Northern Kentucky Law Review is published three times during the academic year by students of Salmon P. Chase College of Law, Northern Kentucky University, Highland Heights, Kentucky 41099. Telephone: 859/572-5444. Facsimile: 859/572-6159. Member, National Conference of Law Reviews. All sections which appear in this issue are indexed by the H.W. Wilson Company in its Index to Legal Periodicals. Northern Kentucky Law Review articles are also available on microfilm and microfiche through University Microfilms International, Ann Arbor, Michigan.

Subscription rates are $35.00 per volume, $10.00 per individual issue. If a subscriber wishes to discontinue a subscription at its expiration, notice to that effect should be sent to the Northern Kentucky Law Review office. Otherwise, it will be assumed that renewal of the subscription is desired.

Please send all manuscripts to the address given above. No manuscript will be returned unless return is specifically requested by the author.
SALMON P. CHASE COLLEGE OF LAW

DENNIS HONABACH, A.B., J.D.
Dean & Professor of Law

LAWRENCE ROSENTHAL, B.A., J.D., L.L.M.
Associate Dean for Academics

JENNY YOUNG,
Registrar of the College of Law

LISA MOORE, B.A., J.D.
Director of Career Services

MOLLY TAM, B.A., J.D.
Associate Dean for Student Affairs and Admissions & Director of Pro Bono Services

ASHLEY GRAY, B.A., J.D.
Director of Admissions

KAREN OGBURN, B.A., M.P.A.
Associate Dean for Administration

SHERRIE TURNER, B.S., M.P.A.
Budget Analyst

DAVID H. MACKNIGHT, B.S., J.D.
Associate Dean for Law School Advancement

MICHAEL WHITEMAN, B.A., M.S.L.S., J.D.
Associate Dean for Library Services and Information Technology & Professor of Law

FACULTY

ERIC ALDEN, B.A., M.A., J.D.
Co-Director of the Transactional Law Practice Center & Assistant Professor of Law

RICHARD A. BALES, B.A., J.D.
Director, Center for Excellence in Advocacy & Professor of Law

DONNA S. BENNETT, A.B., M.A., M.S.L.S.
Professor of Library Services & Assistant Director for User Services

JOHN M. BICKERS, A.B., J.D., L.L.M.
Professor of Law

ROGER D. BILLINGS, Jr., A.B., J.D.
Professor of Law

SHARLENE BOLTZ, B.A., J.D.
Professor of Law

CAROL BREDEMeyer, A.B., M.S.L.S.
Professor of Law Library Services & Assistant Director for Faculty Services

ANTHONY E. CHAVEZ, B.S., J.D.
Associate Professor of Law

URSULA DOYLE, B.A., M.A., J.D.
Assistant Professor of Law

NANCY L. FIRAK, B.S., J.D., LL.M.
Professor of Law

CAROL FURNISH, B.A., M.L.S.
Professor of Law Library Services & Assistant Director for Instruction & Outreach

JOHNNY GARON, B.A., J.D.
Director of Law and Informatics Institute & Professor of Law

RICHARD GRAVES, B.A., J.D., L.L.M.
Assistant Professor of Legal Writing

CHRISTOPHER GULINELLO, B.A., J.D., L.L.M.
Professor of Law

AMY HALBROOK, B.A., J.D.
Director of Children’s Law Center Clinic & Assistant Professor of Law

JACK HARRISON, B.A., J.D.
Assistant Professor of Law

KIMBERLY HAUSBECK, B.A., J.D., L.L.M.
Assistant Professor of Legal Writing

THOMAS E. HEARD, B.A., M.L.S., J.D.
Associate Professor of Law Library Services & Associate Director for Information Technology

JENNIFER JOLLY-RYAN, B.A., J.D.
Professor of Legal Writing

KENNETH D. KATKIN, A.B., J.D.
Professor of Law

DONALD K. KAZEE, B.A., M.A., J.D.
Associate Professor of Legal Writing

JENNIFER KINSLEY, B.A., J.D.
Assistant Professor of Law & Field Placement Program Director

JENNIFER KREIDER, B.A., J.D.
Associate Dean for Faculty Development & Professor of Law

MICHAEL J.Z. MANNHEIMER, B.A., J.D.
Professor of Law

JENNIFER MART-RICE, B.A., M.S.L.S., J.D.
Assistant Professor of Law Library Services & Assistant Director for Collection Development, Serials and Acquisitions

BARBARA MCFARLAND, B.S., J.D.
Director of Student Success Initiatives & Assistant Professor

LIUBOMIR NACEV, B.A., J.D., L.L.M.
Professor of Law

LARRY O. PUTT, B.A., J.D., L.L.M.
Visiting Professor

DAVID SINGLETON, B.A., J.D.
Assistant Professor of Law

PHILLIP SPARKES, B.S., J.D., L.L.M.
Assistant Professor of Law & Director of Chase Local Government Law Center

DONNA M. SPEARS, B.A., M.L.I.S., J.D.
Assistant Professor of Law Library Services & Assistant Director for Research and Instructional Technology

MARK M. STAVSKY, B.A., J.D., L.L.M.
Professor of Law
HENRY L. STEPHENS, Jr., B.A., J.D.  
Professor of Law

JANE UNDERWOOD, B.A., M.L.S., J.D.  
Assistant Professor of Law Library Services &  
Assistant Director for Research and Online  
Services

JOHN T. VALAURI, B.A., J.D.  
Professor of Law

BARBARA WAGNER, B.A., M.S.B.A., J.D.  
Assistant Professor of Law,  
Director of the Small Business & Nonprofit  
Law Clinic & Co-Director of the  
Transactional Law Practice Center

CARYL A. YZENBAARD, A.B., J.D.  
Professor of Law

EMERITI FACULTY

CAROL B. ALLRED, B.A., M.S.L.S., J.D.  
ROBERT M. BRATTON, A.B., M.A., J.D.  
DAVID ELDER, B.S., L.L.M., J.D.  
EDWARD P. GOGGIN, J.D., LL.M.  
W. JACK GROSE, B.S.C., M.B.A., J.D.  
MARTIN J. HUELSMAN, B.B.A., J.D.  
WILLIAM R. JONES, B.S., M.A., J.D.  
KAMILLA M. MAZENAC, A.B., J.D., LL.M.  
LOWELL SCHECHTER, B.S., J.D., L.L.M  
FREDERICK SCHNEIDER, B.A., J.D.  
ROBERT L. SEAVER, A.B., J.D.  
DAVID C. SHORT, B.A., J.D., LL.M.

ADJUNCT FACULTY

DANIELLE ANDERSON, B.A., J.D.  
DONYETTE BAILEY, B.A.,J.D.  
DAVID BARRON, B.S., J.D.  
HON, GREGORY M. BARTLETT, A.B., M.A., J.D.  
JOHN K. BENINTENDI, J.D.  
VICTORIA BOGGS, B.A., J.D.  
NATASHA M. CAVANAUGH, A.B., J.D.  
NAIMA CLARK, B.S., J.D.  
REBECCA DILORETO, B.A., J.D.  
DAVID W. DORTON, B.S., M.S.M.E., J.D.  
ROBERT A. GOERING, B.A., J.D.  
WILLIAM GUSTAVSON, B.A., J.D.  
SHERYL HEETER, J.D.  
PENNY HENDY, B.S., J.D.  
NANCY HERBERT, J.D.  
HON, STEVEN R. JAEGGER, B.A., J.D.  
DAVID E. JEFFRIES, B.A., M.S.BIOTECH, J.D.  
RICHARD KATZ, B.A., J.D.  
JOSEPH T. MORDINO, B.A., J.D.  
FRANK MUNGO, B.S., J.D.  
DANIEL MURNER, B.A., J.D.  
ELIZABETH PEARSON, B.A., J.D.  
MARC PERA, B.S., J.D.  
WILLIAM A. POSEY, B.A., J.D.  
STEVEN H. RAY, B.A., J.D.  
DEBRA ROTHSTEIN, B.S., J.D.  
THOMAS L. ROUSE, B.S., J.D.  
ANN SCHOFEN, B.S., J.D.  
CINDY SHIROONI, B.A., J.D.  
HON, DOUGLAS M. STEPHENS, B.A., J.D., L.L.B  
HON, AMUL THAPAR, B.S., J.D.  
HON, KAREN A. THOMAS, B.A., J.D.  
BERNADEINE C. TOPAZIO, B.A., M.B.A., J.D.  
JUSTICE DONALD C. WINTERSHEIMER, A.B., M.A., J.D.  
J. STEPHEN WIRTHLIN, JR., B.A., J.D.
LAW + INFORMATICS SYMPOSIUM ON LABOR AND EMPLOYMENT ISSUES

ARTICLES

Can’t Escape from the Memory: Social Media and Public Sector Labor Law
William A. Herbert ................................................................. 427

A Call for Uncle Sam to Get Big Brother Out of Our Knickers:
Protecting Privacy and Freedom of Speech Interests in Social Media Accounts
Michelle Poore ........................................................................... 507

From Universal Exclusion to Universal Equality: Regulating Ableism in a Digital Age
Paul Harpur ............................................................................ 529

The Role and Effect of Social Media in the Workplace
Francois Quintin Cilliers ................................................................ 567

Employer Surveillance Versus Employee Privacy:
The New Reality of Social Media and Workplace Privacy
Saby Ghoshray ........................................................................... 593

Changing Dynamics of Employer-Employee Relationship and the Technology Interface:
A Critical Analysis
Tania Sebastian ........................................................................ 627

NOTES

Protecting Privacy of Medical Records of Employees and Job Applicants in the Digital Era
Under the Americans With Disabilities Act
Michael L. Tudor ....................................................................... 635

Access Denied: An Analysis of Social Media Password Demands in the Public Employment Setting
Mark B. Gerano ........................................................................... 665
CAN’T ESCAPE FROM THE MEMORY: SOCIAL MEDIA AND PUBLIC SECTOR LABOR LAW

William A. Herbert

Abstract: The Web 2.0 communicative revolution is impacting many fields of law, including labor and employment law. This article focuses upon the application and impact of statutory and constitutional doctrines on the use of social media in public employment in the United States. As part of that analysis, it will compare and contrast developments under the National Labor Relations Act, state collective bargaining and tenure laws and the First Amendment concerning social media. Through this comparative analysis, the article will highlight the distinctions and similarities of public sector labor law and their implications for the future.

I. INTRODUCTION

Like most human endeavors, the study and practice of law are not immune from the allure of societal fads, which can entice many and repel others. The combined power of rapid technological innovations and creative advertising has created a storm of consumer desire for electronic communicative devices, transforming want into need. The use of digital devices and their networks is reshaping our culture and our workplaces, metamorphosing formerly deniable or forgettable verbal exchanges into discoverable and distributable electronic written records. The Web 2.0 communicative revolution is simply the latest platform accelerating the velocity and growth of digital expressions and interchanges.

Governments, businesses, unions, political and cultural figures, and other individuals are finding social networking an effective tool for communicating, promoting, branding, and organizing. In the public sector, social media has

---

* Mr. Herbert is Deputy Chair of the New York State Public Employment Relations Board (PERB). The article is based upon a paper presented at the 2013 Law + Informatics Symposium on Labor and Employment Issues at the Salmon P. Chase College of Law, and at the 2013 ABA National Symposium on Technology in Labor and Employment Law in Berkeley, California. The opinions expressed are Mr. Herbert’s personal views and do not reflect the views of PERB or the State of New York. Mr. Herbert would like to express his gratitude to PERB Chairperson Jerome Lefkowitz for granting him permission to participate in the symposiums. Finally, Mr. Herbert acknowledges the assistance of Albany Law School student Sean P. Moran.
become an important open government tool for communicative exchanges with
the public.¹

The proliferation and accessibility of interactive electronic communications
are substantially enhancing individual and collective discourse, a vital element
for social interaction and unified workplace activities.² The communicative
revolution has expanded the ability to act collectively or individually concerning
employment, commercial, personal, and political issues. The successful
presidential campaigns of Barack Obama can be attributed, in part, to the
masterful use of social media and other technologies.³ It is too early to judge,
however, whether the use of social media will lead us toward a new renaissance
in political, social, and labor activism or whether it is destined to become just
another passivity-inducing development, leading to a further decline in social
capital.⁴ Generational, economic, cultural, and geographic factors will determine
the ultimate impact social networking will have on collective and associational
activities.

Social media platforms are popular fora for interactive dialogues related to
work, personal matters, and issues of great social and political import. Like
other means of discourse, the content can be thoughtful and profound, banal and
profane, or both. Writers can articulate substantive ideas and criticisms
concerning policies, practices, and current events that may be protected under
public and/or private sector workplace law. At the other end of the spectrum,
electronic statements and interactions can be childish, crude, immoral, disloyal
or just an outlet for thought dreams to be seen. As will be demonstrated in Parts
II(A) and (C), infra, employee posts found opprobrious and abusive toward an

---


². Jeffrey M. Hirsch, Communication Breakdown: Reviving the Role of Discourse in the Regulation of Employee Collective Action, 44 U.C. DAVIS L. REV. 1091, 1094 (2011) (“[C]ollective action requires a significant level of discourse and information transference among individuals; mere sporadic or impersonal contacts are inadequate.”).


employer or co-workers can lose applicable legal protections in the private and public sectors.5

Unlike other products, such as cars and bicycles, the design of social networking does not include built-in mechanical breaks or a clear user manual aimed at minimizing communicative accidents and collisions. Excessive cyberspacial exuberance can lead to the revelation and distribution of confidential, embarrassing, or harmful information for those forgetful or unmindful of their electronic footprints.6 The proverbial slippery slope into electronic mud is of particular concern when social networking involves certain types of relationships such as supervisor-employee or teacher-student.7

Frequently, employers learn of posted off-duty comments and photographs from so-called friends or others with access to an employee’s social media page.8 In one case, a Paterson, New Jersey, first-grade teacher was terminated after her posts describing students as “future criminals” were forwarded to the school district by one of her hundreds of Facebook friends, a former principal.9 Within

5. E.g., Atl. Steel Co., 245 N.L.R.B. 814 (1979) (The employee “called the foreman a ‘lying son of a bitch’ or stated that the foreman had told a ‘m—f—lie’ (or was a ‘m—f—liar’) as to whether he had asked the entire crew to work overtime.”); State of New York (Ben Aaman), 11 NYPERB ¶ 3084 (1978) (describing conduct, including: threatening supervisors during grievance hearing, abusing another supervisor with foul language, and creating a disturbance during an employer investigation).

6. As Robert Sprague has noted, social media “raises issues such as what is the boundary between public and private-at what point does something that is private become public? Can there be seclusion in cyberspace?” Robert Sprague, Invasion of the Social Networks: Blurring the Line Between Personal Life and the Employment Relationship, 50 U. LOUISVILLE L. REV. 1, 13 (2011) (footnotes omitted). See also William A. Herbert, Workplace Consequences of Electronic Exhibitionism and Voyeurism, 30 TECH. & SOCY MAG. 25 (2011).


8. E.g., Vista Nuevas Head Start, 129 Lab. Arb. Rep. (BNA) 1519 (2011) (VanDagens, Arb.) (Arbitrator found Head Start program had just cause to discharge a teacher for her profanity-filled abusive remarks about the program’s administrator, co-workers, students, and parents on a closed Facebook group page, set up primarily for teachers at the school. The school obtained print-outs of the posts from a group member, who was the estranged husband of one of the other teachers in the group.).

a few short days, her posts were the subject of parental outrage and media attention, which led to her termination. In Florida, elementary school teachers were verbally reprimanded after one compared a student to an orangutan in a Facebook post and others responded favorably to the comment. An Ohio middle school math teacher faces possible discharge after her colleague reported to the district that she posted on Facebook a photograph of her students with duct tape over their mouths with the caption: “Finally found a way to get them to be quiet!!” The alleged humor that might have motivated the conduct of the teacher and her students did not translate well in cyberspace, which is another cautionary tale involving social media in the public sector.

There are other examples of unprofessional or inappropriate electronic communications in the public sector leading quickly to disciplinary action or a demand that the employee resign. The steady stream of high-profiled and precipitous public sector falls and stumbles highlights the potential destructive workplace consequences of electronic footprints: the resignation of C.I.A. Director David H. Petraeus, the resignation of Congressman Christopher Lee, the firing of three congressional staff members, and the termination of an Indiana Deputy Attorney General.

Modernity cannot be blamed for unfiltered or unprofessional behavior; they are as old as humankind. The architectural design of the virtual world, however, encourages impulsiveness, exhibitionism, and undiscerning expression. It also ensures that such behaviors are readily discoverable and searchable, thanks to
the multiple repositories of data including tablets, laptops, smart phones, and the cloud. 18 Furthermore, it leads to significant blurring of the once firm line between work and off-duty activities in many occupational settings. 19

Far behind the cacophonous storm of digital communications, and resulting workplace consequences, is the application of labor law to employee social media use. As the United States Supreme Court has observed: “[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior,” 20 and “it is uncertain how workplace norms, and the law’s treatment of them, will evolve.” 21 With the exception of recently enacted laws in a few states placing restrictions on employer access to social media accounts of employees and applicants, 22 there has not been a focused reexamination of current laws and doctrines aimed at placing checks on irrational behavior associated with the use of, and response to, social media. The subject of civil liberties in the workplace must be revisited as well, at a time when an unsolicited photograph or video of off-duty conduct by a public employee can go viral, placing the unwitting subject in danger of losing her or his job. Along with a reconsideration of labor law

18. See Ariana C. Green, Using Social Networking to Discuss Work: NLRB Protection for Derogatory Employee Speech and Concerted Activity, 27 BERKELEY TECH. L.J. 837, 839 (2012) (“Using social networking websites both shares the posts and maintains them, providing employers with a potentially incriminating record that is often unavailable with in-person conversations.”).


21. Id.

22. Six states have enacted laws protecting the privacy of employees and/or applicants concerning their social media activities by prohibiting employers from seeking usernames and passwords: California, Illinois, Maryland, Michigan, Utah and New Mexico. Cal. Lab. Code § 980 prohibits employers from requesting an employee or applicant to disclose a username or password for the purpose of accessing personal media, access personal social media in the presence of the employer or to divulge any personal social media unless a request to an employee is reasonably believe to be related to an investigation into the employee’s misconduct or violation of applicable laws. In Maryland, private sector and governmental employers are prohibited from requesting or requiring an employee or applicant to disclose a username, password, or other means to accessing a personal account or service through an electronic communications device. See Md. Code, Lab. and Emp’t, §§ 3-712(a)(4)(i)(2), 3-712(b)(1). Effective January 1, 2013, the Illinois Right to Privacy in the Workplace Act, 820 Ill. Comp. Stat. Ann. 55 § 10 (West 2013), makes it unlawful for an employer to request or require an employee or prospective employee to provide a password or other related account information in order to gain access to the employee’s or prospective employee's account or profile on a social networking page. See Ariana R. Levinson, Social Media, Privacy and the Employment Relationship: The American Experience, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2265609. Similar legislation has been introduced in other states. See Nat’l Conf. of State Legislatures, Employer Access to Social Media Usernames and Passwords, available at http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx.
doctrines as applied to electronic communications, there needs to be a societal rededication to training and education to encourage mature and sober conduct in cyberspace.

A primary factor in determining the scope of legal protections for collective or individual electronic communications is whether the employee works for a private employer or government agency.23 The private and public sectors are subject to distinct sources of labor law, doctrines, and history.24 There are two related legal questions that arise in both sectors concerning social networking: whether the content of posts is legally protected from adverse personnel action; and whether the employer can lawfully impose and maintain a policy restricting social media activities by its employees.

In general, resolution of the first question requires an examination of various factors including whether: the content was work-related, personal, or touched upon a broad social or political issue; it was directed at other employees, other specific individuals, or the virtual world at-large; it was so egregious to lose legal protections; it had an adverse impact upon the workplace; it was created and distributed during work time or off-duty; it was made pursuant to work duties; and/or it was distributed with a personal device or the employer’s equipment.25

The second issue, the lawfulness of an employer’s policy, requires an analysis into whether the policy restricts or chills protected employee speech and association under applicable law, and whether the subject is mandatorily negotiable with the union that represents the employees subject to the policy. The question of negotiability is more likely to arise in the public sector where the density of union representation far exceeds representation in the private sector.26

A related third legal issue concerns whether an employee has enforceable privacy protections against employer access to a social media page or the right to be free from employer surveillance. Recent state laws concerning that issue

24. Id. at 338, 345, 359-61.
25. These factual issues are generally not relevant to whether the content of an electronic communication is protected under the anti-retaliation provisions of Title VII of the 1964 Civil Rights Act, 42 U.S.C. § 2000e-3(a) (2006), and the plethora of other federal and state laws prohibiting retaliation for reporting or seeking to report violations of law. The Supreme Court has cited to anti-retaliation laws as one rationale for narrowly construing the scope of employment protections for public employees under the First Amendment. See William A. Herbert, The Chill of a Wintry Light? Borough of Duryea v. Guarinieri and the Right to Petition in Public Employment, 43 U. TOL. L. REV. 583, 623-25 (2012) [hereinafter Herbert, The Chill of a Wintry Light?].
have substantially increased privacy protections concerning social networking. The new laws, however, do not limit an employer from accessing social media content from a page with low or no privacy settings or receiving it from individuals with lawful access to the page.

The scope of protected liberties and responsibilities as defined by judicial, legislative, and administrative actions can profoundly influence the shaping of labor strategies in both sectors. The law creates positive and negative incentives for employers, unions, and employees with respect to electronic speech and activities. Arguably, developments in the area of technology and workplace law should encourage collective employee action in the private and public sectors, along with a broadened application of social unionism in cyberspace.

The more posts reflect only individualistic workplace concerns, the less likely they will be legally protected. In contrast, workplace-related content linked with broader policy and social questions has the greatest likelihood of being protected. These objective legal incentives in the current era are eclipsed by predominant cultural and societal forces that encourage self-centeredness in cyberspace.

