McGeorge Law Review

Volume 44 | Issue 3 Article 23

1-1-2013

Cyberfrontier: New Guidelines for Employers Regarding Employee Social Media

Michelle Scheinman
Pacific McGeorge School of Law

Labor

Cyberfrontier: New Guidelines for Employers Regarding Employee Social Media

Michelle Scheinman

Code Section Affected

Labor Code § 980 (new).
AB 1844 (Campos); 2012 STAT. Ch. 618.

I. INTRODUCTION

After taking a brief leave of absence to grieve the loss of his mother, Robert Collins reapplied for his job with the Maryland Department of Corrections.[1] Mr. Collins was shocked when the interviewer not only requested his private Facebook password, but also logged into the site and rummaged through his most personal photographs and messages.[2] Mr. Collins' Facebook page was set to the highest privacy level in an effort to protect its content from public view.[3] When the interviewer requested access to his account, Mr. Collins felt compelled to capitulate because failure to comply might block his reinstatement.[4] Reports of Mr. Collins' experience caused a public outcry[5] and prompted the Maryland State Legislature to enact a novel law forbidding an employer from requesting that an employee or job applicant provide a "user name, password, or other means for accessing a personal account."[6]

The Maryland Department of Corrections is not the only public agency to request access to password-protected social media accounts.[7] Various agencies responsible for staffing law enforcement and 9-1-1 emergency communications officers may routinely require applicants and current employees to divulge social

1. Nick Madigan, *Officer Says He Had to Give Facebook Password for Job*, BALTIMORE SUN, Feb. 24, 2011, at 3A.

2. *Id.*; Melissa Coretz Goemann, *Maryland Passes Nation's First Social Media Privacy Protection Bill*, ACLU BLOG OF RIGHTS (May 4, 2012, 4:30 PM), https://www.aclu.org/blog/technology-and-liberty/maryland-passes-nations-first-social-media-privacy-protection-bill (on file with the *McGeorge Law Review*).

3. Madigan, *supra* note 1.

4. *Id.*

5. *ACLU Responds to Maryland Division of Corrections' Revision of Invasive Social Media Policy*, POGOWASRIGHT (Apr. 6, 2011), http://www.pogowasright.org/?p=22268 (on file with the *McGeorge Law Review*).

6. MD. CODE ANN., LAB. & EMPL. § 3-712(B)(1) (enacted by Chapter 233, Oct. 1, 2012).

7. Manuel Valdes & Shannon McFarland, *Job Seekers' Facebook Passwords Asked for During U.S. Interviews*, HUFFINGTON POST BUS. (Mar. 20, 2012), http://www.huffingtonpost.com/2012/03/20/facebook-passwords-job-seekers_n_1366577.html (on file with the *McGeorge Law Review*).

media accounts, "friend"[8] management, or observe as other individuals navigate their personal web pages.[9] It is unclear how widespread this information-gathering tactic is among private employers or among public employers hiring for positions not already subject to background checks and psychological evaluations.[10] Nonetheless, by August 2012, Congress and many state legislatures, including California's, introduced laws prohibiting employer access to online information intended for friends only.[11]

The United States and California constitutions, as well as federal and state statutes, may already prohibit employers from requesting access to an individual's private online social network.[12] However, according to Chapter 618 author, Assembly Member Nora Campos, as of 2012, "privacy laws have yet to be applied in any meaningful way to employers in the social media context."[13] She introduced Chapter 618 as "a preemptive measure that will provide

8. Facebook recommends sending "friend" requests to people a user "know[s] personally" and has "a real-life connection to." *FAQ: Adding Friends & Friend Requests*, FACEBOOK, https://www.facebook.com/help/friends/requests (select the "Who should I send friend requests to?" hyperlink) (last visited Oct. 26, 2012) (on file with the *McGeorge Law Review*). A User can control whether the specific content on his or her page is accessible to the public or invited "friends" only. *When I Share Something, How Do I Choose Who Can See It?*, FACEBOOK, https://www.facebook.com/help/?faq=120939471321735 (last visited Oct. 26, 2012) (on file with the *McGeorge Law Review*).

9. Valdes & McFarland, *supra* note 7; *see also* Mike Wehner, *Could Employers Begin Asking for Facebook Passwords on Applications? Job Seekers Asked to Throw Their Privacy out the Window*, TECCA (Nov. 30, 2011), http://www.tecca.com/news/2011/11/30/facebook-password-jobs (on file with the *McGeorge Law Review*) (featuring a "snapshot of an application from North Carolina for a clerical position at a police department" that required the applicant to disclose social media account information).

10. *See* Matthew Kauffman, *Claim Check: Employers Asking for Facebook Passwords*, SCOOP (Mar. 27, 2012), http://courantblogs.com/investigative-reporting/claim-check-employers-asking-for-facebook-passwords/ (on file with the *McGeorge Law Review*) (noting the lack of evidence supporting wide-spread employer requests or demands for access to personal social media).

11. Press Release, U.S. Representative Martin Heinrich, Support for Heinrich's Password Protection Act Growing (May 23, 2012) (on file with the *McGeorge Law Review*); Press Release, U.S. Senator Richard Blumenthal, Senators and Congressmen Introduce Password Protection Act of 2012 (May 9, 2012) (on file with the *McGeorge Law Review*); *Employer Access to Social Media User Names and Passwords*, NAT'L CONF. OF STATE LEGISLATORS, http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx (last visited Aug. 5, 2012) (on file with the *McGeorge Law Review*) (listing current and proposed state legislation as California, Delaware, Illinois, Maryland, Massachusetts, Michigan, Minnesota, Missouri, New Jersey, New York, Ohio, Pennsylvania, South Carolina, and Washington).

