

(B) If the employer has specific information about an unauthorized transfer of the employer’s proprietary information, confidential information, or financial data to an employee’s personal electronic account.

(2) Restricting or prohibiting an employee’s access to certain websites while using an electronic communications device paid for in whole or in part by the employer or while using an employer’s network or resources.

(3) 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.

(4) Complying with a duty to screen employees or applicants prior to hiring or to monitor or retain employee communications that is established under federal law or by a self-regulatory organization, as defined in § 3(a)(26) of the Securities and Exchange Act of 1934, 15 U.S.C. § 78c(a)(26).

(5) This Act does not prohibit or restrict an employer from requiring or requesting that an employee or applicant for employment provide access to, allow observation of, or disclose information that allows access to or observation of an employee’s or applicant’s personal electronic account with respect to the particular classes of employees set forth below in subsections (A) through (C) and the employer’s action relates to employees in such class who work or seek to work:

(A) in a position involving contact with individuals under 13 years of age; or
(B) in a position involving law enforcement; or
(C) in a position involving national security.

Notwithstanding the foregoing exceptions, an employer shall be liable under this Act in the event that it discloses an employee’s or applicant’s personal electronic account information unless such disclosure is required to comply with federal or state law.

(6) This Act does not prohibit or restrict an employer from viewing, accessing, or utilizing information about an employee or applicant that can be obtained without any required access information or that is available in the public domain.

Sec. 5. No Creation of Employer Duties
This Act does not create a duty for an employer to search or monitor the activity of a personal electronic account.

Sec. 6. Civil cause of action
(a) An individual who is the subject of a violation of this Act may bring a civil action to recover from the person or entity engaged in that violation such relief as may be appropriate.

(b) Relief. In a civil action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;
(2) damages under subsection (c); and
(3) a reasonable attorney’s fee and other litigation costs reasonably
incurred.

(c) Damages. The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

Sec. 7. Election of Remedies
Nothing in this act shall be deemed to diminish the rights, privileges, or remedies of any employee or applicant under any other Federal or State law or regulation or under any collective bargaining agreement or employment contract; except that the institution of an action in accordance with this act shall be deemed a waiver of the rights and remedies available under any other Federal or State law, rule or regulation, or the common law.