This article examines social media and public sector labor law based on a cross-sectoral analysis of legal doctrines and precedent. The comparison will

---

27. Supra note 22.
28. Supra note 22.
29. See William E. Forbath, Law and the Shaping of the American Labor Movement (1991) (demonstrating how decisions by federal and state courts enjoining labor activities and striking down protective labor legislation shaped the principles, tactics and strategies of the American labor movement at the turn of the 20th century).
30. See City of Ontario, Cal., 130 S. Ct. at 2629-30 (“As one amici brief notes, many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency. Another amicus points out that the law is beginning to respond to these developments, as some States have recently passed statutes requiring employers to notify employees when monitoring their electronic communications.”).
31. Social unionism denotes an anti-economistic strategy and tactics connecting workplace conditions with wider policy and social issues. See Stephanie Ross, Varieties of Social Unionism: Towards a Framework of Comparison, 11 JUST LAB.: A CAN. J. OF WORK & SOC’Y 16 (Autumn 2007), http://www.justlabor.yorku.ca/volume11/pdfs/02_Ross_Press.pdf (“Social unionism, generally understood to involve both engagement with social justice struggles beyond the workplace and methods of union activity beyond the collective bargaining process, is claimed to increase the labour movement’s organizing capacity, bargaining power, and social and political weight.”). Other scholars distinguish between “social unionism” and “social movement unionism,” a distinction without any real difference concerning the scope of protected social media activities under the law. See John W. Budd, Employment with a Human Face: Balancing Efficiency, Equity, and Voice 150 (2006) (“In contrast, social movement unionism embraces labor unions as part of a broader social movement of community, social, and political activist groups that relies on active grassroots participation and mobilization.”) (emphasis in original).
32. In their separate studies, Daniel J. Walkowitz, Paul Johnston, and Craig Reinarman have each demonstrated the value of comparative analyses of the private and public sectors. See Daniel J. Walkowitz, Working with Class: Social Workers and the Politics of Middle-Class
demonstrate that many public employees have broader protections for social networking than their private sector counterparts because of statutory and constitutional protections applicable only to the government workplace. These protections are reflective of the century-old consensus in the United States that a *de jure* regulatory structure for government employment is necessary to check the powers of the state and partisan politics.

American private sector labor relations is primarily regulated by the provisions of the National Labor Relations Act (NLRA), originally enacted in 1935 and substantially modified in 1947. Although the private sector union density rate in the United States is currently 6.6%, the NLRA’s central importance in regulating American private sector workplace has been reinforced as the result of the National Labor Relations Board (NLRB) applying well-established statutory doctrines and concepts to social media. For example, in *Hispanics United of Buffalo, Inc. (Hispanics United)*, the NLRB ruled that an employer violated the NLRA when it terminated five at-will employees based upon their social media posts, which were found to be protected concerted activity for mutual aid and protection regarding their terms and conditions of employment.

In unionized workplaces, collective bargaining agreements commonly contain just cause provisions, permitting challenges to disciplinary action through grievance arbitration procedures. In light of the ever-expanding growth of social media, arbitrators are beginning to hear employee misconduct

---

33. 29 U.S.C. §§ 151-69 (2012). Private sector labor relations in the airline and railroad industries are controlled by the Railway Labor Act, 45 U.S.C. §§151-88 (2012). Private sector employment that is not subject to the NLRA or the Railway Labor Act may be subject to a state collective bargaining law, such as New York’s State Employment Relations Act, N.Y. LABOR LAW §§ 700-18.


37. Id.

cases involving the content of posts on social networking pages.\textsuperscript{39} Therefore, disciplinary “arbitrators need to become familiar with all kinds of social networking platforms, learn how to deal with this kind of evidence, and understand the applicable statutory and case law” including the NLRA.\textsuperscript{40}

Labor relations in the public sector are regulated by a patchwork of rights and remedies from multiple legal sources. According to the latest national statistics, 7.3 million public sector employees are members of a union in the United States, constituting a union density rate of 35.9%.\textsuperscript{41} Many state and local jurisdictions have collective bargaining laws that grant statutory civil liberties to public employees including the rights to engage in union activities and other forms of concerted workplace-related speech and activities.\textsuperscript{42} Those laws limit the authority of public employers to take adverse actions that interfere with or discriminate against employees for exercising statutory rights of concerted speech and association.\textsuperscript{43} In addition, such laws restrict the power of employers to unilaterally impose or maintain policies that chill the exercise of statutory rights.\textsuperscript{44}

Public employees are generally not subject to the at-will employment rule, which is a major distinction between the public and private sectors.\textsuperscript{45} Most government workers have protections from civil service merit and fitness rules, statutory tenure, and disciplinary protections.\textsuperscript{46} In jurisdictions with collective

\textsuperscript{39} See U.S. Steel Corp, 130 Lab. Arb. (BNA) 461 (2011) (Bethel, Arb.) (Employer lacked just cause to discharge employee on the basis of three off-duty Facebook messages sent to his mother-in-law during a contested divorce and child custody fight.); Baker Hughes, Inc, 128 Lab. Arb. (BNA) 37 (2010) (Baroni, Arb.) (Employer had just cause to discharge employee for his off-duty post referencing the plant manager as “German, green card terminator” and stating “I could have sworn that Hitler committed suicide.” The national origin slur violated the employer’s anti-harassment policy and the employee failure to show remorse or apologize for the content of his post.).

\textsuperscript{40} Robert L. Arrington, Aaron Duffy & Elizabeth Rita, \textit{When Worlds Collide: An Arbitrator’s Guide to Social Networking Issues in Labor and Employment Cases}, 66 DISP. RESOL. J., no. 4, (Nov. 2011-Jan. 2012), at 2. See also Vista Nuevas Head Start, 129 Lab. Arb (BNA) 1519 (2011) (VanDagens, Arb.) (An employee’s post regarding a supervisor arriving late to work, read in the context of other employees’ posts on a group Facebook page, was not protected concerted activity but a mere gripe.).

\textsuperscript{41} U.S. DEP’T OF LAB., BUREAU OF LAB. STAT., \textit{supra} note 26.

\textsuperscript{42} See R. Theodore Clark, Jr., \textit{Public Sector Collective Bargaining at the Crossroads}, 44 URB. LAW. 185, 187 (Winter 2012) (According to Clark’s survey, twenty-eight states and the District of Columbia currently have comprehensive collective bargaining laws for their public sector employees and eleven other states grant similar rights to specifically defined job classifications.).

\textsuperscript{43} \textit{Id.}

\textsuperscript{44} \textit{Id.}

\textsuperscript{45} See Herbert, \textit{The Chill of a Wintry Light?}, \textit{supra} note 25, at 592-94, 597-99 (describing the development of statutory tenure and disciplinary protections for public employees in the federal sector and in Pennsylvania).

\textsuperscript{46} \textit{Id.}
bargaining laws, protections against arbitrary disciplinary action can be enhanced through negotiated just cause provisions.\textsuperscript{47} Another major distinction between the public and private sectors is that government employment is regulated by constitutional protections concerning speech, association, and privacy.\textsuperscript{48} Despite the panoply of public sector legal issues connected with social media, most of the legal commentary and media attention involving social networking and the workplace has ignored the public sector.\textsuperscript{49}

The article begins in Parts II(A) and (B) with legal developments concerning the scope of legally protected social networking activities by private employees under the NLRA. Although the NLRA exempts states and political subdivisions from the definition of “employer,”\textsuperscript{50} thereby rendering the federal statute’s protections inapplicable to government employment, NLRB precedent provides a useful framework for examining analogous issues in the public sector. Furthermore, NLRB precedent is considered by state collective bargaining agencies in examining analogous legal issues. In Part I(C), the article compares work-related protections under public sector collective bargaining and other laws in Michigan, Florida, and New York, with legal developments under the NLRA concerning protected concerted activities.

In Part III, the legal limitations on the scope of employer social networking policies in the private and public sectors are compared. Constitutional issues relating to public sector employee social networking under the First and Fourth Amendments is explored in Part IV. It will demonstrate that the First Amendment provides the greatest protections for social networking about public policy issues, while providing no protections for posts made pursuant to an employee’s official responsibilities. It will also show that the applicable scrutiny of an employer’s social media policy under the First Amendment is weaker than the degree of scrutiny applied to policies under the NLRA and state collective bargaining laws.

\textsuperscript{47} Id. at 626.


\textsuperscript{50} “The term ‘employer’ includes any person acting as an agent of an employer, directly or indirectly, but shall not include the United States or any wholly owned Government corporation, or any Federal Reserve Bank, or any State or political subdivision thereof, or any person subject to the Railway Labor Act [45 U.S.C. § 151 et seq.], as amended from time to time, or any labor organization (other than when acting as an employer), or anyone acting in the capacity of officer or agent of such labor organization.” 29 U.S.C. § 152(2) (2012). Whether a particular entity or body is a political subdivision exempt from the NLRA requires resolution of whether it is “(1) created directly by the State, so as to constitute departments or administrative arms of the government, or (2) administered by individuals who are responsible to public officials or to the general electorate.”  NLRB v. Natural Gas Util. Dist. of Hawkins Cnty., 402 U.S. 600, 604-05 (1971).
II. SOCIAL NETWORKING AS A STATUTORILY PROTECTED LABOR ACTIVITY

In four decisions in 2012 and 2013, Hispanics United,51 Costco Wholesale Corp (Costco),52 Karl Knauz Motors, Inc. (Karl Knauz)53 and Design Technology Group, LLC (Bettie Page Clothing),54 the NLRB Board has begun to explore the extent to which the NLRA limits the right of the employers to discipline employees for the content of their social media comments, and regulates the scope of employer policies related to social media. Developing private sector precedent under the NLRA can also constitute persuasive authority with respect to social media in the public sector.

The application of the NLRA to social networking has been the subject of substantial legal commentary and press coverage over the past three years. The genesis of this interest has its origin in the December 2009 termination of an emergency medical technician employed by a New Haven medical services company based upon critical Facebook posts she made about her supervisor, which generated supportive posts by co-workers.55 Following the discharge, an unfair labor practice charge was filed with NLRB Region 34 resulting in an investigation into whether the company’s adverse action against the medical technician and its written policies, violated Section 8(a)(1) and (3) of the NLRA.56 During the investigation, the NLRB General Counsel’s Division of

56. Id.; 29 U.S.C. §§ 158(a)(1) and (3) (2012) state:

It shall be an unfair labor practice for an employer--
(1) to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in section 7;
(3) by discrimination in regard to hire or tenure of employment or any term or condition of employment to encourage or discourage membership in any labor organization: Provided, That nothing in this Act [subchapter], or in any other statute of the United States, shall preclude an employer from making an agreement with a labor organization (not established, maintained, or assisted by any action defined in section 8(a) of this Act [in this subsection] as an unfair labor practice) to require as a condition of employment membership therein on or after the thirtieth day following the beginning of such employment or the effective date of such agreement, whichever is the later, (i) if such labor organization is the representative of the employees as provided in section 9(a) [section 159(a) of this title], in the appropriate collective-bargaining unit covered by such agreement when made, and (ii) unless following an election held as provided in section 9(e) [section 159(e) of this title] within one year preceding the effective date of such agreement, the Board shall have certified that at least a majority of the employees eligible to vote in such election have
Advice issued a memorandum advising the NLRB Regional Director to issue a complaint against the medical services company alleging that it violated Section 8(a)(1) and (3) of the NLRA when it terminated the technician for her Facebook posts and for maintaining overly broad policies concerning internet postings and employee conduct that might reasonably chill the exercise of rights guaranteed by Section 7 of the NLRA.

Section 7 of the NLRA states:

Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection, and shall also have the right to refrain from any or all of such activities except to the extent that such right may be affected by an agreement requiring membership in a labor organization as a condition of employment as authorized in section 8(a)(3).

Following the advisory memorandum, NLRB Region 34 issued a complaint against the New Haven company alleging that the technician’s discharge and the

voted to rescind the authority of such labor organization to make such an agreement: Provided further, That no employer shall justify any discrimination against an employee for non-membership in a labor organization (A) if he has reasonable grounds for believing that such membership was not available to the employee on the same terms and conditions generally applicable to other members, or (B) if he has reasonable grounds for believing that membership was denied or terminated for reasons other than the failure of the employee to tender the periodic dues and the initiation fees uniformly required as a condition of acquiring or retaining membership.

57. The NLRB Division of Advice is delegated the responsibility to prepare advisory memoranda for NLRB Regional Directors concerning novel or complicated legal issues that arise in pending unfair labor practice charges. See Nat’l Labor Relations Bd., Organization and Functions, section 202.1.2, http://www.nlrb.gov/sites/default/files/documents/254/ organdfunctions.pdf. Although the particular NLRB Region is required to follow an advice memorandum, the memorandum is not binding upon the NLRB or its Administrative Law Judges.

58. 29 U.S.C. § 157 (2012). In December 2009, the NLRB General Counsel’s Division of Advice recommended dismissal of an unfair labor charge against another employer, which alleged that its social media policy violated the NLRA because it prohibited “[d]isparagement of company’s or competitors’ products, services, executive leadership, employees, strategy, and business prospects.” In that case, the advice memorandum concluded that the rule, read in the context of the whole policy, would not reasonably be construed by an employee to prohibit activities protected by Section 7 of the NLRA because the policy prohibited a list of other clearly unprotected activities including explicit sexual references and references to illegal drugs and the policy’s preamble stated that it was not aimed as restricting “the flow of useful and appropriate information.” See Advice Memorandum from the NLRB Office of the Gen. Counsel to Martin O. Osthus, Reg’l Dir. of Region 18, Sears Holdings (Roebucks), Case No. 18-CA-19081, at 2-3, 5 (Dec. 4, 2009, available at http://www.employerlawreport.com/uploads/file/ Advice%20memorandum.pdf.

company’s written policies violate Sections 8(a)(1) and (3) of the NLRA. 60

Among the policies alleged to violate the NLRA was the following internet use policy in the employee handbook:

**Blogging and Internet Posting Policy**

- Employees are prohibited from posting pictures of themselves in any media, including but not limited to the Internet, which depicts the Company in any way, including but not limited to a Company uniform, corporate logo or an ambulance, unless the employee receives written approval from the EMSC Vice President of Corporate Communications in advance of the posting;
- Employees are prohibited from making disparaging, discriminatory or defamatory comments when discussing the Company or the employee’s superiors, co-worker and/or competitors. 61

The NLRB announcement concerning the issuance and substance of the complaint against the New Haven company, and the subsequent settlement of the complaint, generated wide publicity. 62 While most media reports focused attention on the complaint’s allegations concerning the discharge, portraying it as a test case over protections for social media postings, the NLRB Acting General Counsel Lafe Solomon described the case as the mere application of well-settled precedent concerning protected employee communications about workplace terms and conditions:

This is fairly straightforward case under the National Labor Relations Act – whether it takes place on Facebook or at the water cooler, it was employees talking jointly about working conditions, in this case about their supervisor, and they have a right to do that. 63


63. Greenhouse, supra note 49. See also Bruce E. Boyden, Oversharing: Facebook Discovery and the Unbearable Sameness of Internet Law, 65 Ark L. Rev. 39, 40 (2012) (“The meme that
The heightened attention given to the NLRB’s actions in the New Haven case is explainable by the trendiness of social networking and the general ignorance about the scope of the associational workplace rights and protections guaranteed by the NLRA. NLRB Albany Resident Officer Barnett L. Horowitz has aptly observed that the press coverage following the NLRB’s press release demonstrated that “there seemed to be a collective disbelief” that Section 7 of the NLRA applied to unrepresented employees.64

The enactment of the NLRA has been described by one historian “as a momentous libertarian victory,” that is “perhaps the single most important civil liberties statute ever passed by Congress, [which] extended, in theory at least, the guarantees of the First Amendment to American workers who had grown accustomed to enjoying their civil liberties on the sufferance of their employers.”65 Nevertheless, if questioned or polled, few Americans would know or recall that the statutory declaration of national public policy favoring broad private sector worker associational rights remains in effect today:

> It is declared to be the policy of the United States to eliminate the causes of certain substantial obstructions to the free flow of commerce and to mitigate and eliminate these obstructions when they have occurred by encouraging the practice and procedure of collective bargaining and by protecting the exercise by workers of full freedom of association, self-organization, and designation of representatives of their own choosing, for the purpose of negotiating the terms and conditions of their employment or other mutual aid or protection.66

Ignorance concerning the “full freedom of association” protected under the NLRA is attributable to a variety of causes, including government policies

everything on the Internet is startlingly different has become so engrained that it is actually fairly common for people to miss instances where the fact that a transaction or communication occurs on the Internet, or using computers, is of no significance at all. In the legal world, there are numerous examples where the standard rules developed over the course of the twentieth century work just fine when applied to the Internet.”).  
favoring deindustrialization, deregulation, and globalization over the past few
decades, which partially explains why 93% of the private sector workforce is
presently unrepresented. It is also traceable to a general cultural shift in favor
of individualism premised upon two amoral precepts: selfishness is a virtue and
greed is good. The lack of knowledge regarding NLRA protections also results
from insufficient education and training regarding protected collective
workplace rights, and labor history in general.

Contrary to the current prevalent misunderstanding, Section 7 of the NLRA
protects unorganized employees who engage in activities for mutual aid and
protection with or without involvement by a union. These protections have
existed since well before the advent of social networking. The liberties granted
by Section 7 of the NLRA also cover collective activities external to the
employer-employee relationship, if aimed at improving workplace conditions
such as petitioning administrative, legislative, and judicial forums. As will be
demonstrated in Parts II(C) and IV, collective activities by government
employees receive similar protections in jurisdictions with collective bargaining
laws, and their activities might also be subject to constitutional protections under
the First Amendment.

---

67. There are multiple additional reasons for the steady decline in union density including the
growth of the decentralized service economy and failed union strategies and tactics. Gary N.
Chaison responded to 2012 statistics showing a continued decline in union density by stating: “It’s
a time for unions to stop being clever about excuses for why membership is declining, and it’s time
to figure out how to devise appeals to the workers out there.” Steven Greenhouse, Share of the
Work Force in a Union Falls to a 97-Year Low, 11.3%, N.Y. TIMES, Jan. 24, 2013, at B1, available at
THE LAST DAYS OF THE WORKING CLASS (2010) (examining the historical, political and cultural
forces leading to the decline of private sector unionization during the 1970’s).

68. See Bill Fletcher & Jane McAlevey, Lessons from Wisconsin, OPINIONNATION (Jun. 26,
2012), http://www.thenation.com/blog/168435/opinionnation-labors-bad-recall (arguing that the
unions have a responsibility to develop and maintain effective worker education programs). The
lack of union leadership support for labor education is not a recent phenomenon. See Al Nash &
May Nash, Labor Unions and Labor Education, UNIV. LAB. EDUC. ASS’N, MONOGRAPH SERIES NO.
1, 5 (June 1970) (“Labor educators generally agree that labor education activities have failed to
become institutionalized in the labor movement or to affect a significant cross-section of labor
leaders. A few larger unions sponsor educational activities and cooperate with universities in the
field, but the majority of unions in American do not sponsor or support labor education.”).

69. See Rita Gail Smith & Richard A. Parr II, Protection of Individual Action As ‘Concerted
Activity’ under the National Labor Relations Act 68 CORNELL L. REV. 369, 371 (1983) (“Section 7
protects employees engaged in concerted activity in a wide variety of circumstances. It protects, for
instance, nonunionized employees engaged in such activity and, in some instances, protects
unionized employees acting outside established grievance procedures. Section 7 even protects
concerted conduct by employees who contemplate neither union activity nor collective
bargaining.”) (footnotes omitted).


While the NLRB complaint against the New Haven company was settled prior to an adjudicatory ruling, social media cases under the NLRA have proliferated with respect to two primary issues: the legality of adverse actions taken against employees for their posts and the lawfulness of employer social media policies. There have been a series of social media decisions issued by the NLRB and its Administrative Law Judges (ALJs) examining those issues, as well as one ALJ decision examining whether a union’s conduct with respect to social media violated its obligations under the NLRA. In describing the NLRB’s actions in this area, NLRB Chairman Mark Gaston Pearce has emphasized that “All we’re doing is applying traditional rules to a new technology.”

The NLRB General Counsel’s Division of Advice has issued numerous advisory memoranda concerning social media cases, and NLRB Acting General Counsel Solomon has issued three reports summarizing those memoranda, which constitute persuasive authority in future social media cases. The NLRB General Counsel plays a central role in developing NLRA case law through the grant of prosecutorial responsibility to accept, investigate, resolve, or dismiss unfair labor practice charges and, following an investigation, to issue and prosecute complaints alleging unfair labor practice charges and, following an investigation, to issue and prosecute complaints alleging unfair labor practices against employers and unions.

The importance of the legal developments regarding social media under the NLRA is reflected in a 2011 study by the U.S. Chamber of Commerce analyzing

---

72. Under the settlement, “the company agreed to revise its overly-broad rules to ensure that they do not improperly restrict employees from discussing their wages, hours and working conditions with co-workers and others while not at work, and that they would not discipline or discharge employees for engaging in such discussions.” A separate agreement between the discharged EMT worker and the company resolved the termination resulting from her Facebook postings. See Press Release, NLRB, Settlement reached in case involving discharge for Facebook comments (Feb. 8, 2011), available at http://www.nlrb.gov/news/settlement-reached-case-involving-discharge-facebook-comments.

73. See Amalgamated Transit Union, Local Union No. 1433, AFL-CIO, Case No. 28-CB-78377 (N.L.R.B. Div. of Judges Nov. 28, 2012).

74. Steven Greenhouse, supra note 62.


the status of NLRB social media cases. The proactive administrative approach adopted by the NLRB Acting General Counsel concerning social media over the past few years has not been free from criticism.

Private sector labor law in this area remains unsettled because the NLRB Board’s social media decisions have not been judicially reviewed and exceptions to other NLRB ALJ decisions have not yet been decided. Moreover, there is a possibility that the NLRB Board decisions in Hispanics United, Costco, Karl Knauz, and Bettie Page Clothing might be judicially nullified as the result of litigated claims that President Obama’s 2012 recess appointments to the NLRB Board were unconstitutional. The final results of the pending litigation regarding those appointments might result in the social media decisions being reversed, and reconsidered by a differently constituted NLRB Board.

77. See Michael J. Eastman, Exec. Dir. Labor Law Policy, U.S. Chamber of Commerce, A Survey of Social Media Issues Before the NLRB 1 (Aug. 5, 2011) (report prepared for the U.S. Chamber of Commerce Labor, Immigration & Emp. Benefits Div.), available at http://www.uschamber.com/sites/default/files/reports/NLRB%20Social%20Media%20Survey.pdf. (“The Board has only just begun to address these many important issues, and it is, of course, hard to speculate as to how the Board will rule as these cases develop and whether those decisions will withstand scrutiny. It is hoped that this survey can assist employers and counsel identify issues with which they should be aware as they grapple with the application of labor law to employee use of social media.”).