12. *Senators Question Employer Requests for Facebook Passwords*, N.Y. TIMES (Mar. 26, 2012), http://www.nytimes.com/2012/03/26/technology/senators-want-employers-facebook-password-requests-reviewed.html (on file with the *McGeorge Law Review*); ASSEMBLY COMMITTEE ON LABOR AND EMPLOYMENT, COMMITTEE ANALYSIS OF AB 1844, at 1–2 (May 2, 2012); *see also* Bob Sullivan, *Govt. Agencies, Colleges Demand Applicants' Facebook Passwords*, RED TAPE CHRONS. (Mar. 6, 2012, 6:13 AM), http://redtape.msnbc.msn.com/_news/2012/03/06/10585353-govt-agencies-colleges-demand-applicants-facebook-passwords (on file with the *McGeorge Law Review*) (reporting that, according to Washington, D.C.-based attorney Bradley Shear, "employers are violating the First Amendment with demands for access to otherwise private social media content."). *But see* Valdes & McFarland, *supra* note 7 (stating the Department of Justice does not intend to enforce the Facebook terms of service that make disclosure of a user's password a federal crime).

13. ASSEMBLY COMMITTEE ON JUDICIARY, COMMITTEE ANALYSIS OF AB 1844, at 2 (Apr. 24, 2012).

[employers] critical guidelines to the accessibility of private information behind the 'social media wall.'"[14]

II. LEGAL BACKGROUND

Prior to Chapter 618, an employee's and job applicant's social media was protected—to varying degrees—by several complex areas of law, including: (A) prohibition of discriminatory employment practices,[15] (B) free speech and employees' protected concerted activity,[16] (C) personal privacy,[17] (D) protection of electronic communications,[18] and (E) computer fraud and abuse.[19]

A. Employment Discrimination

California employers may not discriminate based on "race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, marital status, sex, gender, gender identity, gender expression, age, or sexual orientation."[20] Existing law does not require employees or job applicants to disclose information related to these protected interests, and it prohibits employers from inquiring into those interests unless the information is essential to the job performance or is otherwise "a bona fide occupational qualification."[21]

14. Press Release, Nora Campos, Assembly Member, Cal. State Assembly, Landmark Social Media Privacy Bill Clears California State Assembly on 73–0 Vote: AB 1844 Is the First Bill of Its Kind in California to Ever Address the Issue of Protecting Social Media Logins of Potential Employees (May 10, 2012) [hereinafter Press Release, Assembly Member Campos, Assembly Vote 73–0] (on file with the *McGeorge Law Review*).

15. *See infra* Part II.A (describing how an employee's personal social media may be protected by current anti-discrimination laws); *see also* ASSEMBLY COMMITTEE ON JUDICIARY, COMMITTEE ANALYSIS OF AB 1844, at 2 (Apr. 24, 2012) (noting that requiring employees to disclose the type of information often contained on personal web pages violates Section 12920 of the California Government Code ("discrimination in employment rights and opportunities and housing")).

16. *See infra* Part II.B (reviewing how an employee's social media may constitute protected concerted activity); *see also* ASSEMBLY COMMITTEE ON LABOR AND EMPLOYMENT, COMMITTEE ANALYSIS OF AB 1844, at 1–3 (May 2, 2012) (discussing an employee's "right to protected speech").

17. *See infra* Part II.C (discussing possible inadequacies in privacy law that may leave the personal information posted online unprotected); *see also* ASSEMBLY COMMITTEE ON LABOR AND EMPLOYMENT, COMMITTEE ANALYSIS OF AB 1844, at 1–3 (May 2, 2012) (reviewing the lack of meaningful privacy policies regarding social media).

18. *See infra* Part II.D (characterizing the Stored Communications Act as too antiquated to deal meaningfully with social media); *see also* ASSEMBLY COMMITTEE ON LABOR AND EMPLOYMENT, COMMITTEE ANALYSIS OF AB 1844, at 1–3 (May 2, 2012) (positing shortcomings of the Electronic Communications Act and the Stored Communications Act).

19. *See infra* Part II.E (explaining breach of a websites privacy statement may be a violation of federal law); *see also* ASSEMBLY COMMITTEE ON LABOR AND EMPLOYMENT, COMMITTEE ANALYSIS OF AB 1844, at 1–3 (May 2, 2012) (examining Facebook's privacy statement).

20. CAL. GOV'T CODE § 12940 (West 2011).

21. CAL. DEP'T OF FAIR EMP'T & HOUSING FACT SHEET, DFEH-161, EMPLOYMENT INQUIRIES: WHAT CAN EMPLOYERS ASK APPLICANTS AND EMPLOYEES? (Aug. 2001), *available at* http://www.dfeh.ca.gov/res/

Individuals often share such personal information with friends and family on social media websites.[22] Employment conditioned on an employer's access to one's online social media is likely a violation of state anti-discrimination laws.[23]

Existing state law also protects whistleblowers against retaliatory harassment and adverse employment actions.[24] California law requires employers and the California Department of Industrial Relations to investigate workplace discrimination and harassment allegations.[25] Such investigations may necessitate employer access to private information posted on personal web pages.[26]

B. National Labor Relations Act

Employers routinely define policy regarding the use and access to electronic equipment they own.[27] However, the National Labor Relations Act (NLRA) prohibits employers from hampering workers' participation in "concerted

docs/publications/dfeh-161.pdf [hereinafter DFEH-161] (on file with the *McGeorge Law Review*); *see also* Dothard v. Rawlinson, 433 U.S. 321, 332–34 (1976) (examining the boundaries of the "bona fide occupational qualification" exception).

22. Press Release, Nora Campos, Assembly Member, Cal. State Assembly, Social Media Privacy Bill Receives Unanimous Support: AB 1844, Which Protects Social Media Users' Privacy Rights, A Step Closer to Becoming Law (Apr. 24, 2012) [hereinafter Press Release, Assembly Member Campos, Bill Receives Unanimous Support] (on file with the *McGeorge Law Review*); *Maryland Passes Nation's First Social Media Privacy Protection Bill*, ACLU BLOG OF RIGHTS (May 4, 2012), https://www.aclu.org/blog/technology-and-liberty/maryland-passes-nations-first-social-media-privacy-protection-bill (on file with the *McGeorge Law Review*); Press Release, U.S. Senator Richard Blumenthal, *supra* note 11.

23. *See* GOV'T § 12940(d) (prohibiting "non-job related inquir[ies] . . . that express, directly or indirectly, any limitation, specification, or discrimination as to" any of the enumerated unlawful bases); DFEH-161, *supra* note 21 (cautioning employers: "inquiries that, directly or indirectly, identify an individual on a basis enumerated in the [California Fair Employment and Housing] Act are unlawful").

24. GOV'T § 12940(h).

25. Lyne A. Richardson, & Jolina A. Abrena, *10 Ways to Comply with California's Harassment, Discrimination Law*, 20 CAL. EMP. L. LETTER 3 (2010). Employees may file a discrimination complaint with the California Department of Industrial Relations. *Retaliation and Discrimination Complaints: A Summary of Procedures*, CAL. DEP'T INDUS. REL, http://www.dir.ca.gov/dlse/DiscriminationComplaintProcedure.htm (last visited Sept. 23, 2012) (on file with the *McGeorge Law Review*). Timely complaints must be investigated. *Id.* The California Labor Commissioner is required to determine if a violation has occurred based on a summary of the investigation conducted or after a full hearing. *Id.*

26. ENFORCEMENT GUIDANCE: VICARIOUS EMPLOYER LIABILITY FOR UNLAWFUL HARASSMENT BY SUPERVISORS, U.S. EQUAL EMP'T OPPORTUNITY COMM'N. (June 18, 1999), *available at* http://www.eeoc.gov/policy/docs/harassment.html (on file with the *McGeorge Law Review*); *see* SENATE COMMITTEE ON LABOR AND INDUSTRIAL RELATIONS, COMMITTEE ANALYSIS OF SB 1349, at 4 (Apr. 25, 2012) (analyzing SB 1349, proposed regulation related to AB 1844). "The use of social media has also created another avenue for an employee to be potentially harassed . . . the employee is now able to post harassing messages to a co-worker's social media page during off-work hours." *Id.*

27. *See* Holmes v. Petrovich Dev. Co., 191 Cal. App. 4th 1047, 1050–52, 1071, 119 Cal. Rptr. 3d 878, 883, 898 (3d Dist. 2011) (finding e-mail communication between client and attorney is not privileged when sent on a company computer governed by a clearly stated company policy of monitoring e-mail). *See generally* Matthew J. Norris, *Courts Limit the Privacy Rights of Public and Private Employees*, 34 L.A. LAW. 16, 19 (2011) (discussing best policy practices for employers regarding employee electronic media privacy rights).

activities," such as union organizing.[28] In 2011, the National Labor Relations Board (NLRB) advised a California company that firing an employee who posted negative comments regarding employment conditions on his personal Facebook page violates the NLRA because the posts represent a "continuation of earlier discussions with coworkers that contemplated group action regarding terms and conditions of employment."[29] Yet, not all online comments related to office or employment conditions constitute concerted activity.[30] In 2009, a California hospital disciplined three of its employees for posting Facebook comments implying they "might not provide appropriate care to the [e]mployer's patients."[31] Although the employees' comments were interspersed with protected speech, the NLRB determined that the hospital's disciplinary actions did not violate the NLRA.[32]

C. Constitutional and Common Law Privacy Claims

To recover for an alleged violation of privacy under the Fourth Amendment of the U.S. Constitution,[33] a public employee must show that a government employer infringed upon "an expectation of privacy that society is prepared to consider reasonable."[34] California law allows individuals to recover from both

28. 29 U.S.C. § 157 (2006) (describing concerted activities as "the right to self-organization, to form, join, or assist labor organizations, to bargain collectively . . . and [other] . . . activities for the purpose of collective bargaining"). California law also provides that employers may neither restrict nor discriminate based on an employee's legal online conduct outside of work hours using personal equipment. CAL. LAB. CODE §§ 96, 98.6(k) (West 2011).

29. Advice Memorandum Re: Marco Transp., No. 27-CA-21850 from Barry J. Kearney, Assoc. Gen. Counsel, NLRB to Wanda P. Jones, Reg'l Dir., Region 27, at 1 (Aug. 31, 2011), *available at* http://www.nlrb.gov/case/27-CA-021850 [hereinafter NLRB Advice Memo Re: Marco Transp.] (on file with the *McGeorge Law Review*). The statements in this letter are consistent with previous board holdings that "an employer's discipline of an employee based on website statements relating to terms or conditions of employment and/or a labor dispute is unlawful." Advice Memorandum Re: MONOC, No. 22-CA-029008 from Barry J. Kearney, Assoc. Gen. Counsel, NLRB to J. Michael Lightner, Reg'l Dir., Region 22, at 7 (May 5, 2010), *available at* http://www.nlrb.gov/case/22-CA-029008 [hereinafter NLRB Advice Memo Re: MONOC] (on file with the *McGeorge Law Review*) (citing Valley Hosp. Med. Ctr., 351 NLRB 1250, 1252–54 (2007)); *see* 29 U.S.C. § 158(a)(1) (making the "interference with, restrain, or coerc[ion of] employees" rights granted under 29 U.S.C. § 157 an "unfair labor practice").