82. See Canning v. NLRB, 705 F.3d 490, 514 (D.C. Cir. 2013), cert. granted, No. 12-1281, 2013 WL 1774240 (Jun. 24, 2013); NLRB v. New Vista Nursing & Rehab., Nos. 11-3440, 12-1027 & 12-1936, 2013 U.S. App. LEXIS 9860, at *116-17 (3d. Cir. May 16, 2013) (The U.S. Courts of Appeals for the D.C. and Third Circuits vacated NLRB Board decisions on the grounds it lacked a quorum because President Obama’s appointments of certain Board members violated Art. II §2, cl. 2 of the United States Constitution. Art.II §2, cl. 2 states: “He shall have Power, by and with the Advice and Consent of the Senate, to make Treaties, provided two thirds of the Senators present concur; and he shall nominate, and by and with the Advice and Consent of the Senate, shall appoint Ambassadors, other public Ministers and Consuls, Judges of the supreme Court, and all other Officers of the United States, whose Appointments are not herein otherwise provided for, and which shall be established by Law: but the Congress may by Law vest the Appointment of such inferior Officers, as they think proper, in the President alone, in the Courts of Law, or in the Heads of Departments.”). See also Melanie Trottman, Chamber Urges Businesses to Appeal Labor Rulings, WALL ST. J. (Jan. 31, 2013, 7:26 PM), http://online.wsj.com/article/SB1000142412788732392610457827623323334320.html; Steven Greenhouse, More Than 300 Labor Board Decisions Could Be Nullified, N.Y. TIMES, Jan. 26, 2013, at A10, available at http://www.nytimes.com/2013/01/26/us/labor-relations-board-rulings-could-be-undone.html?ref=nationalabolorrelationsboard.
With those caveats, we begin with an analysis of the developing NLRB case law on the issue of whether social networking constitutes protected concerted activity under the NLRA. The article then explores the comparative scope of protections under public sector collective bargaining and tenure laws in Michigan, Florida, and New York. While Michigan and Florida have collective bargaining provisions similar to Section 7 of the NLRA, their respective administrative case law is not fully consistent with NLRB precedent. In New York, the public sector collective bargaining law omits protections for concerted activity unrelated to forming, joining, and participating in a union. Therefore, NLRB precedent defining the scope of concerted activity for mutual aid and protection has less relevance in New York’s public sector.

A. Standards for Protected Concerted Activity under Section 7 of the NLRA

The regulatory impact of the NLRA on social networking is directly related to the scope of private sector employee activities it protects. By definition, the full right of association guaranteed by the NLRA is inseparable from the statutorily protected civil liberty of free speech regarding private sector terms and conditions of employment.

Whether the NLRA protects employee social media conduct is resolved in each case within the context of an unfair labor practice case, in which it is alleged that an employer violated §§8(a)(1) and/or (3) of the NLRA by taking an adverse action against an employee because of her or his social media activity. The respective burdens of proof in such cases are analyzed within the framework set forth in Wright Line. Under that test, the NLRB General Counsel has the initial burden of proving that protected concerted activity was a substantial or motivating factor in the adverse action taken against an employee. Following that initial showing, the burden shifts to the employer to demonstrate that it would have taken the same action even in the absence of the protected activity.

A central issue in many NLRB social networking cases is whether the postings that formed the basis for an adverse action constituted protected “concerted activities” for “mutual aid and protection” under Section 7 of the

84. Supra note 56.
86. Wright Line, 251 N.L.R.B. at 1089 (“First, we shall require that the General Counsel make a prima facie showing sufficient to support the inference that protected conduct was a ‘motivating factor’ in the employer's decision.”).
87. Id. (“Once this is established, the burden will shift to the employer to demonstrate that the same action would have taken place even in the absence of the protected conduct.”).
NLRA.\textsuperscript{88} Thus far, the social networking involved in NLRB decisions have not related to the more commonly known statutory “right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing.”\textsuperscript{89}

Like other subjects under the NLRA, the application of the legal standards for what constitutes protected “concerted activities” for “mutual aid and protection” under Section 7 of the NLRA is subject to a continuing debate.\textsuperscript{90} This is due, in part, to the fact that the statutory phrase “concerted activities” is undefined, and requires a determination regarding “which particular actions of an individual must be linked to the actions of fellow employees in order to permit it to be said that the individual is engaged in concerted activity.”\textsuperscript{91} In \textit{NLRB v. City Disposal Systems, Inc.,}\textsuperscript{92} the United States Supreme Court noted that it is “not self-evident from the language [of the NLRA]...the precise manner in which particular actions of an individual employee must be linked to the actions of fellow employees in order to permit it to be said that the individual is engaged in concerted activity.”\textsuperscript{93} The uncertainty concerning protections for individual acts led two scholars to acknowledge that “when an individual employee protests alone, without any consultation with and authorization by fellow employees, his legal rights under section 7 may be drastically curtailed, even when he purports to voice the concerns of others but especially when he is speaking only for himself in lodging a protest regarding working conditions affecting him alone.”\textsuperscript{94}

The \textit{sine qua non} of protected “concerted activities” for “mutual aid or protection” is when an employee speaks with co-workers about their need for unionizing.\textsuperscript{95} In such situations, there is little question that the comment is protected because “the guarantees of Section 7 of the Act extend to concerted activity which in its inception involves only a speaker and a listener, for such activity is an indispensable preliminary step to employee self-organization.”\textsuperscript{96} In the unionized context, an individual employee’s reasonable assertion of a contract right based on the terms of a collective bargaining agreement will also be protected because it is an extension of the concerted activity that led to the agreement, and the grievance can impact the rights of all employees covered by
the agreement. At the other extreme, personal gripes by employees unrelated to group action with co-workers or not aimed at inducing collective action, will be found to be unprotected. Narcissistic social media postings about work are least likely to be found protected.

In 1975, the NLRB adopted a broader view when it found that a single employee’s health and safety complaint to a state agency was protected activity, although the employee had never discussed the safety issue with his co-workers, and had not sought their support or requested their assistance in any manner. Despite the lack of such evidence, the NLRB reasoned that the written complaint was protected because the importance of occupational safety was shared by the entire work force, and subject to state legislation. It concluded that “where an employee speaks up and seeks to enforce statutory provisions relating to occupational safety designed for the benefit of all employees, in the absence of any evidence that fellow employees disavow such representation, we will find an implied consent thereto and deem such activity to be concerted.”

The NLRB soundly rejected this analytical standard nine years later in Meyers Industries, Inc. (Meyers I), when it adopted what it described as an “‘objective’ standard of concerted activity” to be applied to the particular facts in each case:

Although the definition of concerted activity we set forth below is an attempt at a comprehensive one, we caution that it is by no means exhaustive. We acknowledge the myriad of factual situations that have arisen, and will continue to arise, in this area of the law. In general, to find an employee’s activity to be “concerted,” we shall require that it be engaged in with or on the authority of other employees, and not solely by and on behalf of the employee himself. Once the activity is found to be concerted, an 8(a)(1) violation will be found if, in addition, the employer knew of the concerted nature of the employee’s activity, the concerted activity was protected by the Act, and the adverse

employment action at issue (e.g., discharge) was motivated by the employee’s protected concerted activity.  

The D.C. Circuit reversed the adoption of the new standard in Meyers I on the grounds the NLRB “erred when it decided that its new definition of ‘concerted activities’ was mandated by the NLRA” and that the decision “stands on a faulty legal premise and without adequate rationale.” Upon remand, the NLRB in Meyers II reaffirmed and clarified the standard for concerted activity. In its supplemental decision, the NLRB emphasized that the standard for concerted activity did not preclude protections for individual conduct. Instead, the standard distinguishes “between an employee’s activities engaged in ‘with or on the authority of other employees’ (concerted) and an employee’s activities engaged in ‘solely by and on behalf of the employee himself’ (not concerted).” In addition, the agency reiterated that the “definition of concerted activity in Meyers I encompasses those circumstances where individual employees seek to initiate or to induce or to prepare for group action, as well as individual employees bringing truly group complaints to the attention of management.” When the “evidence demonstrates group activities, whether ‘specifically authorized’ in a formal agency sense, or otherwise,” it will be found to be concerted conduct.

Although intemperate remarks and impulsive behavior during the course of labor relations will, at times, be protected under the NLRA, opprobrious and egregious conduct or comments by individuals while engaged in concerted activities can result in the loss of statutory protections. In determining whether an employee’s behavior has crossed that line, the NLRB considers four factors first articulated in Atlantic Steel Co.: (1) the place of the discussion; (2) the subject matter of the discussion; (3) the nature of the employee’s

---

104. Id. at 496-97.
105. Prill, 755 F.2d at 942 (emphasis in original).
107. Id.
108. Id. at 885.
109. Id. at 888; see Mushroom Transp. Co. v. NLRB, 330 F.2d 683, 685 (3d Cir. 1964) (stating that to meet the definition of protected concerted activity “it must appear at the very least that it was engaged in with the object of initiating or inducing or preparing for group action or that it had some relation to group action in the interest of the employees”).
110. Meyers II, 281 N.L.R.B. 882, 886 (1986). See also Owens-Corning Fiberglass Corp v. NLRB, 407 F.2d 1357, 1365 (4th Cir 1969) (stating that a single employee’s activities to gain support from fellow employees for their mutual aid and protection is as much ‘concerted activity’ as is ordinary group activity).
111. See NLRB v. Thor Power Tool Co., 351 F.2d 584, 587 (7th Cir. 1965).
outburst; and (4) whether the outburst was, in any way, provoked by the employer’s unfair labor practices.114

Before we examine the NLRB decisions involving employee use of social networking, it is worth examining a case that sheds light on the application of the standards of Meyers I, Meyers II, and Atlantic Steel Co. to the electronic workplace. In Timekeeping Systems, Inc.,115 an e-mail from an employee to his co-workers, with the salutation “Greetings Fellow Traveler,” critical of the employer’s e-mail announcement of proposed changes in a vacation policy, was found to be a protected concerted activity.116 The employer’s announcement to the entire workforce encouraged employees to comment about the changes, and the employee’s e-mail encouraged his co-workers to support his opposition to the modification, after some of them had circulated comments supportive of the change.117 The employee’s e-mail was found to be concerted activity because it implicitly sought to encourage group action to maintain the current vacation policy.118 While the employer found the e-mail to be disrespectful and discourteous, and the ALJ found that the e-mail utilized “some flippant, and rather grating language,”119 the NLRB found that the wording was not opprobrious and egregious thereby warranting exclusion from NLRA legal protections.120

The protected e-mail in Timekeeping Systems, Inc. was directed to co-workers and the employer, and its length and detail strongly suggested that the employee spent a fair amount of time composing it.121 By contrast, electronic communications through social media are not always equivalent to internal workplace e-mail exchanges or traditional water cooler discussions. For one thing, access to social networking pages and tweets are frequently not limited to co-workers. An employee’s social media wall may include responsive posts from friends with no relationship with the workplace. In addition, the speed of the communicative exchanges through social media can blur personal issues with other matters and encourage the posting of workplace gripes filled with unfiltered thoughts and phrases.122 As the case law develops, NLRA standards

114. Id.
115. 323 N.L.R.B. 244, 249 (1997).
116. Id.
117. Id. at 246.
118. Id. at 247.
119. Id. at 246.
120. Id. at 249.
122. See Amalgamated Transit Union, Local Union No. 1433, AFL-CIO, Case No. 28-CB-78377 (N.L.R.B. Div. of Judges Nov. 28, 2012) (social networking page is not the virtual equivalent of a picket line); Advice Memorandum from the NLRB Office of the Gen. Counsel to Daniel L. Hubbel, Reg’l Dir. of Region 17, Wal-Mart, No. 17-CA-25030, at 3 (July 19, 2011), available at http://mynlrb.nlrb.gov/link/document.aspx/09031d458056e73d (directing dismissal of
will probably start to take into consideration the unique design of social media and the consequences of that design.123

B. Social Networking as a Protected Concerted Activity under the NLRA

The first NLRB Board decision to determine whether the content of social networking postings was protected under Section 7 of the NLRA was Karl Knauz.124 In that case, the NLRB affirmed an ALJ’s conclusion that a car salesman was not unlawfully discharged for his Facebook postings based upon the ALJ’s credibility finding that the decision to discharge was based solely upon the content of a particular post regarding a car accident at another dealership owned by the employer.125 The at-issue post did not involve a discussion with co-workers and had no connection to their terms and conditions of employment.126 Therefore, the salesman’s termination was found lawful under the NLRA because it was not based upon concerted activity for mutual aid and protection.127

The decision in Karl Knauz reflects a core evidentiary question that will arise in many social networking cases. Due to the communicative exuberance
associated with social media, a determination concerning whether an adverse action was unlawful under the NLRA will frequently depend upon a credibility finding about which post(s) were the substantial motivating factor in the employer’s decision.\(^{128}\) By relying upon the ALJ’s credibility determination in Karl Knauz, the NLRB avoided examining the ALJ’s alternative conclusion that the salesman’s other posts about a workplace issue were protected concerted activities.\(^{129}\) Those posts were made following comments by sales staff about how the lousy food being offered at a scheduled sales event would adversely impact the size of their commissions.\(^{130}\) At the event, the salesman took photographs of his co-workers holding hot dogs, chips, and water.\(^{131}\) Later he posted the photographs, along with sarcastic remarks about the quality of the food, on his Facebook page.\(^{132}\) The ALJ concluded that the postings concerning the sales event were protected concerted activities because they were an outgrowth of conversations with co-workers related to the impact on their compensation from sales resulting from the inadequacies of the food.\(^{133}\) Finally, the ALJ found that the sarcasm and mocking tone of the posts did not deprive them of protection.\(^{134}\)

In Hispanics United,\(^{135}\) the NLRB held that off-duty workplace-related social media posts by five unrepresented employees of a non-profit social services agency constituted protected concerted activities for mutual aid and protection, and affirmed an ALJ’s finding that the employer violated §8(a)(1) of the NLRA when it terminated the five employees based upon the content of their posts. While Board Member Hayes dissented, he agreed with the majority that the standards articulated in Meyers I and Meyers II were applicable to determining whether social networking posts were protected concerted activity, and that the intent of employees to engage in collective action can be inferred from the posts; intent need not be explicit.\(^{136}\)

---

129.  Id.
130.  Id.
131.  Id.
132.  Id.
133.  Id.; see Mike Yurosek & Son, Inc., 306 N.L.R.B. 1037, 1038 (1992) (finding that employees’ refusal to work overtime was protected because it was a “logical outgrowth” of prior collective disputes reduction in schedule).
136.  Id. at *4-5, n.7.
The facts regarding the at-issue social networking activities in Hispanics United are simple and concise. Shortly after a new domestic violence advocate Lydia Cruz-Moore was hired, she began complaining to another agency employee, Marianna Cole-Rivera, about the job performance of other employees assigned to assist domestic violence victims, particularly those in the housing department. Cruz-Moore also criticized housing department employees directly concerning their work habits. After Cruz-Moore threatened to inform the agency’s executive director about her criticisms concerning the job performance of others, Cole-Rivera made the following off-duty post on her Facebook page, using her personal computer:

Lydia Cruz, a coworker feels that we don’t help our clients enough . . . . I about had it! My fellow coworkers how do u feel?

Four co-workers, using their own personal computers, responded with off-duty posts objecting to Cruz-Moore’s criticisms, defending the quality of their work, and expressing frustrations about workplace conditions including their case load. In addition, a member of the agency’s board of directors and the executive director’s secretary each made responsive posts. Cruz-Moore also made a post stating “…stop with ur [sic.] lies about me.” Cruz-Moore immediately complained to the executive director about the Facebook posts, and provided print-outs of the posts. Cole-Rivera and the four co-workers were terminated on the basis that the content of their posts violated the employer’s policy against bullying and harassment.

In affirming the ALJ in Hispanics United, the majority concluded that there was “no question” the posts were protected concerted activities for mutual aid and protection under Meyers I and Meyers II. They found Cole-Rivera’s initial post was a solicitation implicitly aimed at inducing collective action to defend against Cruz-Moore’s criticism about their job performance, and the solicitation was motivated by Cruz-Moore’s threat to Cole-Rivera to make a complaint to the executive director. The social networking exchange was found to be the first step by the employees to take group action to defend themselves against allegations that they could reasonably believe Cruz-Moore

137. Id. at *10.
138. Id.
139. Id. at *2.
140. Id. at *10-11.
142. Id.
143. Id.
144. Id.
145. Id.
146. Id.
intended to present to the employer. The majority rejected Member Hayes’ dissenting view that the employees’ exchange was an unprotected electronic “group griping” session because the other employees did not know of Cruz-Moore’s threat to inform the executive director.

The majority in Hispanics United denied the employer’s defense premised upon its anti-bullying policy, finding that the at-issue posts cannot reasonably be construed as constituting bullying or harassment, and that the employer could not rely solely upon Cruz-Moore’s subjective reaction to the posts. In rejecting the defense, the NLRB did not rely upon the analysis in Atlantic Steel Co. because the employer contended that the postings were unprotected from the outset and Atlantic Steel Co. “typically applies when determining whether activity that is initially protected has been rendered unprotected by subsequent misconduct.”

The facts in Hispanic United did not require the NLRB to revisit the question of whether employees have an inherent statutory right under Section 7 of the NLRA to use employer computer equipment to solicit other employees through social media during non-work time. The at-issue posts were made off-duty and on personal computer equipment. The case also did not require the NLRB to decide under what circumstances an employer gaining access to employee social media posts constitutes unlawful surveillance or creates the impression of unlawful surveillance under the NLRA. The rapid growth of social networking renders it likely that the NLRB will face those provocative legal issues in future cases.

147. Hispanics United, 359 N.L.R.B. No. 37, at *10-11; but see Advice Memorandum from the NLRB Office of Gen. Counsel to Gail R. Moran, Reg’l Dir. of Region 13, JT’s Porch Saloon & Eatery, Ltd., No. 13-CA-46689 (July 19, 2011), available at http://mynlrb.nlrb.gov/link/document.aspx/09031d458055b9c6 (directing dismissal of an unfair labor charge because the posting exchange between the bartender and his step-sister regarding employer’s tipping policy was not discussed with other employees, none of his co-workers responded to the posts, and there had not been any effort to initiate group action concerning the tipping policy).

148. Hispanics United, 359 N.L.R.B. No. 37; but see Advice Memorandum, Wal-Mart, No. 17-CA-25030, supra note 127 (directing dismissal of a charge because the evidence established that employee’s social networking exchange with other employees concerning a particular Wal-Mart assistant manager was not a concerted activity because it was only his frustrated “expression of an individual gripe” rather than an effort to initiate group action).


150. Id.


152. Hispanics United, 359 N.L.R.B. No. 37, at *1.

153. See Frontier Tel. of Rochester, Inc., 344 N.L.R.B. 1270 (2005), enforced Frontier Tel. of Rochester, Inc. v. NLRB, 181 F. App’x 85 (2d Cir. 2006).
In *Bettie Page Clothing*, the NLRB held that Facebook posts by employees of a Haight Ashbury clothing store were protected concerted activity for three reasons. First, the posts were a continuation of their complaints to the employer concerning working late in an unsafe area. In addition, the posts were protected because they “were complaints among employees about the conduct of their supervisor as it related to their terms and conditions of employment and about management’s refusal to address the employees’ concerns.” Furthermore, the posts discussed consulting a book on California workplace rights, published by the Center for Labor Research and Education at the University of California, Berkeley, to determine whether their rights had been violated. In remedying the violation, however, the NLRB denied the request of the charging party for an order requiring the employer to purchase copies of the book and to distribute them to libraries and schools along with copies of the NLRB decision.

Due to the fact-specific analyses mandated by *Meyers I, Meyers II*, and *Atlantic Steel Co.*, interpretative differences will inevitably arise in future cases among NLRB Board members concerning the protected nature of social networking posts. There is little question that the particular composition of an NLRB Board can impact the analysis, values, and results in certain decisions, particularly those with hot button subjects. As one commentator has stated, “[t]he presidential appointed and highly political NLRB is well known to overrule its own decisions when its composition shifts due to a change in Presidential administration.”

Currently pending before the NLRB are exceptions and cross-exceptions from an ALJ decision in *Triple Play Sports Bar & Grille (Triple Play)*, which found that a sports bar violated §8(a)(1) of the NLRA when it terminated employees based upon the content of their posts on the social networking page of

---

155. *Id.* at *1.
156. *See David A. Rosenfeld, Miles E. Locker, & Nina G. Fendel, California Workers’ Rights: A Manual of Job Rights, Protections and Remedies* (4th ed. 2010). The connection between the book and the NLRB decision was discussed by Kerianne Steele, Esq. from Weinberg, Roger and Rosenfield during a panel discussion at the 2013 ABA National Symposium on Technology in Labor and Employment Law.
160. *Id.*
a former employee. Final resolution of this case may bring greater clarity with respect to the treatment of social networking under the NLRA.

The ALJ in *Triple Play* concluded that the employees’ posts were protected concerted activity because they grew out of prior employee discussions relating to complaints about their individual tax liabilities resulting from the employer’s treatment of their earnings, the content of the posts discussed what they intended to raise at an upcoming meeting called with the employer, and they discussed possible administrative remedies to explore. In reaching her decision, the ALJ did not find it significant that bar customers had access to the Facebook page, which was maintained by a former employee who participated in the exchange. The ALJ also found the content of the posts remained protected under the standards set forth in *Atlantic Steel Co.* noting that the comments did not take place at work, the subject of the posts related to their wages, and the content did not contain offensive language sufficient to remove them from protections under the NLRA.

The definition and application of the concepts “protected concerted activities” and “mutual aid and protection” are at the heart of NLRB precedent concerning social networking by employees. Whether NLRB precedent and analyses will be followed under public sector collective bargaining statues, however, will depend on how each public sector collective bargaining law was drafted and how it has been interpreted.

The next subsection examines precedent under collective bargaining and tenure statutes with respect to the scope of protections for social networking in three states: Michigan, Florida and New York.

162. *Id.*

163. *Id.*; *but see* Advice Memorandum from NLRB Office of Gen. Counsel to Daniel Hubbel, Reg’l Dir. of Region 17, Cox Commc’n. No. 17-CA-087612 (Oct. 19, 2012), available at http://mynlrb.nlrb.gov/link/document.aspx/09031d4580d6f53f (directing dismissal of an unfair labor charge alleging that an employer unlawfully terminated an employee because the employee’s Google+ posting was addressed at a customer and it contained vulgar words of language about the customer, which did not constitute protected concerted activity).