30. *See, e.g.*, NLRB Advice Memo Re: MONOC, *supra* note 29, at 5 (differentiating between posted related to union activities and those unrelated); Advice Memorandum Re: Buel, Inc., No. 11-CA-022936 from Barry J. Kearney, Assoc. Gen. Counsel, NLRB to Jane North, Reg'l Dir., Region 11, at 3 (July 28, 2010), *available at* http://www.nlrb.gov/case/11-CA-022936 [hereinafter NLRB Advice Memo Re: Buel, Inc.] (on file with the *McGeorge Law Review*) (finding employee's personal gripes posted on Facebook to employer "friends" did not constitute concerted activity).

31. NLRB Advice Memo Re: MONOC, *supra* note 29, at 8.

32. *Id.* The Board also stated that restricting access to one's friends does not preclude an employer from legally obtaining private posts through voluntary disclosure by co-workers. *Id.*

33. U.S. CONST. amend. IV (securing "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures").

34. O'Conner v. Ortega, 480 U.S. 709, 715 (1987) (plurality opinion) (quoting United States v.

public and private employers for a breach of privacy under the state constitution and the common law torts of invasion and intrusion of privacy.[35] These actions, however, also require the plaintiff to prove a reasonable expectation of privacy.[36] Like other published information, posts appearing in a public Internet forum carry no expectation of privacy.[37] Whether current law protects personal content on a website governed by privacy policies with restrictive access settings is more ambiguous.[38]

In *City of Ontario v. Quon*, the United States Supreme Court declined to rule specifically regarding an employee's expectation of privacy when using an employer's electronic equipment.[39] The Court expressed concern over setting precedent in this rapidly evolving area of technology because society has yet to define its expectation of privacy.[40] However, the Court unanimously held that auditing an employee's personal text messages sent during employment hours on a city-provided pager did not violate an employee's privacy.[41] The city justified its review of the texts' actual content on grounds of a "legitimate work-related purpose" that "was not excessive in scope."[42]

Jacobsen, 466 U.S. 109, 113 (1984)) (internal quotation marks omitted). "Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer. . . . Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." *Id.* at 718–19.

35. Hernandez v. Hillside, Inc., 47 Cal. 4th 272, 277, 286, 211 P.3d 1063, 1066, 1073 (2009) (examining plaintiff's claim of "intrusion into a protected zone of privacy" under both California Constitution and common law); Richards v. Cnty of L.A., 775 F. Supp. 2d 1176, 1185 (C.D. Cal. 2011) (discussing the possibility of a valid claim for intrusion, if a private California employer was the defendant). *See generally* Mark W. Robertson & Mark A. Kanaga, *Office Watch: Employers Who Monitor Computer Use Must Take into Account Their Employees' Reasonable Expectations of Privacy*, 31 L.A. LAW. 29, 30 (2008) (deducing the state constitution's creation of "a private right of action against private parties" is applicable to private employers).

36. *Hernandez*, 47 Cal. 4th at 277, 278, 211 P.3d at 1066, 1073; *Richards*, 775 F. Supp. 2d at 1185.

37. Moreno v. Hanford Sentinel, Inc., 172 Cal. App. 4th 1125, 1130, 91 Cal. Rptr. 3d 858, 862–63 (5th Dist. 2009) (asserting that the act of posting information on myspace.com made it "available to any person with a computer and thus opened it to the public eye. Under these circumstances, no reasonable person would have had an expectation of privacy. . . ."); *see also* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1210 (2004) (discussing the Supreme Court's holdings regarding information revealed to third parties); ASSEMBLY COMMITTEE ON JUDICIARY, COMMITTEE ANALYSIS OF AB 1844, at 2 (Apr. 24, 2012) ("[E]mployers can access all public aspects of a prospective employee's social media accounts. . . . The burden remains on the individual social media user to limit access . . . .").

38. Steven D. Zansberg & Janna K. Fischer, *Privacy Expectations in Online Social Media—An Emerging Generational Divide?*, 28 COMM. LAW. 1, 26 (2011); ASSEMBLY COMMITTEE ON JUDICIARY, COMMITTEE ANALYSIS OF AB 1844, at 2 (Apr. 24, 2012) ("[P]rivacy laws have yet to be applied in any meaningful fashion to employers in the social media context. . . .").

39. 130 S. Ct. 2619, 2630 (2010) ("A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds.").

40. *Id.* at 2629 ("[C]hanges in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.").

41. *Id.* at 2633; *id.* at 2634 (Scalia, J., concurring).

42. *Id.* at 2632–33 (reasoning an audit of content to ascertain the sufficiency of the minutes on an

D. The Stored Communications Act

Few cases deal specifically with the right of an employer to access an employee's "private" social media.[43] In its 2002 decision in *Konop v. Hawaiian Airlines, Inc.*,[44] the Ninth Circuit Court of Appeals held an employer's unauthorized access to an employee's password-protected website that required agreement with the site's terms and conditions prior to use did not violate the Stored Communications Act (SCA)[45]—under which it is an offense to "accesses without authorization a facility through which an electronic communication service is provided."[46] The court analyzed at great length the differences between "electronic" and "wire" forms of communication, as well as between the acts of "intercepting" and "accessing" communication.[47] Ultimately, its decision turned on the plain meaning of the word "user" in the statute, a term now ubiquitously understood to designate the person logging on to view a website.[48] The court referred to the statute containing the provisions of the SCA as "complex" and "often convoluted," and "observ[ed] that until Congress brings the laws in line with modern technology, protection of the Internet and websites . . . will remain a confusing and uncertain area of the law."[49]

E. Computer Fraud and Abuse Act

Under the federal Computer Fraud and Abuse Act (CFAA), users may not "exceed[] authorized access" in an effort to "obtain information from a protected

employee texting plan is not an invasion of privacy).