164. Three D, LLC, No. 34-CA-12915, 2012 WL 76862 (N.L.R.B. Div. of Judges Jan. 3, 2012). Legal problems might arise under the NLRA if a union or employer fails to carefully monitor and maintain its own social networking page against inappropriate posts. See Amalgamated Transit Union, Local Union No. 1433, AFL-CIO, Case No. 28-CB-78377 (N.L.R.B. Div. of Judges Nov. 28, 2012). In that case, an ALJ dismissed a portion of an unfair labor practice complaint against a union for allegedly violating § 8(b)(1)(A) of the NLRA based upon posts made by rank and file members, who were not union representatives, on the union’s social networking page threatening other employees with less favorable representation and physical harm based upon their failure to participate in an on-going strike. The ALJ rejected the NLRB Acting General Counsel’s contention that the union had an affirmative legal obligation to disavow the threatening comments because the mere posting did not make the union the speaker or publisher. The ruling, if affirmed by the NLRB Board, might have legal relevance for employers who maintain social media pages.
C. Protections for Social Networking Activities under Public Sector Laws

Social networking by government employees can be protected under collective bargaining laws, tenure statutes, and negotiated just cause provisions. Even when public sector collective bargaining is prohibited or merely permissive in a particular jurisdiction, public employees frequently have statutory due process protections or contractual rights limiting an employer’s authority to discipline.

Procedural protections against discipline in public employment are particularly important at a time when an off-duty post can go viral and lead to workplace repercussions. The existence of statutory and contractual protections against discipline is not a license for misconduct, incompetence, immaturity, or unprofessionalism. Rather, they constitute checks against arbitrary, unreasonable, or retaliatory governmental action. Such checks are essential in the government setting because, to paraphrase Madison, public officials and employees are not all angels.165

Although there have been judicial decisions resolving public employee electronic communicative misconduct cases, few decisions have been issued in Michigan, Florida, and New York concerning social networking as a protected activity under their respective public sector collective bargaining laws. Each state, however, has a body of administrative and judicial precedent delineating the contours of statutory liberties in their jurisdiction. Public sector collective bargaining laws and precedent can grant greater or narrower privileges and liberties than the NLRA. When those distinctions exist, federal precedent becomes far less relevant for determining the scope of protections for social networking in the public sector.

---

165. See The Federalist No. 51 (James Madison): “If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary.” As Diane Ravitch has explained concerning job security protections in the public sector:

“Tenure is not a guarantee of lifetime employment but a protection against being terminated without due process. It does not protect teachers from being laid off in a recession, nor does it protect them from being fired for incompetence. Why does due process matter? Teachers have been fired for all sorts of dubious and non-meritorious reasons: for being of the wrong race or religion, for being gay or belonging to some other disfavored group, for not contributing to the right politician, for not paying a bribe to someone or their job, for speaking out on an issue outside the classroom, for disagreeing with the principal, or simply to make room for a school board member’s sister, nephew, or brother-in-law.”

1. Michigan

Like the NLRA, the Michigan Public Employment Relations Act (MPERA)\(^{166}\) grants many public employees within the state a right to participate in union activities, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid and protection.\(^{167}\) MPERA was drafted based on the provisions of the NLRA, and NLRB precedent is considered when applying MPERA.\(^{168}\) The similarities with the NLRA are reflected in the wording of Section 423.209 of MPERA, which states:

> It shall be lawful for public employees to organize together or to form, join or assist in labor organizations, to engage in lawful concerted activities for the purpose of collective negotiation or bargaining or other mutual aid and protection, or to negotiate or bargain collectively with their public employers through representatives of their own choice.\(^{169}\)

Under MPERA, it is an unfair labor practice for a Michigan public employer ‘to interfere with, restrain or coerce public employees in the exercise of their rights guaranteed in [Section 423.209].”\(^{170}\)

To prove that an unfair labor practice has taken place in a mixed motive case, it must be demonstrated that protected concerted activity under MPERA was a motivating or substantial factor in the employer’s decision.\(^{171}\) If that is shown, the burden shifts to the employer to demonstrate that it would have taken the same action in the absence of the protected activity.\(^{172}\) The shifting burden approach under MPERA is clearly modeled upon NLRB precedent.\(^{173}\)

The decision by the Michigan Employment Relations Commission (MERC) in City of Detroit (Police Department)\(^{174}\) suggests how that agency might treat social networking as a protected activity under MPERA. In that case, MERC concluded that the employer violated MPERA when it ordered a police officer to discontinue operating an off-duty website that he, his fellow officers, and the

---

172. Id.
The police officer had created and maintained the website with his own funds for three purposes: to establish a web-based forum for police officers to express their views concerning departmental working conditions; to publish information for a wider audience about the City of Detroit’s municipal leadership; and to provide comic relief through publication of his own satirical fiction. While the website was not sanctioned or funded by his union, MERC found that it constituted a lawful concerted activity for mutual aid and protection because it was used, in part, to address work-related issues including wages, promotions, and discipline, and it provided a forum for officers to post comments. Although the website was used for other purposes with no direct connection to workplace conditions, MERC found that that content did not supersede MPERA protections unless the employer demonstrated that it had an adverse impact on the employer’s legitimate interests. With respect to the latter issue, MERC found that racist, sexist, and otherwise offensive statements posted on the website did not impact the employer’s interests because they were made off-duty and there was no evidence that they affected the performance of other officers.

In City of Detroit (Police Department), MERC applied an arguably broader approach to protected concerted activity than that applied under the NLRA. MERC’s analysis did not refer to the NLRA test under Meyers I and Meyers II for protected concerted activity and MERC did not expressly find that the website was aimed at initiating, inducing, or preparing for collective action about workplace conditions. In addition, unlike the NLRB decision in Karl Knauz, MERC rejected the employer’s claim that its actions were lawful because it was motivated by the unprotected portions of the posts under Michigan’s collective bargaining law. As discussed in Part II(B), supra, the NLRB dismissed the charge in Karl Knauz because the employer demonstrated

---

175. Id.
176. Id.
177. Id.
178. Id.
179. Id.
180. Id.
181. Id.; Cf. Ingham Cnty. v. Capitol City Lodge No. 141, 739 N.W.2d 95, 101 (Mich. Ct. App. 2007) appeal denied, 739 N.W.2d 95 (2007). (“According to the United States Court of Appeals for the Third Circuit, to qualify as a protected activity, ‘it must appear at the very least that it was engaged in with the object of initiating or inducing or preparing for group action or that it had some relation to group action in the interest of the employees.’”) (quoting Mushroom Transportation Co., Inc v. NLRB, 330 F.2d 683, 685 (3rd Cir. 1964)).
that the discharge was motivated by an unprotected post unrelated to workplace terms and conditions, rather than the employee social media comments about the sales event. The distinct approaches by MERC and the NLRB might reflect the constitutional civil liberties applicable only to public employees as well as the breadth of the city’s order to shut down the website, which implicates First Amendment protections against prior restraint. MERC’s analysis might have importance in future MPERA social networking cases because that medium’s culture frequently results in postings with content combining workplace issues with non-work topics, and between co-workers and individuals unconnected with the workplace.

An overly broad reading of City of Detroit (Police Department) must be tempered with consideration of two MERC decisions from 2012. In City of Detroit (Water & Sewage Dept), Meyers I and Meyers II were expressly cited in support of dismissing an unfair labor practice charge because the employee’s workplace complaint during a supervisory meeting to discuss the employee’s work performance was not a concerted activity even though the meeting was attended by a union representative. NLRB standards were applied again in Genesee Township Police Department to conclude that an e-mail sent by a laid-off employee to his union president and fellow laid-off employees urging them to join him in fighting against the layoffs was protected concerted activity for mutual aid and protection.

In general, employee comments made in the course of protected concerted activity that are rude, insulting, or offensive will retain their protections under MPERA unless the conduct is “so flagrant or extreme as to seriously impair the maintenance of discipline or render that individual unfit for future service.” Similarly, employee misconduct “in the course of concerted activity, including insubordination, is not beyond an employer’s right to discipline.” To determine whether employee conduct has gone beyond the pale and, therefore, lost statutory protections, MERC will examine the full context of the behavior including time, place, and audience.

The first MERC decision involving social media was Mid-Michigan Community College. In that case, the agency dismissed an unfair labor practice charge alleging that an at-will adjunct professor was discharged in

---

184. Id.
185. 26 MPER ¶ 3 (2012).
186. Id.
187. Id.
189. See id.
190. 26 MPER ¶ 4 (2012).
retaliation for meeting with union representatives about an organizing drive and by sending emails to the adjunct faculty and the college president announcing the campaign’s commencement.\textsuperscript{191} While the professor’s union organizing efforts were clearly protected under MPERA, the college was found to have not violated MPERA because its decision to discharge was motivated by the professor’s inappropriate and unprofessional Facebook posts concerning a student.\textsuperscript{192}

The scope of statutory protections under MPERA for employee’s use of employer equipment to distribute e-mail in the workplace is likely to be relevant in future social networking cases. In \textit{City of Saginaw},\textsuperscript{193} MERC affirmed an ALJ’s decision finding an employer violated MPERA when it disciplined a police officer for sending a group e-mail through the employer’s computer system criticizing the employer for engaging in bad faith bargaining, and making a negative reference to the city manager’s relationship with a public administrator’s organization.\textsuperscript{194} The e-mail was found to be protected concerted activity because it discussed the employer’s conduct during negotiations, and the reference to the city manager was in the context of the discussion concerning negotiations.\textsuperscript{195} Finally, MERC found the discipline to be discriminatory under MPERA because other employees were permitted to send non-work related emails through the system, and the union used the system to send e-mails to its members.\textsuperscript{196}

Well before the development of Web 2.0, the Michigan Supreme Court recognized that the state’s civil service law provides general protections for employees to engage in lawful off-duty activities:

[The Civil Service Commission’s] power does not extend, however, to the blanket prohibition of off-duty activities, political or otherwise, as a matter of policy simply because such activities may conceivably interfere with satisfactory job performance. What an employee does during his off-duty hours is not of proper concern to the Civil Service Commission unless and until it is shown to adversely affect job performance. Even then the commission’s authority is not to curtail the off-hours activity, it is to deal with the adequacy of job performance. Certainly, it is within contemplation that off-duty political involvement may adversely affect a classified employee’s performance at work. If

\begin{itemize}
  \item \textsuperscript{191} Id.
  \item \textsuperscript{192} Id.; see also Rodriguez v. Wal-Mart Stores, No. 3:11–CV–2129–B, 2013 WL 102674, at *6 (N.D. Tex. 2013) (supervisor’s criticism of subordinates in social media posts constituted a legitimate nondiscriminatory reason for her termination because it violated the employer’s policy).
  \item \textsuperscript{193} 23 MPER ¶ 106 (2010).
  \item \textsuperscript{194} Id.
  \item \textsuperscript{195} Id.
  \item \textsuperscript{196} Id.
\end{itemize}
and when it does, the commission is empowered to deal with such circumstances on a case-by-case basis.197

Tenure protections for lawful off-duty activities can extend far afield from political and civic engagement. In 2007, a Michigan teacher was terminated after photographs were posted on a website showing her engaged in oral sex with a male mannequin during an off-duty 2005 party.198 The photographs were taken during the party without the teacher’s knowledge and posted on the website without her consent.199 As would be expected, news within the school spread rapidly resulting in some industrious students abandoning their studies for peeks at the photographs.200 Although the photographs were removed from the website at the teacher’s insistence, the school district terminated her for engaging in lewd behavior that undermined her moral authority and professional responsibility.201 Upon review, the State Tenure Commission reversed the discharge on the grounds the event took place at a private party two years earlier with no students present, the conduct was not illegal, it did not have any nexus to school activities, and it was not related to her pedagogical responsibilities.202 Despite the negative publicity caused by the posting of the photographs, the State Tenure Commission concluded that it was insufficient to demonstrate just and reasonable cause under Michigan’s teacher tenure law.203

In 2011, the Michigan legislature lessened the standard for terminating a tenured teacher from just and reasonable cause to “a reason that is not arbitrary and capricious.”204 This modification may well affect future Michigan teacher disciplinary cases involving employer reactions to social networking activities.

199. Id.
200. Id.
201. Id.
202. Id.
203. Id. In contrast, the discharge of an Ohio high school mathematics teacher was upheld by an arbitrator under contractual just cause and progressive discipline provisions after the teacher’s estranged wife posted obscene nude photographs of him on websites and on a popular social media page. The arbitrator upheld the termination because high school students were able to access the photographs thereby undermining the teacher’s role model status and his credibility. The arbitrator criticized the teacher for failing to secure the photographs, from failing to take appropriate legal action in response to his estranged wife’s threats, and in failing to warn his principal of the potential release of the photographs. Warren Cnty. Bd. of Educ., 124 Lab. Arb. Rep. (BNA) 532 (2007) (Skulina, Arb.).
that are not protected concerted activity under that state’s collective bargaining law.

2. Florida

Unlike Michigan and New York, the Florida state constitution includes an explicit right of public employees to bargain collectively:

The right of persons to work shall not be denied or abridged on account of membership or non-membership in any labor union or labor organization. The right of employees, by and through a labor organization, to bargain collectively shall not be denied or abridged. Public employees shall not have the right to strike.205

Under the state constitutional provision, Florida public employees have a right to collectively bargain like private sector employees, but without the right to strike.206 Florida precedent recognizes that due to the inherent differences between public and private sector collective bargaining, it is impractical to adopt, in whole, analogous private sector precedent.207

Florida’s public sector collective bargaining statute, like Michigan’s law, is modeled after the NLRA. Section 447.301 of the Florida Public Employees Relations Act (FPERA) states:

Public employees shall have the right to engage in concerted activities not prohibited by law, for the purpose of collective bargaining or other mutual aid or protection. Public employees shall also have the right to refrain from engaging in such activities.208

The Florida Public Employees Relations Commission (FPERC) has concluded that the state legislature intended for FPERA to grant public employees “a very broad scope of protection” for any concerted activity relating to employees’ employment relationship.209 This construction is premised, in part, on FPERA’s free speech clause, which states:

Notwithstanding the provisions of subsections (1) and (2), the parties’ rights of free speech shall not be infringed, and the expression of any arguments or opinions shall not constitute, or be evidence of, an unfair

206. Dade Cnty. Classroom Teachers Ass’n, Inc. v. Ryan, 225 So. 2d 903 (Fla. 1969); Dade Cnty. Classroom Teachers Ass’n, Inc. v. Legislature, 269 So. 2d 684 (Fla. 1972).
209. City of N. Port, 15 FPER ¶ 20179 (1989) (quoting City of Venice, 4 FPER ¶ 4059, at 130 (1978)).
employment practice or of any violation of this part, if such expression contains no promise of benefits or threat of reprisal or force."  

This statutory free speech clause might form the legal basis for public employees in Florida to have greater protections for social networking than employees in other states.

To demonstrate that an employer violated FPERA through an adverse personnel action, a preponderance of evidence must be presented proving that the conduct was protected and it was a substantial and motivating factor in the employer’s decision. If the employer was motivated by an impermissible reason under FPERA, the burden shifts to the employer to demonstrate that it would have taken the same adverse action anyway. Like Michigan, Florida’s shifting burden standard is analogous to the standard applied under the NLRA.

In order for conduct to be protected under FPERA, it must be concerted in nature. The applicable test for determining that issue is whether it was for “the well-being of fellow employees.” Unlike NLRB precedent, in order for a contract grievance to be protected under FPERA, it has to seek more than personal benefits for the grievant or it must have been “prepared in collaboration with or on behalf of employees other than himself.” In Florida, personal complaints about work or a supervisor do not constitute protected concerted activity. As a result, “criticism for ‘criticism’s sake’” is treated as mere griping and not an effort to obtain a remedy over wages, hours, and other terms and conditions. Therefore, content of an employee’s social networking posts limited to venting about workplace issues will not be found protected under FPERA.

In one case, FPERC concluded that a police union president engaged in protected concerted activity when his two articles were posted on the union’s website discussing contract issues, which contained disparaging, belittling, and

212. Id.
213. City of Cape Coral, 39 FPER ¶ 185 (2012) (quoting City of Venice, 4 FPER ¶ 4059 (1978)).
214. City of Mount Dora, 8 FPER ¶ 13260 (1982).
215. Id.
insubordinate statements about the sheriff’s chief deputy. The agency’s
decision was based upon prior precedent concluding that Florida’s state
collective bargaining law mandated a “very high degree of protection for speech
uttered in the context of public sector labor-management relations.”

When a Florida public employee engages in speech or an activity that is
libelous, coercive, physically threatening, or “creates a real threat of immediate
disruption in the workplace,” it will be found to be unprotected. Similarly,
“[i]nsubordinate behavior, including a verbal act, that creates a real threat of
disruption in the workplace is not protected even if the employee acts in concert
with others.” As a result, Florida public employees, like their private sector
counterparts under NLRA, need to apply self-restraint in the manner in which
they engage in concerted activities in cyberspace to avoid losing protections
under FPERA.

Finally, the scope of protected activities between public employees during
working hours is constrained by a particular provision in FPERA. It is
unlawful for a union or its members to engage in solicitation during working
hours or to distribute literature during working hours in areas where work is
performed except during an employee’s lunch hour or in areas not specifically
devoted to performance of official duties. Based upon those restrictions,
FPERC dismissed a charge alleging that an employer engaged in an unfair labor
practice when it disciplined a union official for sending an e-mail from his
personal account while on vacation to sheriff’s employees at their work e-mail
addresses. The e-mail urged the employees to vote against a pending labor
agreement negotiated by an incumbent union and encouraged them to join his
competing union.

3. New York

The scope of statutory protections for employee activities under New York’s
Public Employees’ Fair Employment Act, commonly referred to as the Taylor

---

(per curiam).
220. Dist. Bd. of Tr. of Palm Beach Junior Coll., 11 FPER ¶ 16101, at 327 (1985), aff’d, Dist.
Bd. of Tr. of Palm Beach Junior Coll. v. United Faculty of Palm Beach Junior Coll., 489 So. 2d
221. Palm Beach Junior Coll. 11 FPER ¶ 16101; Miami Ass’n of Fire Fighters, 11 FPER ¶
222. Palm Beach Gardens, 17 FPER ¶ 22052.
223. Fla. STAT. § 447.509(1)(a).
224. Id.
226. Id.
Law, is more limited than protections under the NLRA, MPERA, and FPERA.\textsuperscript{228} Unlike those statutes, the Taylor Law does not protect public employees who engage in concerted activities for mutual aid and protection unrelated to forming, joining or participating in a union.

Section 202 of the Taylor Law states:

\begin{quote}
Public employees shall have the right to form, join and participate in, or to refrain from forming, joining, or participating in, any employee organization of their own choosing.\textsuperscript{229}
\end{quote}

Under Section 203 of the Taylor Law, New York public employees are guaranteed the right to be represented by a union in collective bargaining with their public employers over terms and conditions of employment, and in the administration of grievances under a negotiated agreement.\textsuperscript{230} All public employees and their unions covered by the Taylor Law are prohibited from engaging in strikes or condoning strikes.\textsuperscript{231}

An employer engages in an improper practice in violation of Sections 209-a.1(a) and (c) of the Taylor Law\textsuperscript{232} when its conduct is unlawfully motivated by a protected activity under that law. To prove such a violation, it must be demonstrated by a preponderance of evidence that: the charging party engaged in a protected activity under the Taylor Law; such activity was known to the person or persons taking the employment action; and the employment action would not have been taken “but for” the protected activity.\textsuperscript{233} If a prima facie case of improper motivation is demonstrated, the employer must demonstrate that it was motivated by a legitimate nondiscriminatory reason, which is subject to

\begin{enumerate}
\item[228.] \textit{See} Cnty. of Tioga, 44 NYPERB ¶ 3016 (2011); Love Canal Area Revitalization Agency (Bannister), 28 NYPERB ¶ 3040 (1995).
\item[229.] N.Y. CIV. SERV. LAW §§ 200-214 (McKinney 2002).
\item[230.] \textit{Id.}
\item[231.] \textit{Id.}; N.Y. CIV. SERV. LAW § 210(1) states: “No public employee or employee organization shall engage in a strike, and no public employee or employee organization shall cause, instigate, encourage, or condone a strike.”
\item[232.] \textit{Id.}; N.Y. CIV. SERV. LAW § 209-a.1 states in relevant part that: “It shall be an improper practice for public employer or its agents deliberately (a) to interfere with, restrain or coerce public employees in the exercise of their rights guaranteed in section two hundred two of this article for the purpose of depriving them of such rights; and (c) to discriminate against any employee for the purpose of encouraging or discouraging membership in, or participation in the activities of, any employee organization.”
\end{enumerate}
rebuttal. Notably, the shifting burdens under the Taylor Law are distinct from those applied in similar cases under the NLRA, MPERA, and FPERA.

The lack of mutual aid and protection language in Section 202 of the Taylor Law is substantive, and substantially limits the relevance of NLRB case law concerning whether social media posts by unrepresented employees is a protected concerted activity. In fact, the Taylor Law expressly mandates that “fundamental distinctions between private and public employment shall be recognized, and no body of federal or state law applicable wholly or in part to private employment, shall be regarded as binding or controlling precedent.”

In Rosen v. New York Public Employment Relations Board, the New York Court of Appeals sustained an administrative determination by the New York State Public Employment Relations Board (NYPERB) that a community college teacher who presented grievances on behalf of herself and a group of other employees to the associate dean did not engage in a protected activity under the Taylor Law because there was no evidence that the teachers were in a union, were seeking to form a union, or were being represented by one. The Rosen holding demonstrates that, in contrast to the standard set forth in Meyers I and Meyers II, a New York public employee “bringing truly group complaints to the attention of management” is unprotected unless the complaint is related to forming, joining or participating in a union.

In determining the limited breadth of protections under Section 202 of the Taylor Law, the Court of Appeals compared that Taylor Law provision with the wording of Section 7 of the NLRA:

Conspicuously absent from the formulation of a public employee’s right to organize in section 202 is the additional right guaranteed in the NLRA “to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection.” We conclude from the otherwise parallel terminology in each provision that the Legislature, by omitting from section 202 of the Taylor Law the additional reference to “concerted activity”, intended to afford a public employee only the right to form, join or participate in an employee organization. Because the Legislature has by its definition restricted the reach of section 202, it must not have intended for section 202 to

234. Id.
237. N.Y. CIV. SERV. LAW §§ 209-216.
240. Rosen, 526 N.E.2d at 29.
protect precisely the same broad range of employee activity as is protected under section 7 of the NLRA.\(^{242}\)

The same statutory distinction between the Taylor Law and the NLRA was relied upon in *New York City Transit Authority v. New York Public Employment Relations Board* \(^{243}\) in overturning a NYPERB decision that found New York public employees had an implicit statutory right under Section 202 of the Taylor Law to union representation during a disciplinary interview. In reaching its decision, the court cited the fact that a private sector right to representation during a disciplinary interrogation under the NLRA was upheld by the U.S. Supreme Court in *NLRB v. J. Weingarten, Inc* \(^{244}\) based upon that statute’s protection for engaging in concerted activities for mutual aid or protection.\(^{245}\)

In the absence of mutual aid and protection language in the Taylor Law, New York public employee social networking activities must be related to forming, joining, or participating in a union in order to be protected.\(^{246}\) New York’s public sector union density rate was 73% in New York in 2011-12,\(^{247}\) but that statistic does not reveal the percentage of union members who participate in union activities, including union-sponsored cyberspace initiatives. It is reasonable to speculate, however, that the vast majority of union members engage in social networking primarily for personal purposes unrelated to any activity that would fall under the protections of Section 202 of the Taylor Law.

NYPERB examines “the totality of all relevant circumstances, with a focus upon the purpose and effect of that activity,”\(^{248}\) in deciding whether a particular activity is protected. In *County of Tioga*,\(^{249}\) it described the types of employee activities protected by the Taylor Law:

Employee statements and actions that are organized, prompted or encouraged by an employee organization will, in general, be found to be protected concerted activity for purposes of the [Taylor Law]. The wide scope of protected concerted activities under the [Taylor Law] includes statements and activities by a unit employee as part of an employee organizational activity, relates to an employee organization

---

244. 420 U.S. 251 (1975).
246. Cnty. of Tioga, 44 NYPERB ¶ 3016 (2011).
249. 44 NYPERB ¶ 3016 (2011).
policy, involves employee organizational representation or stems from a dispute emanating from a collectively negotiated agreement.250

Under that standard, electronic comments on a union-run social media page will generally be found to be protected under the Taylor Law. Similarly, e-mail encouraging members to engage in protected activities or that discusses a pending grievance is generally protected. While purely partisan political activity by non-policymaking public employees is subject to First Amendment protections,251 it is not protected under the Taylor Law.252

Otherwise protected conduct can be found to be unprotected under the Taylor Law if objective evidence demonstrates, under the totality of the circumstances, that it was overzealous, confrontational, and actually disruptive.253 To prove that defense, an employer must introduce “objective evidence of disruption emanating from the conduct. It cannot rely upon a mere prediction of disruption or a workplace disruption caused by its own overreaction to the at-issue conduct.”254 As will be demonstrated in Part III, the requirement that actual disruption take place in order to lose statutory protections is a more rigorous standard than the one applied under the First Amendment.

Inaccurate employee statements are protected under the Taylor Law regardless of whether employer representatives are disturbed, unless it is proven that the inaccuracies were deliberate and intended to falsify, or were maliciously aimed at injuring the employer. Grievances and contract claims are protected under the Taylor Law unless an employer demonstrates that they are undeniably frivolous.255 A union, however, “has no protected right to use for its benefit information about students obtained by a teacher in the course of his official activities.”256 Therefore, the posting of student information on a union social media page may constitute an unprotected activity under the Taylor Law.

In State of New York (Division of Parole),257 NYPERB rejected an employer’s claim that a shop steward’s off-duty e-mail, which encouraged unit members to report to work on a holiday to test a contractual argument, was unprotected. NYPERB concluded that the e-mail could not be reasonably

---

250. Id.
251. infra Part IV(A).
257. 41 NYPERB ¶ 3033 (2008).
construed as seeking to disrupt, confront, or to instigate an unprotected protest.258 In contrast, NYPERB found in State of New York (Public Employees Federation)259 that an employer did not violate the Taylor Law when it blocked a union activist’s access to its e-mail system, because it was motivated by the activist’s insubordination for refusing to stop sending controversial blast e-mails to union members relating to budgetary and collective bargaining issues.260

Public employees in New York have other possible statutory protections for social networking activities. New York Labor Law § 201-d prohibits, in general, workplace discrimination and retaliation against employees who engage in off-duty political or recreational activities.261 Neither Michigan nor Florida has a similar statute. Presumably, off-duty social networking using a personal device would satisfy the definition of a recreational activity under New York Labor Law § 201-d(1)(b).262 While courts have not yet decided the applicability of the statute to social networking, the law explicitly excludes protections for any activity that takes place on the employer’s premises or with the use of employer equipment and property.263 It also excludes conduct that creates a conflict of interest or constitutes a violation of applicable public sector ethical rules and limitations.264

Many public employees in New York are entitled to statutory due process protections against discipline or are subject to negotiated disciplinary arbitration provisions.265 There have been three New York court decisions that reviewed disciplinary actions taken against public employees based upon their on-line behavior. All three decisions were issued in the context of judicial review of

258. Id.
260. Id.
262. N.Y. LABOR LAW § 201(d)(1)(b) (McKinney 2009) states: "Recreational activities’ shall mean any lawful, leisure-time activity, for which the employee receives no compensation and which is generally engaged in for recreational purposes, including but not limited to sports, games, hobbies, exercise, reading and the viewing of television, movies and similar material.” Cf. State v. Wal-Mart Stores, Inc., 207 A.D.2d 150 (N.Y. App. Div.1995) (holding that a dating relationship does not satisfy the definition of a recreational activity under the statute).
263. N.Y. LABOR LAW § 201(d)(2)(a).
264. Id. at d(3)(a)-(d).
statutorily mandated disciplinary procedures. Absent from the decisions are facts explaining the allure of the electronic medium for unfiltered thoughts, feelings, and conduct.

In *City School District of the City of New York v. McGraham*, 266 New York courts at every level grappled with the appropriateness of the arbitral disciplinary penalty imposed on a tenured high school teacher found guilty of serious misconduct for the content of her electronic communications with and about a 15-year old student. 267 During the arbitration, the evidence established that the teacher provided the student with her personal e-mail address, and frequently communicated electronically with him after school about cultural and personal issues. 268 Although she never acted upon her feelings, the communicative exchanges and her anonymous blog entries demonstrated feelings that went well beyond those appropriate for a teacher-student relationship.

Despite the seriousness of her misconduct, the arbitrator imposed a ninety-day suspension without pay and directed that the teacher be assigned to another school. 270 In deciding that the discharge was inappropriate, the arbitrator considered the teacher’s remorse when confronted with the allegations, her cessation of communications with the student, the abandonment of her personal blog, and the fact she obtained professional therapy to heal the emotional issues that led to her misconduct. 271 Efforts by the school district to have the arbitral penalty vacated, as violative of public policy, were unsuccessful. The unanimous New York Court of Appeals concluded that, regardless of the facts in a particular case, the broad public policy favoring protection of children did not constitute an absolute mandate requiring vacatur of an arbitral penalty short of discharge. 272

In a second teacher misconduct case, an intermediate appellate court affirmed the judicial vacatur of the discharge of a New York City tenured teacher for making inappropriate off-duty Facebook posts after the drowning death of a school district student. 273 In one post, the teacher stated: “After today, I am thinking the beach sounds like a wonderful idea for my 5th graders! I

---

266. 958 N.E.2d 897 (N.Y. 2011).
267. Id.
268. Id. at 898.
269. Id.
270. Id.
271. Id.
HATE THEIR GUTS! They are the devils [sic] spawn!” She also answered a responsive post from a Facebook friend by indicating that she would not throw a life jacket to a drowning student. The termination imposed by the arbitrator was set aside based upon the teacher’s unblemished 15-year career, the posts were made off-duty following a difficult day at school, they were deleted three days after they were posted, students and parents were not on-line friends of the teacher, and the comments did not impact her ability to teach and did not harm her students.

In the third case, New York courts sustained the discharge of a Fire Department emergency medical services supervisor and lieutenant, who posted on his Facebook page a photograph of a computer screen containing the name, address, and confidential medical information of a female caller, which was accessible to hundreds of his Facebook friends. At the time of the posting, the lieutenant knew that the disclosure of patient information violated departmental rules and was a breach of trust.

To discourage employee misconduct and ensure that the benefits of social media outweigh the potential harm, many departments and agencies are developing social media policies that distinguish between official and personal. Private sector employers are also imposing social media policies to avoid commercial harm, the disclosure of confidential information, and the creation of a discriminatorily hostile work environment, and for other business reasons. The content of workplace policies can also limit the scope of privacy

---

274. Id.
275. Id.
276. Id.
protections employees may have with respect to the content of their social media pages under applicable law.280

Constructing the proper balance in a social networking policy can be as difficult as drafting a general internet use policy.281 Both forms of policies can alienate productive employees, and might adversely impact recruitment of younger employees raised in the culture of social networking. The right to implement and apply such workplace policies, however, is subject to legal restrictions under the NLRA and analogous laws in Michigan, Florida, and New York, particularly when it places limitations upon an employee’s off-duty conduct. We shall now turn to those statutory restrictions, beginning with the NLRA.

III. THE LAWFULNESS OF EMPLOYER SOCIAL MEDIA POLICIES

A. Policies that Chill Protected Concerted Activities under the NLRA

Although media attention regarding the NLRB case from New Haven focused on the lawfulness of terminating an employee based upon Facebook postings, an issue of wider significance in that case was the allegation that the company’s written workplace rules were overbroad and tended to chill the liberty of employees “to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection” under Section 7 of the NLRA.282 Whether maintenance of a particular workplace policy violates Section 8(a)(1) of the NLRA will depend upon the specific content of each particular policy and rule.

The lawfulness of employer policies under Section 8(a)(1) of the NLRA was the subject of the first two 2012 NLRB Board decisions relating to social media. In Costco,283 it held that certain workplace policies maintained by Costco violated Section 8(a)(1) of the NLRA because its employees would reasonably construe those policies as prohibiting or restricting activities protected by Section 7 of the NLRA.284 Among the policies found to violate Section 8(a)(1) of the NLRA was a provision of the employee handbook entitled “Electronic Communications and Technology Policy,” which stated in part:

281. Herbert, supra note 154, at 63.
284. Id.
Any communication transmitted, stored or displayed electronically must comply with the policies outlined in the Costco Employee Agreement. Employees should be aware that statements posted electronically (such as online message boards or discussion groups) that damage the Company, defame any individual or damage any person’s reputation, or violate the policies outlined in the Costco Employee Agreement, may be subject to discipline, up to and including termination of employment.285

In Costco, the NLRB concluded the policy’s broad prohibition against communications that “damage the Company, defame any individual or damage any person’s reputation” implicitly includes employee statements and activities protesting workplace conditions.286 In reaching that conclusion, the agency noted that “there is nothing in the rule that even arguably suggests that protected communications are excluded from the broad parameters of the rule.”287 In finding the work rule violated Section 8(a)(1) of the NLRA, the NLRB reversed a contrary conclusion by an ALJ who found that employees would not reasonably interpret the rule as restricting or inhibiting Section 7 activities; rather, the ALJ concluded that employees would reasonably infer that it was a workplace civility rule.288

Prior to Costco, there was established NLRB precedent concerning whether maintenance of particular work rules violate Section 8(a)(1) of the NLRA.289 Under that case law, if an employer maintains an explicit rule restricting employees from engaging in activities protected under Section 7 of the NLRA, the rule is unlawful.290 Therefore, an employer’s rule expressly prohibiting employees from discussing terms and conditions of employment with each other through social media would be unlawful. Even if a workplace rule is not explicit, it still can be found to violate Section 8(a)(1) of the NLRA, “upon a showing of one of the following: (1) employees would reasonably construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response

285. Id.
286. Id.
287. Id.
288. Id.
290. See Lutheran Heritage Village-Livonia, 343 N.L.R.B. at 646.
to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights.291

The primary issue in NLRB decisions concerning the lawfulness of an employer policy under Section 8(a)(1) is whether it contains a work rule that would be reasonably construed by the employees as restricting them from engaging in protected activities under Section 7 of the NLRA. In determining whether a particular rule would chill protected activities, the rule will be read in context of the policy and without a strained construction of its language.292 Broad ambiguous restrictions may be found to violate the NLRA unless the rule contains clarifying language about its inapplicability to the rights and liberties protected by Section 7 of the NLRA or sets forth a list of examples of unprotected conduct that would lead a reasonable employee to conclude that the rule does not restrict NLRA protected activity.293

Applying those standards, the NLRB in Costco affirmed the ALJ’s dismissal of a separate allegation in the complaint that the “appropriate business decorum” provision in the following section of the same electronic communication policy did not violate Section 8(a)(1) of the NLRA because employees would not reasonably conclude that it restricted their rights to engage in concerted activities:

Costco recognizes the benefits associated with electronic communications for business use. All employees are responsible for communicating with appropriate business decorum whether by means of e-mail, the Internet, hard-copy, in conversation or using other technology or electronic means. Misuse or excessive personal use of Costco technology or electronic communications is a violation of Company policy for which you may be disciplined, up to and including termination of employment. Your use of Costco technology and electronic communication systems represents your agreement with the following policies.294

291. Lutheran Heritage Village-Livonia, 343 N.L.R.B. at 646-47; Lafayette Park Hotel, 326 N.L.R.B. at 825 (“The appropriate inquiry is whether the rules would reasonably tend to chill employees in the exercise of their Section 7 rights. Where the rules are likely to have a chilling effect on Section 7 rights, the Board may conclude that their maintenance is an unfair labor practice even absent evidence of enforcement.”) (citations omitted). See also Flex Frac Logistics, LLC, 358 N.L.R.B. No. 127, 2012-13 NLRB Dec. ¶ 15615, at *2 (Sept. 11, 2012) (“Board law is settled that ambiguous employer rules—rules that reasonably could be read to have a coercive meaning – are construed against the employer. This principle follows from the Act’s goal of preventing employees from being chilled in the exercise of their Section 7 rights whether or not that is the intent of the employer . . . .”).


293. See supra note 283.

In *Karl Knauz*, the NLRB affirmed an ALJ’s conclusion that maintenance of the following workplace rule violated Section 8(a)(1) of the NLRA:

> (b) Courtesy: Courtesy is the responsibility of every employee. Everyone is expected to be courteous, polite and friendly to our customers, vendors and suppliers, as well as to their fellow employees. No one should be disrespectful or use profanity or any other language which injures the image or reputation of the Dealership.

The NLRB majority concluded that the prohibition against “disrespectful” conduct and “language which injures the image or reputation” of the employer can be reasonably interpreted to encompass activities protected by Section 7 of the NLRA. It found that statements objecting to working conditions or seeking support for improvement in those conditions might run afoul of the employer’s rule. As part of its analysis concerning the chilling effect of the rule, the Board majority echoed the reasoning in *Costco* by highlighting that “there is nothing in the rule, or anywhere else in the employee handbook, that would reasonably suggest to employees that employee communications protected by Section 7 of the Act are excluded from the rule’s broad reach.”

In dissent, member Hayes criticized the majority’s construction of the at-issue rule, alleging that the majority read the words and phrases in isolation and departed from prior Board precedent. The interpretative differences in *Karl Knauz* between the majority and member Hayes are bound to be replicated in future NLRB decisions for a number of reasons: the wide variations in workplace policies among employers; the reasonableness standard applied in these cases when interpreting employer policies; and the distinct analytical approaches applied by different NLRB Board members. The pending litigation concerning the recess appointments of NLRB Board members who participated in *Costco* and *Karl Knauz* could result in the cases being reexamined by a differently constituted NLRB Board.

In addition to the two NLRB Board decisions there have been ALJ decisions and NLRB General Counsel advice memoranda addressing the legality of particular social media policies maintained by private employers. Prior to the decisions in *Costco* and *Karl Knauz*, three ALJ decisions addressed whether particular social media policies violated Section 8(a)(1) of the NLRA because employees would reasonably construe the policy to prohibit protected speech and

---

296. *Id.*
297. *Id.*
298. *Id.*
299. *Id.*
300. *Id.*
activities under the Section 7 of the NLRA. Although some of the ALJs’ conclusions are now in question following the decisions in Costco and Karl Knauz, they illustrate the legal issues that arise concerning social media and internet policies under the NLRA.

In one case, the ALJ dismissed a complaint’s allegation that an employer’s internet policy stating that an employee may be subject to discipline for “engaging in inappropriate discussions about the company, management and/or co-workers” violated Section 8(a)(1) of NLRA. Relying upon the NLRB’s decision in Tradesmen International, the ALJ found that the rule was lawful because it sought to restrict speech similar to restrictions on speech having a potentially detrimental impact on the employer, which the Board has found to be permissible. The construction of the rule by the ALJ was based, in part, on its context within the full policy:

This conclusion is supported by the context of the allegedly unlawful segment of the policy. The policy begins by stating that Respondent “supports the free exchange of information” among its employees, and states that only when electronic communications “extend to confidential and proprietary information” or “inappropriate discussions” would they potentially be subject to disciplinary action. Immediately following that statement is a requirement that employees clearly identify opinions they share regarding Respondent as their own, as opposed to those of Respondent. The policy closes by stating that it will have no effect to the extent it conflicts with state or federal law. Under the case law discussed above, I find that in this context the prohibition on “inappropriate discussions about the company, management and/or co-workers” would not be reasonably construed as restricting Section 7 activity.

In G4S Secure Solutions (USA), Inc., an ALJ concluded that a social media policy maintained by a security services employer prohibiting commenting on “work-related legal matters” without permission violated Section 8(a)(1) of the NLRA. The ALJ reasoned that the rule failed to define the phrase “legal matters,” and would be reasonably interpreted by employees as

---

302. Tradesmen Int’l, 338 N.L.R.B. 460 (2002); see also Ark Las Vegas Rest. Corp., 335 N.L.R.B. 1284, n.2 (2001) (finding that employer rules prohibiting on-duty or off-duty employee conduct, which discredits or damages employer or co-workers are not unlawful under the NLRA).
304. Id.
306. Id.
prohibiting them from discussing lawsuits and administrative complaints about workplace conditions through social media.\textsuperscript{307}

The ALJ dismissed, however, the claim that another social media rule restricting the posting of photographs, images, and videos of employees in uniform did not violate Section 8(a)(1) of the NLRA because the employer had legitimate business reasons tied with patient privacy concerns in providing and avoiding the adverse business consequences caused by broad distribution of images of uniformed employees engaged in unprofessional conduct.\textsuperscript{308} In reaching her finding, the ALJ relied, in part, on Flagstaff Medical Center,\textsuperscript{309} in which an NLRB Board majority upheld an employer’s work rule prohibiting the use of cameras during work time to record images of patients or hospital equipment and property. In Flagstaff Medical Center, NLRB Chairman Pearce dissented, stating that he would find a violation based upon the employer’s maintenance of the ban because it would tend to restrain employees from engaging the concreted activity of documenting unsafe working conditions through photographic images.\textsuperscript{310}

In a third case, General Motors, LLC,\textsuperscript{311} an ALJ rejected an employer’s argument that its policy did not run afoul of Section 8(a)(1) because it included an explicit disclaimer that it will be enforced consistent with applicable laws including the NLRA. With respect to the specifics of the policy, the ALJ concluded that maintenance of the following elements of the policy violated Section 8(a)(1) of the NLRA: an explicit prohibition against employees discussing the performance and compensation of co-workers on public social networking sites; the requirement that posts be “completely accurate” and “not misleading”; the obligation of employees to consult with the company regarding whether particular information is covered by the policy; and the prohibition against posting photographs and personal information of others without their consent.\textsuperscript{312} The ALJ found, however, that the policy’s suggestions that employees “treat everyone with respect,” and “to think carefully about friending co-workers” were lawful because they were advisory in nature, rather than a rule that could be the basis for discipline.\textsuperscript{313}

Following Costco and Karl Knauz, there have been two ALJ decisions concerning the lawfulness of employer social media policies under the NLRA.
In *Echostar Technologies, LLC*, the ALJ concluded that maintenance of the following social media rule in the employee handbook violated the NLRA:

(i) You may not make disparaging or defamatory comments about EchoStar, its employees, officers, directors, vendors, customers, partners, affiliates, or our, or their, products/services; and

(ii) Unless you are specifically authorized to do so, you may not: Participate in these activities with EchoStar resources and/or on Company time . . . .

Citing *Costco*, the ALJ concluded that prohibition against “disparaging” improperly intruded upon rights guaranteed by Section 7 of the NLRA even when the term is read in the context of other phrases such as “[r]emember to use good judgment.” The employer’s reliance upon the following introductory handbook disclaimer and offer of assistance was rejected because it would not lessen the chill in a reasonable employee caused by the offending social media rule:

Should you have questions about the Handbook, please contact the Human Resources Department.

Should a conflict arise between an EchoStar policy and the law, the appropriate law shall be applied and interpreted so as to make the policy lawful in that particular jurisdiction.

In another decision, an ALJ relied upon *Costco* and *Karl Knauz* to find that a social media policy prohibiting employees from making “disparaging or defamatory comments” about the employer and its employees and prohibited negative electronic discussions during “Company time” violated Section 8(a)(1) of the NLRA.

---

315. *Id.*
316. *Id.*
317. *Id.*
318. *Dish Network Corp.*, Nos. 16-CA-62433, 16-CA-66142 & 16-CA-68261, 2012 WL 5564372 (N.L.R.B. Div. of Judges, Nov. 14, 2012). In an advisory memorandum, issued following *Costco* and *Karl Knauz*, the Division of Advice found that an employer’s social media policy was not overbroad because it included sufficient examples of prohibited activities so that an employee would not reasonably believe that it prohibits protected activities under the NLRA. Attached to his third memorandum concerning employer social media policies, the Acting General Counsel attached the final version of Wal-Mart’s revised social media policy, which was found to be lawful. *See Memorandum from the NLRB Office of Gen. Counsel (OM 12-59), Report of the Acting General Counsel Concerning Social Media Cases, 22-24 (May 30, 2012), available at http://mynlrb.nlrb.gov/link/document.aspx/09031d4580a375cd.*
In *Walmart*, the NLRB General Counsel’s Division of Advice found an employer’s social media policy prohibiting “inappropriate postings that may include discriminatory remarks, harassment and threats of violence or similar inappropriate or unlawful conduct” to be lawful because it provided examples of egregious and unlawful conduct covered under the rule so that a reasonable employee, reading the rule in context, would understand that it does not prohibit the liberties protected by Section 7 of the NLRA. Similarly, the policy’s mandate that social networking posts be respectful, fair, and courteous was deemed lawful because an employee would not reasonably construe the rule as prohibiting protected activities based upon the examples of plainly egregious conduct set forth in the rule including: “malicious, obscene, threatening or intimidating” posts; “offensive posts meant to intentionally harm someone’s reputation” and posts that may create a discriminatorily hostile work environment.