43. Zansberg & Fischer, *supra* note 38, at 27.

44. 302 F.3d 868 (9th Cir. 2002) (adjudicating an employer's potentially illegal access to an employee's personal online site before construction of today's sophisticated social media sites using law created prior to development of the Internet).

45. 18 U.S.C. §§ 2701–11 (2006).

46. *Id.* § 2701; *Konop*, 302 F.3d at 880.

47. *Konop*, 302 F.3d at 874–80. "[T]he term 'wire communication' was defined to include storage of the communication, while 'electronic communication' was not. The court concluded that this textual difference evidenced Congress' understanding that, although one could 'intercept' a *wire* communication, one could not 'intercept' an *electronic* communication in storage . . . ." *Id.* at 877 (referencing the Fifth Circuit's 1994 holding in *Jackson Games Inc. v. U.S. Secret Service*, 36 F.3d 457).

48. *Id.* at 880 ("Based on the common definition of the word 'use,' we cannot find any evidence in the record that Wong ever used Konop's website"). *See generally* Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979, 999–1000 (2011) (discussing the complexity of SCA interpretation and its relation to the court's holding in *Konop*).

49. *Konop*, 302 F.3d at 874. *See generally* Kerr, *supra* note 37 (providing an overview of the SCA and analyzing how it could be updated to protect information on the Internet); Junichi P. Semitsu, *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, 31 PACE L. REV. 291 (2011) (suggesting modification to the Electronic Communication Privacy Act [which contains the SCA] is necessary to protect information posted online).

computer."[50] Consequently, both parties involved in transferring a private username or password—from an employee or job applicant to employer—may be violating federal law.[51] In 1984, Congress enacted the CFAA to protect government computers from hackers.[52] Today, some courts apply the statute in some cases involving claims against disloyal employees who misappropriated confidential information in violation of company policies or statutory provisions such as trade secrecy.[53]

The Ninth Circuit Court of Appeals rejected this broad interpretation of the CFAA in 2012 because the statute "makes every violation of a private computer use policy a federal crime."[54] Social media and other online service providers require users to agree to specific terms of service.[55] Facebook, for example, forbids users from disclosing their passwords to any third party.[56] In some jurisdictions, an employee can be criminally prosecuted for violating federal law by exceeding his or her authority when providing an employer access to his or her social media.[57] The Supreme Court has yet to resolve this split of authority.[58]

III. CHAPTER 618

Chapter 618 provides clarification regarding protection for "social media"[59] posted by employees and job applicants on their personal networks,[60] but the law

50. 18 U.S.C. § 1030; United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (interpreting the meaning of "exceeds authorized access" under the CFAA). *See generally* Thomas E. Booms, Note, *Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act*, 13 VAND. J. ENT. & TECH. L. 543, 549 (2011) (discussing 1996 Congressional changes to the FCAA and defining "protected computer").

51. *Nosal*, 676 F.3d at 861; Jacob Sullum*, From Hackers to Slackers: How a Federal Law Can Be Used to Prosecute Almost Anyone Who Uses a Computer*, REASON.COM (Apr. 18, 2012), http://reason.com/archives/2012/04/18/from-hackers-to-slackers (on file with the *McGeorge Law Review*).

52. Booms, *supra* note 50, at 548.

53. *Id.* at 557–67 (summarizing the "broad view" court split).

54. *Nosal*, 676 F.3d at 859.

55. *Id.* at 861; Sullum*, supra* note 51.

56. *Nosal*, 676 F.3d at 861; ASSEMBLY COMMITTEE ON LABOR AND EMPLOYMENT, COMMITTEE ANALYSIS OF AB 1844, at 3 (May 2, 2012); Erin Egan, *Protecting Your Passwords and Your Privacy*, FACEBOOK (Mar. 23, 2012, 5:32 AM), https://www.facebook.com/notes/facebook-and-privacy/protecting-your-passwords-and-your-privacy/326598317390057 (on file with the *McGeorge Law Review*).

57. *Nosal*, 676 F.3d at 859 ("Take the case of the mom who posed as a 17-year-old boy and cyber-bullied her daughter's classmate. The Justice Department prosecuted her under 18 U.S.C. § 1030(a)(2)(C) [CFAA] for violating MySpace's terms of service . . . ."); *see also* Sullum*, supra* note 51 (discussing *United States v. Nosal* and possible future applications of CFAA).

58. Booms, *supra* note 50, at 563–70.

59. CAL. LAB. CODE § 980(a) (enacted by Chapter 618) (defining "social media" as "an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, e-mail, online services or accounts, or Internet Web site profiles or locations").

60. *Id.*

does not grant any "private right of action."[61] Chapter 618 specifically bars California employers from "requir[ing] or request[ing]" an employee or applicant provide his or her username, password, or access to private information posted online.[62] The legislation protects employees and job applicants from termination or disciplinary action for refusing to provide access to social media.[63] However, employers explicitly retain the right to demand access to any equipment provided for employee use, investigate allegations of work-related misconduct, and discharge or discipline employees for all legal reasons.[64] Section 2 of Chapter 618 makes clear the legislative intent to relieve the Labor Commissioner from any requirement to investigate or make determinations regarding alleged violations of the new law.[65]

IV. ANALYSIS

According to Assembly Member Nora Campos, when she introduced Chapter 618, there were "129 cases from across the nation before the National Labor Relations Board in which employer workplace policies around social media [were] being scrutinized."[66] The new law is intended to provide clarification and guidance to California employers by (A) clearly defining social media,[67] (B) prohibiting access to an employee's or applicant's personal online content,[68] (C) protecting concerted employee activities taking place in online forums,[69] (D) arguably setting California's "expectation of privacy" regarding

61. 2012 Cal. Stat. ch. 618, § 2; Philip L. Gordon, *California (Surprisingly) Becomes First State to Take a More Balanced Approach to Social Media "Password Protection" Laws*, WORKPLACE PRIVACY COUNSEL (Sept. 5, 2012), http://privacyblog.littler.com/2012/09/articles/state-privacy-legislation/california-surprisingly-becomes-first-state-to-take-a-more-balanced-approach-to-social-media-password-protection-laws/ (on file with the *McGeorge Law Review*).

62. LAB. § 980(b) (enacted by Chapter 618).

63. *Id.* § 980(e) (enacted by Chapter 618).

64. *Id.* § 980(c)–(e) (enacted by Chapter 618).

65. 2012 Cal. Stat. ch. 618, § 2.

66. Press Release, Assembly Member Campos, Assembly Vote 73–0, *supra* note 14.

67. LAB. § 980(a) (enacted by Chapter 618) (defining "social media" as "an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, e-mail, online services or accounts, or Internet Web site profiles or locations."); *see also infra* Part IV.A (specifying the updated definition of social media).

68. LAB. § 980(b) (enacted by Chapter 618); SENATE RULES COMMITTEE, COMMITTEE ANALYSIS OF AB 1844, at 5 (July 2, 2012); *see also infra* Part IV.B (postulating one intended effect of prohibiting employer access to private social media is to guard against potential discriminatory employment practices).

69. *See* LAB. § 980 (enacted by Chapter 618) (explicitly applying current law in the social media context); SENATE RULES COMMITTEE, COMMITTEE ANALYSIS OF AB 1844, at 5 (July 2, 2012) (asserting that this legislation augments current law protecting free speech and political activity so that it explicitly includes exercising these rights via social media); *see also infra* Part IV.C (indicating Chapter 618 is consistent with the NLRB's opinion that and employee's online concerted activity is protected).

social media,[70] and (E) encouraging the separation of personal and business use of social media accounts.[71]

A. What Constitutes Social Media?

Chapter 618 avoids the complexity associated with the SCA by defining social media as "an electronic service or account, or electronic content," and not in terms of "wire or electronic communication."[72] It further simplifies social media classification by including a non-exhaustive, illustrative list of examples.[73] Although this definition of social media does not specifically address the CFAA, it reduces the likelihood that unauthorized access to protected equipment will lead to litigation by limiting an employer's ability to request disclosure of passwords.[74] Unfortunately, because of rapidly advancing technologies, courts applying Chapter 618 in the future may encounter difficulties similar to those encountered by modern courts when applying outdated SCA definitions to sites on the World Wide Web.[75]

B. Is Publicly Posted "Personal" Information Protected Social Media?

Many human resources managers and employment recruiters use the Internet to screen job candidates.[76] Due to the recent proliferation of applications designed

70. *See* LAB. § 980 (enacted by Chapter 618) (establishing an employee's expectation of privacy in personal social media passwords); SENATE RULES COMMITTEE, COMMITTEE ANALYSIS OF AB 1844, at 9 (July 2, 2012) ("[T]his is a common sense measure that ensures a level of privacy for employees and prospective employee's social media accounts"); *see also infra* Part IV.D (discussing the plausible impact of Chapter 618 on employee privacy rights in California).

71. SENATE COMMITTEE ON LABOR AND INDUSTRIAL RELATIONS, COMMITTEE ANALYSIS OF AB 1844, at 6 (June 27, 2012); *see also infra* Part IV.E (suggesting that the intended separation of business and personal social media may negatively affect the revenue of some social media forum providers).

72. LAB. § 980(a) (enacted by Chapter 618); *see also supra* Part II.D (explaining how courts have interpreted the vague language of the SCA).

73. LAB. § 980(a) (enacted by Chapter 618) (listing "videos, still photographs, blogs, video blogs, podcasts, instant and text messages, e-mail, online services or accounts, or Internet Web site profiles or locations" as examples of social media).

74. *Id.* § 980(b)(1) (enacted by Chapter 618). *See generally* United States v. Nosal, 676 F.3d 854, 861 (9th Cir. 2012) (scrutinizing possible interpretations of CFAA language and its application by the courts).

75. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874–80 (9th Cir. 2002).

76. David Burt, *Microsoft Releases a Study on Data Privacy Day*, MICROSOFT PRIVACY & SAFETY (Jan. 26, 2010, 9:40 AM), http://blogs.technet.com/b/privacyimperative/archive/2010/01/27/microsoft-releases-a-study-on-data-privacy-day.aspx (on file with the *McGeorge Law Review*) (revealing results of a 2010 study completed by Microsoft that found seventy percent of human resources professionals did not extend job offers to specific candidates because of material posted on the Internet); Press Release, CareerBuilder.com, Thirty-Seven Percent of Companies Use Social Networks to Research Potential Job Candidates, According to New CareerBuilder Survey (Apr. 18, 2012), *available at* http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr691&sd=4%2f18%2f2012&ed=4%2f18%2f2099 (on file with the *McGeorge Law Review*).

to gather information posted by, or associated with, an individual, the number of employers who review an applicant's or employee's social media content as part of a background check may be on the rise.[77] Sponsors of Chapter 618 intend the legislation to reduce the probability of discrimination by limiting employer access to personal information that is not associated with an individual's "job-related function."[78]