**B. Employer Policies under State Collective Bargaining Laws**

The case law in Michigan, Florida, and New York concerning the lawfulness of employer social networking policies is less developed than under the NLRA. Michigan and New York have no decisions on point but each state has precedent suggesting the analytical approach it might take regarding the maintenance and application of policies restricting social networking. In Florida, FPERC has issued one decision, *Orange County Board of County Commissioners*, concerning restrictions on posting of images through social media that reached a different conclusion than the NLRB ALJ’s decision in *G4S Secure Solutions (USA), Inc.*

1. **Michigan**

In *City of Bay City*, MERC held that a public employer’s maintenance of the following work rule in a municipal resolution restricting employee communications with elected officials constituted an unfair labor practice under Section 10(1)(a) of MPERA:


320. *Id.* In an advisory memorandum issued following *Costco* and *Karl Knauz Motors, Inc.*, the Division of Advice found that an employer’s social media policy was not overbroad because it included sufficient examples of prohibited activities so that an employee would not reasonably believe that it prohibits protected activities under the NLRA. See Advice Memorandum, *Cox Commc’n, supra* note 163.


323. 20 MPER ¶ 96 (2007).
[I]t shall hereafter be the policy of the City to grant to those individuals employed by the City of Bay City the right and privilege to freely communicate with their elected representatives and to address the City Commission in a public forum according to the rules of said forum to the same degree as those who are not employed by the City of Bay City so long as the communication deals with issues entirely outside of labor relations or employment related matters. There remain clearly established restraints on employee-commissioner communication and/or interaction related to employment and labor relations issues.324

In finding the resolution unlawful, MERC applied the NLRB standard for analogous work rules in the private sector: city employees would reasonably construe the resolution as prohibiting protected concerted activity.325 It concluded, therefore, that the overbroad policy violated MPERA because it would have a chilling effect on protected activities by city employees.326 The holding and analysis in City of Bay City suggests that MERC would follow NLRB precedent concerning the maintenance of a rule or policy restricting employee social media activities.327

The application of a work rule restricting employee social networking in future cases might be examined under the test formulated by a Michigan intermediate appellate court in Ingham Co. v. Capitol City Lodge No. 141.328 In that case, the court set forth a three-part test based upon NLRB precedent for determining whether a public employer violated MERC when it applied a work rule to discipline an employee for engaging in conduct ordinarily protected under MERA.329 Under the three-part test, the following factors are considered: whether the employer’s action adversely affected the employee’s statutory right to engage in protected concerted activity; whether the employer satisfied its burden of demonstrating a legitimate and substantial business justification for instituting and applying the rule; and whether the diminution of employee rights because of the rule’s application outweighed the employer’s interests protected by the rule.330

Applying that test, the court in Ingham Co. v. Capitol City Lodge No. 141 overturned a MERC determination331 that the employer violated Sections 10(1)(a) and (c) of MPERA by disciplining a union president for violating a

324. Id. (emphasis added).
325. Id. (citing Cintas Corp., 344 N.L.R.B. 943 (2005), enforced Cintas Corp v. NLRB, 482 F.3d 463 (D.C. Cir. 2007); Lutheran Heritage Village-Livonia, 343 N.L.R.B. 646 (2004); Lafayette Park Hotel, 326 N.L.R.B. 824 (1998), enforced 203 F.3d 52 (D.C. Cir. 1999).
327. See id.
329. Id. at 100-01.
330. Id.
331. 18 MPER ¶ 44 (2005).
work rule prohibiting the external dissemination of confidential information by faxing to union counsel an internal sheriff’s department memorandum setting forth a new policy requiring detectives to wear pagers while on and off-duty.\textsuperscript{332} The court concluded that the union president’s dissemination of the policy without prior approval did not constitute protected concerted activity because she received the memorandum in her capacity as a detective.\textsuperscript{333} In the alternative, the court found that the sheriff’s department had a legitimate and substantial security justification for the rule that outweighed the union president’s statutory right to engage in protected activity.\textsuperscript{334}

2. Florida

In \textit{Orange County Board of County Commissioners},\textsuperscript{335} FPERC held that portions of a county fire department’s social media policy violated Section of 447.501(1)(a) of FPERA because it was overbroad and chilled the firefighters’ right to engage in concerted activity for mutual aid and protection.\textsuperscript{336} The departmental policy was imposed after receipt of citizen complaints about on-duty firefighters taking pictures at accidents using personal cameras and then posting the photographs on social media pages.\textsuperscript{337} FPERC found that prohibiting the firefighters from using personal devices to access the internet constituted interference with their statutory rights to engage in off-duty electronic protected concerted activities.\textsuperscript{338} It also found the policy’s rule mandating that a firefighter “shall not criticize or ridicule or debase the reputation of the Department, its officers or other employees through speech, writing or other expression” violated the free speech clause in 447.501(3) of FPERA.\textsuperscript{339} The agency also found the prohibition against posts that “[t]ends to interfere with the maintenance of proper discipline” and or that “[d]amages or impairs the reputation and/or efficiency of the Department or its employees” interferes with protected concerted activities.\textsuperscript{340}

\begin{itemize}
\item \textsuperscript{332} Ingham Co., 739 N.W.2d at 105-06.
\item \textsuperscript{333} \textit{Id}.
\item \textsuperscript{334} \textit{Id}.
\item \textsuperscript{335} 38 FPER ¶ 131 (2011).
\item \textsuperscript{336} \textit{Id}.
\item \textsuperscript{337} \textit{Id}.
\item \textsuperscript{338} \textit{Id}.
\item \textsuperscript{339} \textit{Id}.
\item \textsuperscript{340} \textit{Id}; \textit{see also} Fla. Bd. of Educ., 29 FPER ¶ 89 (2003) (adopting hearing officer’s findings of fact and conclusions of law that state university’s ban on solicitation and distribution at all times and in all work areas, including use of university’s e-mail system, was overbroad and violative of Section 447.501(1)(a) of FPERA); City of Clearwater, 32 FPER ¶ 210 (2006) (finding that fire department policy which strictly prohibited all union messages and activities while employees were on duty and on employer property was unlawful because, with three rotating twenty-four hour
However, FPERC concluded that the policy’s restriction on employee use of department property and resources to engage in social networking did not facially or intentionally interfere, restrain, or coerce employees in exercising their rights under Section 447.301 of FPERA. Interestingly, with the exception of its analysis concerning the employer equipment use policy, the decision was based only upon the provisions of Florida statutory and case law.

3. New York

Although NYPERB has not ruled on the lawfulness of an employer social networking policy under the Taylor Law, its precedent provides guidance for future cases. An employer can violate the Taylor Law by applying a rule that interferes with the fundamental statutory liberties granted to public employees to form, join, or participate in a union of their choosing. Case law under the Taylor Law suggests that a broad policy restriction on employee off-duty social networking relating to forming, joining, or participating in a union would violate Section 209-a.1(a) of the Taylor Law. However, the mandatory duty to bargaining terms and conditions of employment under the Taylor Law might constitute the biggest impediment to a public employer unilaterally implementing restrictions on employee social media activities.

Relatively few NYPERB decisions have examined whether the maintenance or application of an employer rule constitutes unlawful interference with the fundamental statutory rights granted under the Taylor Law. In Village of Depew, NYPERB held that an employer violated Section 209-a.1(a) of the Taylor Law when it prohibited union officers and members from conducting a union fundraiser in support of a member facing disciplinary charges. In reaching its decision, NYPERB stated:

It is beyond any dispute that employees have the protected right to participate freely in the legitimate affairs of their chosen bargaining agent without suffering job-related consequences for such participation. The right is not so absolute, however, as to permit for no examination of the nature of the union activity, the manner in which it is carried out or the employer’s legitimate interests in regulating the activity. As with shifts, the policy denied employees the opportunity to engage in off-duty discussions about union matters in work or non-work areas).

342. See id.
343. See id.
345. See id.
346. Id.
many of the issues which arise under the [Taylor Law], we believe that the correct approach to the disposition of this question necessitates a balance of employee, union and employer rights and interests, subject, of course, to the provisions of the [Taylor Law].

Relying on private sector precedent, NYPERB has also held that a rule prohibiting employees from wearing a union pin while off-duty violated Section 209-a.1(a) of the Taylor Law because there was no special circumstances demonstrating that the employer’s interests outweighed the employee’s right to participate in the union under Section 202 of the Taylor Law by displaying the labor insignia, which is a form of union participation. A rule that interferes with the free exercise of employees to change union representatives by denying workplace access to a competing union seeking to solicit employee support can violate the Taylor Law. However, the Taylor Law does not restrict an employer from prohibiting employees from leafleting the public on its property about the status of negotiations. Finally, before an employer imposes limitations on off-duty employee activities, including political activities, it is generally obligated to engage in good faith negotiations with the union representing its employees pursuant to Section 209-a.1(d) of the Taylor Law.

Social media developments under the NLRA and state statutory law concerning protected activities and the breadth of employer social media policies provide a useful framework for exploring analogous constitutional issues applicable only to the public sector, to which we now turn.

IV. CONSTITUTIONAL PROTECTIONS FOR PUBLIC SECTOR SOCIAL MEDIA ACTIVITIES

Unlike in private sector employment, social networking by government employees is subject to protections under the First and Fourth Amendments to the United States Constitution. The constitutional protections constitute a floor of liberties that are supplemented in jurisdictions like Michigan, Florida,
and New York through legislative measures granting collective bargaining and tenure rights. As we have seen, the Florida constitution also guarantees public sector collective bargaining rights. For public employees in other jurisdictions without collective bargaining and/or other protections, the First and Fourth Amendments are the central, if not sole, legal bulwark against adverse workplace actions resulting from social networking.

As will be seen, infra, the First Amendment restricts workplace retaliation based upon the content of a public employee’s social media posts that touch upon issues of public concern. It also limits the scope of employer policies that might chill constitutionally protected speech. In addition, the Fourth Amendment provides some privacy protections when a public employee has a reasonable expectation of privacy regarding her or his social media activities.

A. The First Amendment’s Application to Public Employee Social Networking

Contemporary First Amendment jurisprudence in the field of government employment emerged from the shoals of a dark period in American public sector labor history. For roughly three decades, public employment was conditioned on loyalty oaths, associational restrictions, and prohibitions against what was broadly labeled subversive thoughts and activities. During this period, public sector unionism began its steady growth with some unions advancing a social union perspective in conjunction with bread and butter issues. The existence of tenure protections were generally a product of the legislative process, rather than negotiated agreements, because public sector collective bargaining remained largely anathema under the law. Public employees were subject to investigations, terminations, and resignations based upon perceived or actual viewpoints, actions, and associations unrelated to their fitness and competence to perform their job duties. One child of a victim from that period, Seventh Circuit Court of Appeals Judge Richard A. Posner, has observed:


354. See Mark H. Maier, City Unions: Managing Discontent in New York City 57-58 (1987); Walkowitz, supra note 32, at 189-96 (describing the activities of social services employees represented by United Public Workers of America (UPWA) on behalf of social services recipients).

355. See Geoffrey R. Stone, supra note 353. Marjorie Heins, Priests of Our Democracy: The Supreme Court, Academic Freedom, and the Anti-Communist Purge (2013); David Caute, The Great Fear: The Anti-Communist Purge Under Truman and Eisenhower 339-45, 431-45 (1978); Marjorie Murphy, Blackboard Unions: The AFT & The NEA 1900-1980 175-95 (1990); Clarence Taylor, Reds at the Blackboard: Communism, Civil Rights and The New York City Teachers Union 130-77, 203-33 (2011); Ellen W. Schrecker, No Ivory Tower: McCARTYISM & THE UNIVERSITIES 287-92 (1986). Militant public sector labor unions like UPWA were subjected to multiple attacks from employers and legislative bodies during this period. For example, the New York City Board of Education passed the Timone Resolution in 1950 to
I believe I have a closer personal acquaintance with civil-liberties abuses than you. My mother was forced out of her job as a public school teacher, and later hauled before the House Un-American Activities Committee, because of her communist sympathies. I consider her political views to have been idiotic, but I am quite sure that she was completely harmless.356

The dark cloud over public employee speech and associational rights began to lift as the result of successful legal challenges under the First Amendment to broad statutory restrictions.357 For example, in Shelton v. Tucker,358 an Arkansas teacher with twenty-five years of experience persuaded the United States Supreme Court to strike down a state law mandating, as a condition of continued employment, the filing of an affidavit listing “the names and addresses of all incorporated and/or unincorporated associations and organizations that [he] within the past five years has been a member of, or to which organization or association [he] is presently paying, or within the past five has paid regular dues or to which the same is making or within the past five years has made regular contributions.359 The Arkansas law was declared unconstitutional because the comprehensive scope of its infringement on teacher associational freedom went “far beyond what might be justified in the exercise of the State’s legitimate inquiry into the fitness and competency of teachers.”360

In Keyishian v. Board of Regents,361 the Court held that two state laws, which disqualified teachers from employment for making “treasonable or

prohibit Board members, administrators and supervisors from engaging in any form of negotiations or interactions with the New York City Teachers Union, a UPWA affiliate, concerning teacher grievances, personal or professional problems. Heins, supra, at 95-97; Taylor, supra, at 163-65, 176-77.


357. See Connick v. Myers, 461 U.S. 138, 144 (1983) (“The Court cast new light on the matter in a series of cases arising from the widespread efforts in the 1950s and early 1960s to require public employees, particularly teachers, to swear oaths of loyalty to the state and reveal the groups with which they associated.”).


359. Id. at 481, n.1 (quoting from Section 2 of Act 10 of the Second Extraordinary Session of the Arkansas General Assembly of 1958).

360. Id. at 490.

361. 385 U.S. 589 (1967). See Heins, supra note 355, for a thorough analysis of the Keyishian case and the Supreme Court’s decision. In the book, Heins weaves together constitutional legal history, the history of the anti-Communist purge in academia, personal stories of the victims of the purge, and the implications of that era on present day academic free speech issues.
seditious” utterances, and advocating for the “overthrow of the government by force, violence or any unlawful means,” were unconstitutionally vague. The Court’s decision centered on the imprecise draftsmanship of the at-issue laws, finding that key terms were undefined or ambiguous to pass constitutional muster. In addition, the Court found that the statutory disqualification for membership in an organization that advocated the forceful overthrow of the government was overbroad because it bars “employment both for association which legitimately may be proscribed and for association which may not be proscribed consistent with First Amendment rights.”

One of the notable aspects of the Keyishian decision is its unequivocal emphasis on the special status of academic freedom under the First Amendment:

> Our Nation is deeply committed to safeguarding academic freedom, which is of transcendent value to all of us and not merely to the teachers concerned. That freedom is therefore a special concern of the First Amendment, which does not tolerate laws that cast a pall of orthodoxy over the classroom.

Decisions like Shelton and Keyishian, which overturned overly broad restrictions on public employee associations and speech, helped set the stage for the Court’s landmark decision in Pickering v. Board of Education. Another key societal factor leading to the Pickering decision was the aggressive public sector union organizing efforts taking place throughout the nation.

In Pickering, the Court enunciated for the first time a constitutional framework for judicial post-hoc examination of an adverse action taken against a public employee based upon the content of her or his speech. Under Pickering and its progeny, a public employee’s right to speak as a citizen on an issue of public concern or importance under the First Amendment is balanced against a government employer’s interest “as an employer, in promoting the efficiency of

363. Id.
364. Id. at 603.
365. Id. at at 603.
368. Pickering, 391 U.S. at 568.
the public services it performs through its employees.”

The balancing test described in *Pickering* was later refined in *Connick v. Myers* and in subsequent decisions.

Protected civil liberties for public employees under the First Amendment are broader in some respects, and narrower in others, than those protected by the NLRA and other collective bargaining laws. Like collective bargaining laws, the First Amendment protects public employees associating with each other in a union. However, that constitutional provision “is not a substitute for the national labor relations laws” and it does not require a government employer to listen to, respond to, recognize or bargain with the union. In contrast to the private sector, as well as to the scope of protections under the Taylor Law, the First Amendment affords non-policymaking public employees broad protections for engaging in off-duty political activities. Individual and collective concerted activities limited to government workplace conditions are less likely to be protected under the First Amendment than similar activities under the NLRA and analogous state collective bargaining laws. The shifting burdens of proof in retaliation claims under the First Amendment, NLRA, MPERA, and FPERA are similar.

While case law applying the First Amendment to public sector social networking is not yet fully developed, the legal principles developed under *Keyishian*, *Pickering*, *Connick*, and subsequent decisions provide clear guidance. The analytical framework for determining whether public employee speech is protected under the First Amendment supports the Supreme Court’s dictum “that the government as employer indeed has far broader powers than does the government as sovereign” over the citizenry.

Constitutional protections for speech and association by public employees are strongest when the activities are off-duty, related to social and political

---

372. *Ark. State Highway Emp.*, 441 U.S. at 464. The potential application of the public concern standard to associational activities would undermine the proposition that public employees have First Amendment protections for associating into a union. See Herbert, *The Chill of a Wintry Light?*, supra note 25, at 629-30.
issues, and not directly connected to the workplace.\textsuperscript{376} To be protected, the
activities do not have to be concerted but the substance has to be more than
personal gripes over workplace issues such as a job assignment and the behavior
of supervisors.\textsuperscript{377} A stand-alone off-duty post by a public employee, without any
response from others, might be protected under the First Amendment so long as
it is found to touch upon a matter of public concern.

1. Posts Made Pursuant to an Employee’s Official Duties

The first step in determining whether the First Amendment protects a public
employee’s social media post is whether it was undertaken pursuant to the
employee’s official duties. This step is necessary because in \textit{Garcetti v. Ceballos},\textsuperscript{378} the Court held that speech by a public employee pursuant to official
duties is devoid of First Amendment protections. Under \textit{Garcetti}, when a public
employee speaks pursuant to official duties, he or she is speaking as an employee
rather than a citizen, and therefore the speech is unprotected.\textsuperscript{379} The \textit{Garcetti}
exclusionary rule is an important counterpoint to the private sector, where an
essential element for protections under Section 7 of the NLRA is that the activity
was undertaken by an employee for mutual aid and protection.\textsuperscript{380}

When the Court announced the rule in \textit{Garcetti}, it declined to articulate a
“comprehensive framework” for defining in future cases what constitutes an
employee’s official duties.\textsuperscript{381} While stating that “the proper inquiry is a practical
one,” the Court rejected reliance upon the content of job descriptions because they “often bear little resemblance to the duties” employees are expected to
perform.\textsuperscript{382}

Although most public employees are not officially assigned to engage in
work-related social networking, the content of posts by employees related to
work responsibilities might lack any First Amendment protections.\textsuperscript{383} The lack
of constitutional protections in that context might have particular repercussions
in the field of public education, where teachers are increasingly using social

\begin{itemize}
\item \textsuperscript{376} \textit{See City of San Diego}, 543 U.S. at 80 (“[When public] employees speak or write on their
own time on topics unrelated to their employment, the speech can have First Amendment
protection, absent some governmental justification ‘far stronger than mere speculation’ in
\item \textsuperscript{377} \textit{See Ricciuti v. Gyzeni}, 832 F. Supp. 2d 147, 158 (D. Conn. 2011) (“Considering the
public interest in an employee's speech also helps to guard against a danger that government
employees will feel tempted to ‘go public’—an easy thing to do in an age of blogs and social
media—every time they lodge a complaint or criticism at work.”).
\item \textsuperscript{378} \textit{Garcetti v. Ceballos}, 547 U.S. 410 (2006).
\item \textsuperscript{379} \textit{Id. at 424-25.}
\item \textsuperscript{380} \textit{See id.}
\item \textsuperscript{381} \textit{Id. at 424.}
\item \textsuperscript{382} \textit{Id. at 424-25.}
\item \textsuperscript{383} \textit{See Secunda, supra note 48, at 687-88.}
\end{itemize}
media for various purposes including peer-to-peer exchanges,\textsuperscript{384} and as a means of communicating with students and parents.

In response to Justice Souter’s dissent, the \textit{Garcetti} majority included \textit{dicta} in the decision concerning academic freedom under the First Amendment. The scope of protections for social networking by academics and teachers in public education will depend upon how the following \textit{dicta} is applied in future cases:

Second, Justice Souter suggests today’s decision may have important ramifications for academic freedom, at least as a constitutional value. There is some argument that expression related to academic scholarship or classroom instruction implicates additional constitutional interests that are not fully accounted for by this Court’s customary employee-speech jurisprudence. We need not, and for that reason do not, decide whether the analysis we conduct today would apply in the same manner to a case involving speech related to scholarship or teaching.\textsuperscript{385}

As Marjorie Heins has noted “[t]he Court’s once full-bodied appreciation of academic freedom as essential to the educational enterprise and to democracy was reduced [in \textit{Garcetti}] to a querulous and ambiguous aside.”\textsuperscript{386}

Since \textit{Garcetti}, circuit courts have ruled that so long as a public employee’s speech is in furtherance of his or her work responsibilities, it is considered to be pursuant to official duties, regardless of whether it was required by a job description or responsive to an employer’s directive.\textsuperscript{387} Those circuit decisions call into question a District Court decision holding that a high school teacher’s use of social networking to communicate with his students about homework and to forge better teacher-student relationships was not pursuant to his official


\textsuperscript{385} \textit{Garcetti}, 547 U.S. at 425.

\textsuperscript{386} Heins, supra note 355, at 263.