Chapter 618 prohibits an employer from requesting or requiring an employee to "[d]ivulge any *personal* social media."[79] Whether the legislation protects publicly posted social media is unclear.[80] Currently, companies such as Social Intelligence scour the Internet for *publicly* available information and provide employers sanitized profiles, devoid of any specific reference to legally protected information such as race, age, or gender.[81] Employees must agree to the background check and employers treat the private information provided similarly to that of a credit agency rating report.[82] It is uncertain whether Chapter 618 makes this type of background check illegal because the aggregation is based on openly published, not privately restricted, information.[83]

77. *See* Bob Sullivan, *When It Comes to Online Reputation, 'Life's Not Fair, and Companies Aren't Either'*, RED TAPE CHRONS. (Sept. 30, 2011, 8:59 AM), http://redtape.msnbc.msn.com/_news/2011/09/29/8044153-when-it-comes-to-online-reputation-lifes-not-fair-and-companies-arent-either?GT1=43007 (on file with the *McGeorge Law Review*) (discussing Social Intelligence, an online information aggregation application); Joshua Brustein, *Keeping a Close Eye on Employees' Social Networking*, N.Y. TIMES BITS BLOG (Mar. 26, 2010, 6:15 PM), http://bits.blogs.nytimes.com/2010/03/26/keeping-a-closer-eye-on-workers-social-networking/ (on file with the *McGeorge Law Review*) (discussing Teneros and Social Sentry social media monitoring applications); Valdes & McFarland, *supra* note 7 (discussing BeKnown, a third party application that reviews public social media profiles).

78. *See* Press Release, Assembly Member Campos, Bill Receives Unanimous Support, *supra* note 22 ("Our social media accounts offer views into our personal lives and expose information that would be inappropriate to discuss during a job interview due to the inherent risk of creating biases in the minds of employers."); *see also* Press Release, CareerBuilder.com, *supra* note 76 ("[H]iring managers and human resources departments have to make a careful, determined decision as to whether information found online is relevant to the candidates' qualifications for the job.").

79. CAL. LAB. CODE § 980(b)(3) (enacted by Chapter 618) (emphasis added).

80. *See* Moreno v. Hanford Sentinel, Inc., 172 Cal. App. 4th 1125, 1130, 91 Cal. Rptr. 3d 858, 862–63 (5th Dist. 2009) (discussing the unreasonableness of an expectation of privacy related to information posted on myspace.com); *see also* Kerr, *supra* note 37, at 1210 (discussing the Supreme Court's holdings regarding information revealed to third parties); Zansberg & Fischer, *supra* note 38, at 25–26, 31 n.8 (stating that what one "knowingly *exposes to the public*" is not protected information); ASSEMBLY COMMITTEE ON JUDICIARY, COMMITTEE ANALYSIS OF AB 1844, at 3 (Apr. 24, 2012) (noting an employer may still access publicly available information and placing "[t]he burden . . . on the individual social media user to limit access").

81. *Social Intelligence Hiring*, SOCIAL INTELLIGENCE, http://www.socialintel.com/social-media-employment-screening/ (last visited July 18, 2012) (on file with the *McGeorge Law Review*).

82. *FAQ: Is Social Intelligence a Consumer Reporting Agency?*, SOCIAL INTELLIGENCE, http://www.socialintel.com/faqs/#emp-1 (from homepage, select FAQ, click on Employment FAQs) (last visited Aug. 5, 2012) (on file with the *McGeorge Law Review*); *see also* Anita Ramasastry, *Cyber-Screening, Social Media, and Fair Credit Reporting: Why We Need to Move Beyond the FTC's Recent Spokeo Enforcement Action*, VERDICT (July 17, 2012), http://verdict.justia.com/2012/07/17/cyber-screening-social-media-and-fair-credit-reporting (on file with the *McGeorge Law Review*) (discussing Federal Trade Commission (FTC) oversight of companies providing social media based employee background checks).

83. *FAQ: Do You Find Profile Information on Social Networks? If the Profile Is Private Does This*

C. Is a Chat Between Friends on Facebook Concerted Activity?

The NLRB has signified that a conversation regarding organizing or collectively pursuing modification of employment terms or conditions is protected activity even if it takes place online.[84] Employers may not discipline, discriminate against, or terminate employees based on a personal post or an exchange of posts between coworkers that discusses such concerted activity.[85] Chapter 618 protects against intrusion into such activities by restricting an employer's ability to request access to password-protected websites where employees can conveniently rally.[86]

D. Is Employer Access to Restricted Webpages an Invasion of Privacy?

Prior to Chapter 618, it was unclear whether an employer's request for access to an employee's or applicant's social media—either through acquisition of usernames and passwords or by viewing pages in the individual's presence—was an invasion of privacy.[87] The courts will likely interpret Chapter 618 as establishing California employees' reasonable expectation of privacy in their social media without disturbing the Supreme Court's allowance of access under "legitimate work-related purposes."[88] While Chapter 618 does not affect an employer's right to operational control over employer-owned equipment and the ability to investigate misconduct, it makes clear that an employer may not generally request disclosure of information posted on password-protected personal websites.[89]

Violate the Individuals Privacy?, SOCIAL INTELLIGENCE, http://www.socialintel.com/faqs/#do-you-find-profile-information-on-social-networks-if-the-profile-is-private-does-this-violate-the-individuals-privacy (from homepage, select FAQ) (last visited Aug. 5, 2012) (on file with the *McGeorge Law Review*); *see also* Ramasatry, *supra* note 82 (indicating at least one FTC approved company gathers most of its data not from typical social media sites, but from "blogs and posts on smaller social sites, and even on Craigslist").