\textsuperscript{387} See Weintraub v. Bd. of Educ. of the City of New York, 593 F.3d 196, 198 (2d. Cir. 2010) (holding that elementary school teacher’s grievance complaint about the failure of an administrator to discipline a student “was in furtherance of one of his core duties as a public school teacher, maintaining class discipline, and had no relevant analogue to citizen speech,” and therefore was pursuant to his official duties); Renken v. Gregory, 541 F.3d 769, 773 (7th Cir. 2008) (finding that professor’s complaint to university officials concerning the handling of an educational grant was “for the benefit of students” and therefore aided in the fulfillment of his pedagogical duties); Williams v. Dall. Indep. Sch. Dist., 480 F.3d 689, 694 (5th Cir. 2007) (holding that “[a]ctivities undertaken in the course of performing one's job are activities pursuant to official duties.”); Phillips v. City of Dawsonville, 499 F.3d 1239, 1242 (11th Cir. 2007) (holding that “a public employee's duties are not limited only to those tasks that are specifically designated.”). See also Rohrbough v. Univ. of Colorado Hosp. Auth., 596 F.3d 741 (10th Cir. 2010). Cf Elkins v. City of Sierra Madre, 710 F.3d 1049 (9th Cir 2013); Fuerst v. Clarke, 454 F.3d 770 (7th Cir. 2006) (holding that speech by a public employee in her or his capacity as a union representative is not subject to the \textit{Garcetti} exclusionary rule).
duties because the school district did not obligate him to use social media. As one scholar has rightfully stated, *Garcetti* “might give schools absolute authority to prevent or restrict their teachers’ use of social media” for pedagogical purposes. Even casual social networking between teachers and students on subjects unrelated to course work might be excluded from constitutional protections under a broad reading of *Garcetti*. Nevertheless, a strong argument can be made that pedagogically related teacher-student social networking should not be exempt from First Amendment protections under *Garcetti*, based upon the importance of academic freedom.

Segregating work-related posts in a separate social media account and using a disclaimer may be prudent employee measures to maximize the likelihood of First Amendment protections. Separating work-related social media activities from personal social networking is a cornerstone of a policy implemented by at least one large school district. This type of protocol can help avoid problems resulting from the way social media blurs the line between professional and personal discussions.

The prophylactic value of a disclaimer is exemplified in *Stengle v. Office of Dispute Resolution*, where the express purpose of an off-duty blog maintained by an impartial hearing officer raised an issue of fact as to whether the blog was pursuant to official duties. The blog entries included her comments on special education issues under a class action settlement agreement and her experiences as a hearing officer. Although she was one of two hearing officers appointed to the class action settlement advisory board, the disclaimer stated that the blog was intended as a forum to present her perspectives as a parent of a class member and to share information with other class members. Nevertheless, the use of a mere disclaimer by a public employee, without additional facts, will

---

390. *Id.*
391. *See* Elise Rosen Puzio, *Why Can’t We Be Friends?: How Far Can The State Go In Restricting Social Networking Communications Between Secondary School Teachers and Their Students?*, 34 CARDOZO L. REV. 1099, 1121 (2013) (“In sum, if teachers are to fulfill their vital role in democracy, they must be free to utilize all tools and employ all methods that will bring our society closer to achieving our educational goals. The courts have given extensive guidance regarding what they consider to be of central importance to the principle of academic freedom. This principle should be defined to cover a teacher’s interest in communicating with students through social networking because these communications encompass many of the qualities courts consider central to an interest protected by academic freedom.”).
392. *Social Media Guidelines, supra* note 278.
394. *Id.* at 570.
395. *Id.*
probably not be sufficient evidence to demonstrate that a social media post was not pursuant to official duties.396

2. Whether the Post Touches Upon An Issue of Public Concern

If the social networking is found not to be pursuant to the employee’s official work duties, the second step of the inquiry is whether the posting touches upon a matter of public concern. As stated elsewhere, the public concern standard is an amorphous one, leading to contradictory results.397 To meet the standard, a posting must relate “to any matter of political, social, or other concern to the community”398 or be the subject of “legitimate news interest, that is, a subject of general interest and of value and concern to the public at the time of publication.”399 The fact that the speech may be controversial in nature, or was made in private, does not affect whether it relates to a matter of public concern.400 However, if the speech does not satisfy the public concern standard, balancing under *Pickering/Connick* is unnecessary because it is unprotected under the First Amendment.401

To determine whether a public employee statement meets that public concern standard, a court will examine “the content, form, and context of a given statement, as revealed by the whole record.”402 For example, in *Connick*, the content of an assistant district attorney’s intra-office questionnaire to her professional colleagues, as well as the context of the questionnaire, were considered in determining that the vast majority of the questions did not touch upon a matter of public concern.403 The questionnaire was prepared and distributed after the assistant district attorney was involuntary transferred, and it solicited responses about the office’s transfer policy, supervisors, office morale, the need for a grievance committee, and whether others felt pressured to work on particular political campaigns.404 The Court found that while the inquiry concerning political pressure touched upon an issue of public concern, the

---

396. *See id.*
400. Rankin v. *McPherson*, 483 U.S. 378, 387 (1987) (“The inappropriate or controversial character of a statement is irrelevant to the question whether it deals with a matter of public concern.”); *Givhan* v. *W. Line Consol. Sch. Dist.*, 439 U.S. 410, 415-16 (1979) (“Neither the Amendment itself nor our decisions indicate that this freedom is lost to the public employee who arranges to communicate privately with his employer rather than to spread his views before the public.”).
401. *Connick*, 461 U.S. at 141.
402. *Id.* at 147-48.
403. *Id.* at 148.
404. *Id.*
remaining questions were tied to internal workplace grievances and, therefore, unprotected.405

The more the content of employee speech comments on a news report or social and political events, the more likely it will be found to satisfy the public concern test.406 For example, a probationary employee’s short oral response in the workplace to a radio report about the attempted assassination of President Reagan satisfied the test.407 On the other hand, speech limited to the sale of pornography by a public employee is not likely to meet the public concern test because it does “nothing to inform the public about any aspect of [the employer’s] function or operation” nor was there any basis for concluding that the activities were “of concern to the community.”408

Connick, Rankin v. McPherson,409 and City of San Diego v. Roe410 demonstrate that, in contrast to collective bargaining laws, the First Amendment is far less likely to provide protection for public employee social media exchanges limited to a discussion about work issues, and/or a possible collective grievance concerning workplace conditions. For example, a first grade teacher’s post describing herself as the warden of future criminals was found to constitute a personal complaint about her job rather than a statement on a matter of public concern.411 To have constitutional protections, the content of a post must be explicitly or implicitly infused with social, public policy, or political issues. There is usually a relationship between workplace issues and broader public policy questions, which may explain why public sector employees are more likely to engage in off-duty community and political activities tied with work than their private sector counterparts.412 Linkage between public sector workplace conditions and public policy issues in social networking posts does not occur in a vacuum, however. Increased expressions of those connections will not occur without fertilization through education, training, and mentoring.

The First Amendment and collective bargaining laws share some common ground with respect to the self-absorbed egotism prevalent in the culture of social networking. Neither set of doctrines protect employees for social media content limited to personal complaints about work or narcissistic announcements and musings. For example, a student teacher’s posting of a photograph of herself wearing a pirate’s hat and holding a cup with a caption that read “drunken pirate” was found not to touch upon a matter of public concern based

405. Id. at 149.
407. Id.
412. REINARMAN, supra, note 32, at 186-88, 192-94.
upon the teacher’s admission at trial that the posted photograph was personal in nature.\footnote{413}

To determine whether a posting meets the public concern test under the First Amendment requires an examination of the facts and circumstances of the at-issue post based upon a textual and contextual analysis similar to that applied in NLRB cases, but using distinct constitutional standards.\footnote{414} In one First Amendment case, a District Court ruled that anonymous posts by a deputy sheriff on a local newspaper’s on-line forum did not meet the public concern standard when the posts are “taken as a whole and in full context.”\footnote{415} The posts mixed the deputy sheriff’s opinions concerning candidates in the upcoming sheriff’s election with allegations concerning his supervisor and statements about the personal life of one of his co-workers.\footnote{416} In another federal case,\footnote{417} the court found that two off-duty posts made by a county clerk employee on her Facebook wall about the firing of four colleagues touched upon a matter of public concern because the terminations received wide publicity and information about the discharges generated angry responses from county residents who were Facebook friends of the employee.\footnote{418} The parallel nature of the inquiries under the First Amendment and the NLRA is further exemplified by two decisions considering the relatively narrow question of whether the selection of the “like” option on a Facebook page is a protected activity. A federal judge held that a deputy sheriff’s mere “liking” of a Facebook page of the sheriff’s political opponent is not sufficient speech to merit First Amendment protections.\footnote{419} In contrast, the ALJ in \textit{Triple Play},\footnote{420} concluded that selection of the “like” option on a Facebook page “constituted participation in the discussion that was sufficiently meaningful as to rise to the level of concerted activity” under the NLRA.\footnote{421} Final resolution of whether selecting the “like” option on Facebook is protected awaits appellate review by

\begin{flushleft}
\footnote{416. Id. at 1090.}
\footnote{418. Id.}
\footnote{421. Id.}
the Fourth Circuit and a determination of exceptions from the ALJ’s decision pending with the NLRB.422

3. The Balancing of Interests Concerning Posts under Pickering/Connick

After a court finds that a social media post by a public employee was not in furtherance of official duties, and that the substance touched upon an issue of public concern, it will then balance the interests of the employee to speak out on such issues against “the government’s interest in the effective and efficient fulfillment of its responsibilities to the public.”423 Among a public employer’s interests are avoiding disruptions in regular operations, disharmony among co-workers, erosion of close working relationships requiring personal loyalty and confidentiality, impairment of discipline and supervisory control, and obstructions in the employee’s ability to perform work responsibilities.424

In applying the balance, a court will give “greater deference to government predictions of harm used to justify restriction of employee speech than to predictions of harm used to justify restrictions on the speech of the public at large.”425 A public employer is not obligated to “allow events to unfold to the extent that the disruption of the office and the destruction of working relationships is manifest before taking action.”426 Actual disruption does not have to be demonstrated; a reasonable prediction of future workplace disruptions can suffice to tip the balance in the employer’s favor under certain circumstances.427 The closer the content is to core issues of public concern, and the activity takes place off-duty, the greater the employer’s burden under the balancing test.428 Prior to taking an adverse personnel decision, however, an

422. Legal issues arising from Facebook exchanges are not limited to labor and employment law. There have been conflicting judicial ethics opinions from various jurisdictions concerning the ethical appropriateness of social network befriending between judges and attorneys. See Craig Estlinbaum, Social Networking and Judicial Ethics, 2 ST. MARY’S J. ON LEGAL MAL. & ETHICS 2, 5-6, 15-21 (2012).

423. Connick v. Myers, 461 U.S. 138, 150 (1983). “Among the relevant facts and circumstances that will be examined is whether a statement impairs discipline, disrupts workplace harmony, has a detrimental impact on close working relationships, impedes the performance of the employee’s duties, or otherwise interferes with the operations of the public agency.” See Herbert, The Chill of a Wintry Light?, supra note 25, at 613.


426. Connick, 461 U.S. at 152.


employer is legally obligated to act reasonably in gathering the facts necessary to
decide whether the speech may have constitutional protections.429

In Connick, the Court found that an employer’s interests outweighed the assistant district attorney’s interests regarding the questionnaire because the employer had a reasonable belief that its distribution constituted insubordination and might have disrupted the functioning of the office, undermined supervisory authority, and destroyed close working relationships.430 In contrast, the First Amendment interests of the employee in Rankin,431 to comment on an attempted assassination of a president, was found to outweigh the employer’s interest in that case because there was no evidence of an actual, or a reasonably potential, adverse impact in the workplace resulting from the comment. In reaching its decision, the Court emphasized that the statement was made in private to another employee and did not discredit the office.432

The weight given to an employer’s reasonable prediction of workplace disruption under the Pickering/Connick balancing constitutes a substantial difference from public sector collective bargaining laws. As demonstrated in Part II(C), an employee can lose statutory protections only when there is evidence of a “real threat” of disruption in Florida,433 and evidence of actual disruption in New York,434 emanating from an employee’s conduct. The different applicable standards concerning workplace disruption resulting from speech can have major significance in the area of public sector social networking.

Court of Appeals’ decisions in Richerson v. Beckon435 and Curran v. Cousins436 illustrate the current state of First Amendment protections under the Pickering/Connick balancing test concerning internet-based communications. In Richerson v. Beckon, the Ninth Circuit affirmed the dismissal of a First Amendment claim by a teacher based upon evidence that the content of her blog posts resulted in actual workplace disruption.437 In 2007, Tara L. Richerson was assigned by the school district to new positions requiring her to coach and mentor less experienced teachers.438 A core component of those duties was

---

429. Waters, 511 U.S. at 678.
430. Connick, 461 U.S. at 151–52.
432. Id.
433. Dist. Bd. of Tr. of Palm Beach Junior Coll., 11 FPER ¶ 16101 at 327 (1985), aff’d, Dist. Bd. of Tr. of Palm Beach Junior Coll. v. United Faculty of Palm Beach Junior Coll., 489 So. 2d 749 (Fla. Dist. Ct. App. 1986).
434. Cnty. of Tioga, 44 NYPERB ¶ 3016 (2011).
436. Curran v. Cousins, 509 F.3d 36 (1st Cir. 2007).
438. Id. at *1.
maintaining a confidential and trusting relationship with each mentee. After participating in interviews of candidates for her former position, Richerson posted a blog entry critical of the selection process including derogatory comments about the “Boss Lady 2.0” and the selected replacement. Subsequently, Richerson posted another entry critical of the union’s chief negotiator: “What I wouldn’t give to draw a little Hitler mustache on the chief negotiator.” When the blog entries became known, the school district received complaints from teachers and other employees including at least one teacher who refused to be mentored by Richerson. Following a review of the posts and the employee complaints, the district transferred Richerson from her new positions.

As noted, however, actual disruption is not a prerequisite in many cases to tip the balance under Pickering/Connick in favor of an employer. In Curran v. Cousins, the First Circuit deferred to the sheriff’s reasonable prediction of substantial risk of disruption in the sheriff’s department caused by a correction officer’s posts on the discussion board of a password protected union website. The postings referred to the sheriff, who is African-American, as Hitler, urged Department administrators to engage in insubordination, and compared correction officers to the victims of the Shoah. The First Circuit concluded that the statements were unprotected under the First Amendment because they “directly went to impairing discipline by superiors, disrupting harmony and creating friction in working relationships, undermining confidence in the administration, invoking oppositional personal loyalties, and interfering with the regular operation of the enterprise.”

439. Id. at *2.
440. Id.
441. Id.
442. Id.
444. Curran v. Cousins, 509 F.3d 36 (1st Cir. 2007).
445. Id. at 41.
446. Id. at 50; see also Dible v. City of Chandler, 515 F.3d 918, 928 (9th Cir. 2008) (to the extent that police officer’s sexually explicit website touched upon an issue of public concern, the City’s interests in maintaining an effective and efficient police department is particularly strong, which outweighed the officer’s interests. After the officer’s website became publicly known, the public started to denigrate other officers in the department, potential recruits asked questions about the website, and there was a concern whether the website would adversely impact the recruitment of female officers.); Gillman v. Schlager, 777 F.Supp.2d 1084, 1095 (S.D. Ohio 2010) (termination of police officer due his anonymous postings did not violate the First Amendment because comments interfered with the efficient operation of a public safety organization creating disharmony in the department and destroyed trust between plaintiff and the rest of the department); Stengle v. Office of Dispute Resolution, 631 F. Supp. 2d 564 (M.D. Pa. 2009) (Hearing officer’s blog entries were not constitutionally protected because employer’s interests in efficiency and maintaining the appearance impartiality were sufficient to justify the adverse action. In reaching
There is a strong societal need for courts, when applying the *Pickering/Connick* balancing test to employee social networking, to be vigilant in examining the reasonableness of an employer’s response, instead of deferring to the reactions of supervisors, co-workers, or others to the content and virality of a post. The easy accessibility and fast dissemination of a post, along with the volatile subcultural response when an item “goes viral,” can result in irrational and uninformed workplace overreactions. The speed of distribution of a post’s content from the internet to newspapers, cable, and radio can increase the power of the heckler’s veto in public employment.

The failure to apply adequate judicial scrutiny can lead to the suppression of unpopular off-duty speech and associations in social networking because the power of the medium can precipitate hysteria. Judicial restraint in the face of electronically-generated overreactions can take the law back to the pre-*Pickering* era of public sector labor history, when individuals and organizations were lawfully hounded by government employers based upon the unpopularity of their speech and associations. To avoid that risk, the law needs to proceed with prudence to ensure that our society’s libertarian principles are not tossed out with the bathwater when it comes to speech in cyberspace.

4. Employer Policies That May Chill Protected Activity under First Amendment

As we saw in Part II(A) and (B), *supra*, broad employer social media policies can run afoul of the NLRA and state collective bargaining laws when they chill employee rights to engage in protected activities. In the public sector, the First Amendment also places legal limitations on policies that prohibit or restrict potential speech through social media. The scope of constitutional scrutiny, however, is less stringent than under the NLRA, which calls into this conclusion, the court emphasized that the government can restrict employee speech based on its potential to disrupt, not only actual disruptiveness).

447. Frenzied and instantaneous misinformation disseminated through social media was on full display following the Boston Marathon bombings in April 2013. *See* James Gleick, “Total Noise,” *Only Louder*, NY MAG (Apr. 20, 2013), available at http://nymag.com/news/intelligencer/boston-manhunt-2013-4/ (“The Boston bombings, shootings, car chase, and manhunt found the ecosystem of information in a strange and unstable state: Twitter on the rise, cable TV in disarray, Internet vigilantes bleeding into the FBI’s staggeringly complex (and triumphant) crash program of forensic video analysis. If there ever was a dividing line between cyberspace and what we used to call the ‘real world,’ it vanished last week.”).

448. *See* City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2629 (2010) (emphasizing the need for caution “when considering the whole concept of privacy expectations” in the electronic workplace under the Fourth Amendment).

question the dictum in Garcetti about private and public sector employers having an equal need for “a significant degree of control over their employees’ words and actions . . . ."450

To determine whether employer prohibitions on employee speech violate the First Amendment, courts will apply the standards from Pickering, Connick, Roe, and Garcetti. For example, a written policy requiring that “all Sheriff’s Office employees shall keep official agency business confidential” was found constitutional because it restricted only unprotected speech under Garcetti relating to employees’ professional duties.451 In another case, a ban on an employee continuing personal communications with a recently terminated friend was found permissible under the First Amendment because personal communications do not satisfy the public concern standard.452

If the subject matter of the prohibition relates to a core issue of public concern, an employer has a greater burden to justify a prior restraint under the Pickering/Connick balancing test.453 When a workplace prohibition extends to future off-duty employee speech regarding issues of public concern, the employer must show “that the interests of both potential audiences and a vast group of present and future employees in a broad range of present and future expression are outweighed by that expression’s ‘necessary impact on the actual operation’ of the government.”454 In Whitney v. City of Milan455 the Sixth Circuit held that a mayoral directive prohibiting an employee from participating in litigation by a recently terminated employee alleging gender discrimination and public corruption was unconstitutional because the litigation raised issues of public concern, and the mayor failed to demonstrate that his interest in restricting the speech outweighed the employee’s interests under the legal standard applied to prior restraint.456 In finding the balance in favor of the employee, the court cited the limitless duration of the prohibition, the lack of prior actual disruption caused by the employee, and the speculative nature of the mayor’s concerns over workplace disharmony.457

The first court decision to address the constitutionality of an explicit ban on public employee use of social networking was rendered in 2011 by a Missouri state court judge.458 In that case, the court enjoined a newly enacted state law

---

451. Milwaukee Deputy Sheriffs Ass’n v. Clarke, 574 F.3d 370, 381-85 (7th Cir. 2009).
453. Id. at 296.
455. Whitney, 677 F.3d at 297.
456. Id.
457. Id. at 298.
prohibiting teachers from establishing, maintaining, or using a non-work related internet site that permits “exclusive access” with a current or former student.\textsuperscript{459} In enjoining the law, the judge found that as a matter of fact “social networking is extensively used by educators. It is often the primary, if not sole manner, of communications between [teachers] and their students.”\textsuperscript{460} In his three-page decision and order, the judge did not examine the law under \textit{Pickering/Connick/Garcetti}.\textsuperscript{461} Instead, the judge concluded that the law was unreasonably broad, noting that it might prohibit social networking between teachers and their own family members, and it would have a chilling effect on speech. Following issuance of the injunction, the Missouri state legislature repealed the statute.\textsuperscript{462}

The ubiquity of social networking, and the multiplicity of its forms, creates challenges for employers in crafting social media policies that are both lawful and practical. While First Amendment case law concerning social networking remains in an embryonic stage, the constitutional implications of workplace policies on electronic communications under the Fourth Amendment, to which we now turn, are much clearer.

\textbf{B. Privacy Protections for Public Sector Social Networking}

As Pauline T. Kim has argued, there is a strong connection between employee rights to free speech and privacy.\textsuperscript{463} Employee personal and associational discourse frequently occurs through private communications. Access to an individual’s social media account is protected through a user name and password. While Facebook permits users to restrict access to the content of a page through privacy settings, a 2012 study found that close to 13 million Facebook users in the United States admit to not using the privacy settings.\textsuperscript{464} Nevertheless, many in our society incorrectly assume that social networking and other forms of workplace-related electronic communications have strong, enforceable privacy protections.

In order for the content of a social media page to be protected under the Fourth Amendment against an unreasonable search and seizure by the

\begin{footnotesize}
\begin{enumerate}
\item Id.
\item Id.
\item Id.
\item Kim, supra note 19, at 925-29.
\item Facebook & your privacy: Who sees the data you share on the biggest social network? \textit{Consumer Reports} (June 2012), http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm.
\end{enumerate}
\end{footnotesize}
government, an individual must have a reasonable expectation of privacy. The applicable test for determining that issue was first articulated by Justice John M. Harlan in his concurrence in Katz v. United States: “My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person [has] exhibited an actual (subjective) expectation of privacy and second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”

When a reasonable expectation of privacy exists, the Fourth Amendment generally requires a government official to obtain a judicial warrant before conducting the search and seizure. The warrant requirement, however, is inapplicable when a public employer engages in a work-related search of its workplace. In a recent decision by the New York Court of Appeals, however, the majority concluded that a warrant was not required before a public employer attached a GPS device to an employee’s personal car for purposes of monitoring his movements outside of the workplace. A warrant is also unnecessary when data is in plain view or when it has been voluntarily provided by a third person.