84. NLRB Advice Memo Re: Marco Transp., *supra* note 29.

85. 29 U.S.C. § 157 (2006); *see also* NLRB Advice Memo Re: Marco Transp., *supra* note 29, at 2 ("That the Facebook activity encouraged the Charging Party's co-worker to confront the Employer about the employees' shared concerns demonstrates that the postings were more than mere gripping, but rather an activity that induced group action.").

86. CAL. LAB. CODE § 980 (enacted by Chapter 618).

87. Zansberg & Fischer, *supra* note 38, at 26; ASSEMBLY COMMITTEE ON JUDICIARY, COMMITTEE ANALYSIS OF AB 1844, at 2 (Apr. 24, 2012).

88. LAB. § 980(b)–(e) (enacted by Chapter 618); *see also* O'Conner v. Ortega, 480 U.S. 720, 715 (1987) (plurality opinion) ("In the case of searches conducted by a public employer, we must balance the invasion of the employees' legitimate expectation of privacy against the government's need for supervision, control, and the efficient operation of the workplace."); Holmes v. Petrovich Dev. Co., 191 Cal. App. 4th 1047, 1051–52, 119 Cal. Rptr. 3d 878, 883, 898 (3d Dist. 2011) (holding plaintiff had no expectation of privacy of email contents sent to attorney over private employer's computer system due to the company's policy regarding email monitoring); Norris, *supra* note 27, at 18 (discussing employee's inability to recover for invasion of privacy under California law when an employer has a clear policy of computer monitoring).

89. LAB. § 980 (enacted by Chapter 618).

E. Will Social Media Service Providers Be Impacted by Chapter 618?

Only the Securities Industry and Financial Markets Association (SIFMA) argued openly in opposition to Chapter 618.[90] SIFMA argues that Chapter 618 forces securities firms to violate Financial Industry Regulatory Authority (FINRA) regulations that require companies to monitor all employee communications with customers, even those posted to social media sites.[91] The Senate determined that FIRNA recommends "employers avoid this problem altogether by expressly prohibiting employees from using personal accounts for business purposes."[92] Thus, the legislature intended Chapter 618, in part, to reinforce the separation between "business use" and "personal use" of social media.[93] This could negatively affect advertising revenue streams generated by social media providers.[94]

V. CONCLUSION

Chapter 618 imposes civil liability upon California employers that require access to personal usernames, passwords, or private social media as part of their hiring, promotion, or employee-review process.[95] However, the legal effect of Chapter 618 remains uncertain in two regards: employer use of third-party social media rating systems to review publicly available content[96] and employer leveraging of employee personal media for customer development.[97] Employees

90. SENATE RULES COMMITTEE, COMMITTEE ANALYSIS OF AB 1844, at 8 (July 2, 2012).

91. *Id.* at 9.

92. SENATE COMMITTEE ON LABOR AND INDUSTRIAL RELATIONS, COMMITTEE ANALYSIS OF AB 1844, at 6 (June 27, 2012).

93. *Id.* (acknowledging that FINRA does require monitoring of any employee personal social media used for business and finding that securities firms should adopt the recommended stance of not allowing personal social media use for business purposes).

94. Complete separation of business and personal social networking may hamper the common marketing technique of developing a "personal relationship" with customers through social media. See generally the recommended marketing tactics using social media by the U.S. Small Business Administration (search "http://www.sba.gov/" for "social media") (last visited Oct. 9, 2012) (posting articles related to "getting started with social media marketing" and making "social media pay off").

95. CAL. LAB. CODE § 980(b)(3) (enacted by Chapter 618) (stating an employee need not "[d]ivulge any *personal* social media" (emphasis added)).

96 Moreno v. Hanford Sentinel, Inc., 172 Cal. App. 4th 1125, 1130, 91 Cal. Rptr. 3d 858, 862–63 (5th Dist. 2009); *see also* Kerr, *supra* note 37, at 1210 (discussing the Supreme Court's holdings regarding information revealed to third parties); Zansberg & Fischer, *supra* note 38, at 25–26, 31 n.8 (reiterating information exposed to public viewing is no longer protected information); ASSEMBLY COMMITTEE ON JUDICIARY, COMMITTEE ANALYSIS OF AB 1844, at 3 (Apr. 24, 2012) (discussing employers' ability to access publicly available information through third parties).

97. SENATE COMMITTEE ON LABOR AND INDUSTRIAL RELATIONS, COMMITTEE ANALYSIS OF AB 1844, at 6 (June 27, 2012) (recommending companies adopt the stance of not allowing personal social media use for business purposes).

should continue to be mindful of posting personal information online and of their employer's social media policies.[98]

Chapter 618 does not require the California Department of Industrial Relations or the Labor Commissioner to investigate any alleged violations of this law, nor does it specifically grant any "private right of action."[99] While it remains unclear how many employers have actually requested or mandated access to usernames or passwords,[100] Chapter 618 provides important clarification for both employers and employees in light of rapidly evolving technology and the pervasiveness of social media in the workplace.

98. *See generally* Norris, *supra* note 27, at 16 ("Employees should be very wary of engaging in any activity at work that they do not want their employer to discover and should assume that all workplace communications [conducted on employer owned equipment] may be monitored, especially if the employer has announced this policy."); Sullivan, *supra* note 77 ("[A] single moment of bad judgment . . . can live forever in friends' Facebook posts or tweets.").

99. 2012 Cal. Stat. ch. 618, § 2; Gordon, *supra* note 61.

100. *See* Kauffman, *supra* note 10 (investigating claims regarding employer use of private social media during hiring process)