There are distinct standards with respect to enforceable employee privacy protections in the government workplace under the Fourth Amendment. In O’Connor v. Ortega, the plurality applied a two-step test to decide whether a public employer’s search of an employee’s office violated the Fourth Amendment. The initial issue is whether the employee had a reasonable expectation of privacy based upon the “operational realities of the [particular] workplace.” To make that determination, a court examines workplace practices, procedures, and regulations. If the employee had a reasonable expectation of privacy, then the court examines the reasonableness of the

465. The Fourth Amendment states: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. CONST. amend. IV.
467. Id.
471. Semitsu, supra note 468, at 329-30.
473. Id. at 717.
474. Id.
employer’s intrusion into the employee’s privacy expectations resulting from the work-related search.\textsuperscript{475}

The Supreme Court began to tackle constitutional privacy issues involving public sector electronic communications in \textit{City of Ontario, Cal. v. Quon}.\textsuperscript{476} While the case involved text messaging, the constitutional privacy principles are relevant to public sector social networking, particularly when the activity involves use of the employer’s equipment.

In rendering its decision, the Court expressed deep concerns about the risk of judicial error “by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.”\textsuperscript{477} In words equally relevant to privacy issues in the rapidly evolving social media culture, the Court observed:

\begin{quote}
Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instrument for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matter can purchase and pay for their own.\textsuperscript{478}
\end{quote}

In \textit{Quon}, a unanimous Court rejected a police officer’s Fourth Amendment challenge to his employer accessing and reading his text messages sent and received through an employer-provided pager.\textsuperscript{479} It held that the employer’s search was reasonable under Fourth Amendment standards because it was justified from inception and its scope was reasonable under the circumstances.\textsuperscript{480} The purpose of the employer’s search was premised upon reasonable concerns about the adequacy of the character limit in its lease agreement with the service provider and whether the employer was paying for extensive personal texts by its officers.\textsuperscript{481} The scope of the search was found reasonable because it was limited

\begin{flushright}
\textsuperscript{475}\textit{Id.} at 725-26. \\
\textsuperscript{477}\textit{Id.}
\textsuperscript{478}\textit{Id.} at 2630.
\textsuperscript{479}\textit{Id.}
\textsuperscript{480}\textit{Id.}
\textsuperscript{481}\textit{Id.} The search in \textit{Quon} emanated from the employer’s unilateral decision to end a past practice of permitting officers to pay for monthly overages they incurred and thereby avoid having their text usage scrutinized by their supervisor. The unilateral change in that practice was probably mandatorily negotiable under the applicable California public sector collective bargaining law. See Claremont Police Officers Ass’n v. City of Claremont, 139 P.3d 532 (Cal. 2006). \textsc{Cal. Gov. Code} § 3504 states: The scope of representation shall include all matters relating to employment conditions and employer-employee relations, including, but not limited to, wages, hours, and other terms and conditions of employment, except, however, that the scope of representation shall not
\end{flushright}
to reviewing the content of on-duty text messages during a two-month period when the officer exceeded the allotted characters.\footnote{City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2629 (2010).}

Without determining the issue, the Court concluded that the officer had, at best, a limited reasonable expectation of privacy in his text messages because the pager was for use during police emergencies, the officer received notice from workplace policies that his texts were subject to audit, and he should have reasonably known that his on-duty texts may be subject to scrutiny during litigation.\footnote{Id. at 2631.} Other factors mentioned for determining an enforceable privacy expectation included whether reviewing the messages is necessary for performance evaluations and compliance with freedom of information laws.\footnote{Id. at 2629.} Under the circumstances of the case, the Court concluded “a reasonable employee would be aware that sound management principles might require the audit of messages to determine whether the pager was being appropriately used.”\footnote{Id. at 2631.} Notably unresolved by the decision was the dispute between the parties over whether supervisory statements and practices that deviated from the employer’s policies created an enforceable expectation of privacy.

The Supreme Court emphasized in \textit{Quon} the centrality of employer policies in determining whether workplace privacy expectations are reasonable: “And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.”\footnote{Id. at 2630.} The difference in design between social media and texting may make workplace policies less significant in determining workplace privacy rights concerning social networking. The operational realities of a username, password, and privacy settings on a social media account might outweigh the impact of a government workplace policy stating that employees lack an expectation of privacy in social networking when using the employer’s equipment.\footnote{See R.S. ex rel. S.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F. Supp. 2d 1128 (D. Minn. 2012) (finding that a student had a reasonable expectation of privacy with respect to her privacy protected social media messages). See also United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002), rev’d on other grounds, 90 F. App’x 3 (1st Cir. 2009) (finding defendant lacked a subjective expectation of privacy and commenting that “[w]hile it is true that there is no case law on point regarding this issue, it strikes the Court as obvious that a claim to privacy is unavailable to someone who places information on an indisputably, public medium, such as the Internet, \textit{without taking any measures to protect the information.”’) (emphasis in original); Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 872 F. Supp. 2d 369, 373-74 (D. N.J. 2012). See also}
There is a tendency among social media enthusiasts to “friend” multiple individuals including supervisors, co-workers, and even strangers. The lack of discernment in requesting and accepting invitations increases the probability that an employer may learn of a post, particularly one deemed offensive or troubling, from an employee’s social media friend without implicating the Fourth Amendment.488

V. CONCLUSION

It is possible that in the next few years, an enterprising group of scholars will post a report outlining their findings on American culture and values based upon a study of the content of social media. Rather than using polling, questionnaires or semi-structured interviews, the report will be based upon the content of data sets provided by social media companies. Unlike other research subjects, participants in social media cannot escape from their virtual memory. A portion of the data studied by the scholars will be available shortly through the Library of Congress’s archive of billions of tweets, thanks to a 2010 contract the library has with Twitter.489 In devising the research project, the scholars chose to ignore the central commercial component of social media because information about

Herbert, supra note 154, at 73-76 (discussing precedent concluding that the sender of an unrestricted e-mail lacks a reasonable expectation of privacy).

488. See United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) (“Where Facebook privacy settings allow viewership of postings by ‘friends,’ the Government may access them through a cooperating witness who is a Facebook friend without violating the Fourth Amendment.”). The same employer conduct, however, might still violate federal and state electronic privacy laws. See Pietrylo and Marino v. Hillstone Rest. Group, No. 06–5754, 2009 WL 3128420 (D. Ct. N.J. 2009) (holding that evidence supported jury finding that employee did not voluntarily consent to restaurant manager gaining access to employees’ chat room); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548 (S.D.N.Y. 2008) (employer violated Stored Communications Act 18 U.S.C. §§ 2701-2711 when it accessed former employee’s Hotmail account without authorization by utilizing former employee’s username and password information stored on employer’s computers). But see City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2629 (2010) (finding that public employer did not violate the Fourth Amendment when it read the transcripts of police officer’s text messages obtained from the service provider), with Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008), cert. denied sub nom. USA Mobility Wireless, Inc. v. Quon, 130 S. Ct. 1011 (2009) (concluding that the service provider violated the Stored Communications Act by providing employer with the transcripts of a police officer’s texts without his consent).

489. See Gayle Osterbert, Update on Twitter Archive at the Library of Congress, Lib. of Congress Blog (Jan. 4, 2013), http://blogs.loc.gov/loc/2013/01/update-on-the-twitter-archive-at-the-library-of-congress/ (“The Library’s focus now is on addressing the significant technology challenges to making the archive accessible to researchers in a comprehensive, useful way. These efforts are ongoing and a priority for the Library.”).
what people purchase, eat, read and watch is perpetually monitored and studied by social media companies and their advertisers.\footnote{See Al Gore, \textit{The Future: Six Drivers of Global Change} 79 (2013) (“Social media sites like Facebook and search engines like Google are among the many companies whose business models are based on advertising revenue and who maximize the effectiveness of advertising by constantly collecting information on each user in order to personalize and tailor advertising to match each person’s individual collection of interests.”).}

The future report is destined to disappoint. It is unlikely to reflect a society that prioritizes education, knowledge, virtue, enterprise, and equality. Instead, the report might describe a contemporary culture of narcissism far beyond what Christopher Lasch decried over three decades ago.\footnote{Christopher Lasch, \textit{The Culture of Narcissism: American Life in an Age of Diminishing Expectations} (1979).} The scholars will likely find that posts and tweets about political, labor, community, or spiritual issues were substantially outnumbered by idle words about banal topics written by people who appeared to have no time to think. To the extent the content involved work, the posts will have primarily focused on individualized complaints about supervisors, work frustrations, and other burdens associated with having a job. At the same time, the report will inevitably highlight posts filled with extraordinary forms of creative expression.

Whether the scholarly study is already in progress is unknown. What is known, however, is that social networking is substantially expanding electronic written communications, for good and ill, on many subjects including work. It constitutes a modern-day printing press with a potential readership that far exceeds what is possible with traditional print media. It is also a powerful tool for various forms of organizing. Users can write, read and exchange thoughts, and help to mobilize others to engage in action such as voting.

There are troublesome qualities, as well. By design, social networking is a documentation medium permitting access, review, and surveillance of communications and activities on a scale far beyond the dreams of espionage agents for 20th century domestic intelligence agencies and employers.\footnote{See Auerbach, supra note 65, at 97-114 (describing the use of espionage by private sector employers to spy upon union organizing efforts); Frank J. Donner, \textit{The Age of Surveillance: The Aims and Methods of American Political Intelligence System} (1980) (delineating a system of clandestine federal government spying on political and labor activities in the Twentieth Century); Frank J. Donner, \textit{Red Squads and Police Repression in Urban America} 41-43 (1990) (describing the use of local police agencies to monitor labor activities).} Electronically stored information related and unrelated to a protest can become the target of prosecutorial demands for access even when a person is charged with mere violations.\footnote{See People v. Harris, 945 N.Y.S.2d 505 (N.Y. Crim. Ct. 2012) (denying motion by a defendant charged with disorderly conduct during a protest, which sought to quash a subpoena \textit{duces tecum} seeking subscriber information and content information from his social networking service provider); People v. Harris, 949 N.Y.S.2d 590 (N.Y. Crim. Ct. 2012) (granting, in part, and...}
The architecture and culture of social media can also cause communicative misjudgments resulting in serious workplace consequences. The ubiquity of personal devices and the impulsiveness encouraged by the technology increases the substantial risk of electronic communicative collisions. While participants in social media are responsible for their behavior, the regularity of stories about inappropriate employee posts and tweets, particularly in the public sector, indicates that the conduct is not solely due to personal or professional failings.

Until the development of social networking, few desired or had the means to expose their inner thoughts, feelings, daily personal events and humor to a world-wide audience. Humor, in fact, frequently falls flat in the electronic communicative world. Attempts at humor in social media are less likely to constitute tools, as Langston Hughes described, that can “suddenly cleanse and cool the earth, the air and you.”\textsuperscript{494} The lack of facial expressions and vocal intonations, and the rapidity of the exchanges, can lead to substantial misinterpretations, a result that undermines the medium’s communicative value.

The NLRB’s actions over the past few years, and the national publicity it has generated, have resulted in a helpful societal recognition of the relevance of labor law to the use of technological communicative devices. Developments in the private sector might reawaken societal recognition of the importance of the liberties and rights granted by public sector collective bargaining laws and statutory and negotiated tenure protections. Despite a public sector labor law regime favoring associational activities under the First Amendment and state laws, the case law discussed in this article does not indicate that there has been an overwhelming embrace of social media for associational purposes. This may be due to the particular issues presented in the reported cases, the cultural shift over the past decades towards individualism over group activities, and/or the lack of available information concerning the scope of protected activities.

The case law and interpretative memoranda concerning social media delineate two core labor law questions: what constitutes protected speech in cyberspace and what are legal limits to the terms of employer policies. As we have seen, these issues are central in both the public and private sectors, along with questions of privacy and unlawful surveillance.

This growing body of decisions has applied well-established legal principles without regard to the differences inherent in interactive electronic communications. Those differences include the fact that, unlike most water cooler discussions, social networking frequently involves exchanges between employees and individuals with no connection to the employer or a union.

Determining intent and purpose in that context is more difficult. The transcriptions of social media posts are often disjointed, and subject to multiple meanings and interpretations. Discussions related to work can bleed into personal and political discussions making it difficult to pinpoint whether the subject is protected. The blending of topics can also complicate conclusions with respect to the employer’s motivation. To determine future social media cases under collective bargaining laws and the First Amendment may require a combination of dexterous dissection and careful suturing of electronic comments.

While the law will never be able to keep pace with the current speed of technological innovation, the behavioral norms associated with social networking demonstrate a need for retuning labor law doctrines to ensure that work-related civil liberties and protections are maintained in cyberspace. This can best be accomplished through legislative initiatives like the recent state laws restricting employer access to social media accounts. In addition, carefully drafted workplace policies, collective bargaining and workplace training can significantly aid in avoiding conflicts over public sector social networking. Finally, in determining whether public sector social media activities are protected, greater consideration should be given to the impulsiveness caused by the technology, the overreactions posts can engender, and the importance of legal checks to ensure that the principles of free speech, freedom of association, privacy and due process are preserved.
A CALL FOR UNCLE SAM TO GET BIG BROTHER OUT OF OUR KNICKERS:
PROTECTING PRIVACY AND FREEDOM OF SPEECH INTERESTS IN SOCIAL MEDIA ACCOUNTS

Michelle Poore*

I. INTRODUCTION

No one should be naïve enough to believe that content in social media accounts is entirely private. However, recently-exposed demands from public and private employers and academic institutions for access to such accounts of applicants, employees, and students, as well as the monitoring of personal social media accounts by these entities, go too far. They evoke thoughts of George Orwell’s fictional world of “Big Brother,” in which cameras spied ominously into all facets of everyday lives,1 and they are akin to asking for a key to someone’s house or going through private mail.2

Such invasions ought to be deemed a violation of information privacy, but the public nature of social media will often defeat claims of privacy interests and expectations in social media accounts. They could present freedom of speech concerns as well, if they restrict, or punish an individual for, speech protected by the First Amendment,3 labor laws regarding collective speech,4 whistleblower protections,5 or antidiscrimination laws.6

Of equal concern, employers and academic institutions that pry could face liability based upon their actions. What they learn about their employees or students could give rise to a duty to act or warn, and they might fail to take adequate action. Additionally, they could learn that an individual is a member of

* Lieutenant Colonel, U.S. Army Judge Advocate General’s Corps. Presently serving as the Chief of the International Law Branch, Office of The Judge Advocate General, Washington D.C. The views expressed in this paper are those of the author and not The Judge Advocate General’s Corps, the U.S. Army, or the Department of Defense.

1. GEORGE ORWELL, 1984 (1949).
a protected class, and any adverse action or inaction with regard to that individual could be, or appear to be, discriminatory.

While existing federal and state constitutions and statutes, as well as state common law, may provide some protection for employees and students from such intrusions, they are inadequate for a variety of reasons. In many cases, such laws were conceived prior to the dawn of social media, and therefore were not designed to protect interests they could not anticipate. Additionally, social media exposes information to more than just small, discrete groups of people, which, under traditional information privacy tort laws, would defeat any claim of an enduring privacy interest in the information. Finally, applicants and employees might provide consent to an employer’s access of their social media accounts out of fear that they might not be hired or be fired, especially in at-will employment arrangements. Students similarly could face comparable pressure to provide coaches and teachers access to their social media accounts as a condition for participation in athletic and other extracurricular activities.

Therefore, to adequately protect privacy interests in social media accounts, legislatures need to create statutes specifically tailored to the unique privacy concerns created by social media and with appreciation for the leverage that employers and academic institutions wield over prospective and current employees and students in today’s competitive environment. While employers and academic institutions have valid interests in monitoring users on their own networks for reasons related to security, productivity, protecting confidential and proprietary information, and protecting their reputations and brands, the legislation can carve exceptions for such monitoring, and at the same time, shield off-duty social media activity and protected social media communications in the workplace and academic setting from invasions of privacy.

California, Delaware, Illinois, Maryland, Michigan, and New Jersey have passed laws prohibiting employers, academic institutions, or both from demanding access to social media accounts of employees or students. Several other state legislatures are considering similar bills. While these developments

7. See Jill L. Rosenberg, How Social Networking is Changing the Face of Labor and Employment Law, 880 PLI/LIT 489 (Mar. 30, 2012); Stephanie Clifford, Video Prank at Domino’s Taints Brand, N.Y. TIMES, Apr. 16, 2009, at B1 (describing events where two employees were fired after posting a videotape of themselves engaging in a prank that involved numerous health-code violations, including putting cheese in one employee’s nose and putting nasal mucus on sandwiches being prepared for delivery).
are laudable, some of the enacted laws and proposed legislation leave gaps and loopholes for circumvention. Some fail to provide exceptions for employers and academic institutions to: permit social media monitoring on their own computer systems and services, to request information regarding social media usage of employees and students in order to comply with financial industry rules, and to investigate allegations of employee and student misconduct. Federal legislation could provide a comprehensive set of protections with appropriate exceptions and resolve apparent conflicts between state laws and other federal laws in this subject area.

In 2012, Congress rebuffed an attempt to implement legislation prohibiting employers from demanding passwords to social media accounts. However, there are indications that the efforts could be revived; members of Congress recognize the need for legislation in this area, because existing privacy and freedom of speech protections are not enough. Congress needs to resurrect this effort soon and address the invasive prying of academic institutions, as well as that by public and private employers.

Part II of this paper will discuss the intrusive actions that public and private employers and academic institutions have taken regarding private social media accounts. Part III explains why such actions might violate information privacy and freedom of speech rights and could give rise to unanticipated liability on the part of the snooping entity. Finally, Part IV will explore legislation that has been introduced in Congress and state legislatures in recent years.
enacted or proposed at the state and federal level to protect privacy interests in
social media accounts, and it will propose a way-ahead incorporating the best
parts of the enacted laws or bills under consideration into a comprehensive
federal law.

II. INTRUSIONS OF EMPLOYERS AND ACADEMIC INSTITUTIONS INTO PRIVATE
SOCIAL MEDIA ACCOUNTS

Along with our Facebook and MySpace friends and Twitter followers, many
other individuals might be keeping tabs on our online activity. While it can be
anticipated that ex-boyfriends and girlfriends may occasionally take a peek at a
former paramour’s social media activity to see who has replaced him or her, or
that a nosey neighbor may seek to gather a little gossip on the “Joneses,” other
less-likely individuals and entities might be snooping, as well.

Savvy debt collectors are using Facebook to engage in a strategy of
“friending” debtors who trust too much and accept friends requests from just
about anyone.10 This enables collection agencies to use Facebook email and
instant messages as additional venues for trying to convince debtors to pay up
and to determine if the debtor has collectible assets, which might be described or
photographically depicted on the debtor’s social media profile.11 Similarly, in
the legal profession, an attorney might peruse an opposing party’s social media
account content that has not been shielded from public view in order to find
information that could be beneficial to a client in litigation, particularly in
domestic relations cases.12

Employers have a valid interest in investigating prospective hires to
determine if they have unsavory backgrounds or tendencies that could damage
the reputation of the employer or indicate that the employee would not be a good
fit for the company.13 They may want to keep tabs on the social lives of their

Romo, Elusive Debtors Foiled by Their Social Media Sites, NPR (July 12, 2010 3:00 PM),
11. See Herb Weisbaum, Debt Collectors Troll Facebook – Are They Going Too Far?
MSNBC.COM (Apr. 25, 2012), http://www.msnbc.msn.com/id/42687734/ns/business-
consumer_news/t/debt-collectors-troll-facebook-are-they-going-too-far/.
12. See, e.g., Leanne Italie, Divorce Lawyers: Facebook Tops in Online Evidence in Court,
USA TODAY (June 29, 2010 10:41 AM), http://www.usatoday.com/tech/news/2010-06-29-
facebook-divorce_N.htm; Drew Bowling, How Lawyers Use Twitter, Facebook in Court Cases,
WEBPRONEWS (Apr. 12, 2012), http://www.webpronews.com/how-lawyers-use-twitter-facebook-
in-court-cases-2012-04.
13. See Patricia Sanchez Abril, Avner Levin, & Alissa Del Riego, Blurred Boundaries: Social
Media Privacy and the Twenty-First-Century Employee, 49 AM. BUS. L.J. 63 (2012) (discussing
surveys of employers indicating that a large number of them research job candidates using publicly
available content on applicant’s social networking profiles).
current employees to ensure that they are not engaging in activities that are potentially harmful to the business. With the advent of social media websites, employers can now peer into the private world of future and current employees with ease, in ways that previously would have required the hiring of a background investigator.

While the scanning or monitoring of social media sites for publicly-available information by debt collectors, members of the legal profession, and employers seems moderately intrusive and somewhat underhanded, it generally does not constitute an invasion of privacy under federal or state law. However, there is a disturbing emergence of reports of demands by public and private employers and academic institutions for access to users’ private social media account content. Such entities request the username and password for the user’s account, require that the user become an online friend of someone at its organization, consent to monitoring by a third-party application, or require that the user display his or her social media postings to someone from the entity during an interview or background investigation.

A. Employer Actions

The Maryland Department of Public Safety and Corrections was in the news in 2011 for requiring prospective hires and current employees to “voluntarily” provide their social media site usernames and passwords as part of a background investigation.\(^\text{14}\) The policy had been in effect for about a year, and the Department accessed social media accounts allegedly to check for gang affiliations, in order to deter gang violence in Maryland prisons.\(^\text{15}\) A report showed that, of 2,689 applications, seven candidates were rejected in part due to the information found on their social media accounts, and one was rejected solely on account of his social media account content.\(^\text{16}\)

After learning of the Department’s practice, the American Civil Liberties Union (ACLU) of Maryland issued a press release and news story about the policy.\(^\text{17}\) Both highlighted the experience of a current employee of the Department who felt compelled to provide access to his social media accounts or risk not being recertified to work in Maryland’s prison system.\(^\text{18}\) Shortly after the ACLU brought attention to this matter, Maryland’s Secretary of Public Safety and Correctional Services informed the ACLU that the practice of

\(^{14}\) Aaron C. Davis, Maryland Corrections Department Suspends Facebook Policy for Prospective Hires, WASH. POST (Feb. 22, 2011 9:58 PM), http://www.washingtonpost.com/wp-dyn/content/article/2011/02/22/AR2011022207486.html.
\(^{15}\) Id.
\(^{16}\) Maryland Becomes First to OK Password Protection Bill, supra note 2.
\(^{17}\) Id.
\(^{18}\) Id.
requesting access to social media sites of prospective and current employees had been suspended.19

The ACLU brought to light similar cases. The Richmond Times-Dispatch reported that as of January 1, 2012, “Anyone seeking to become a Virginia state trooper must make available the contents of his or her social media accounts — including private profiles — as part of the department’s extensive background-screening process.”20 Although the prospective hires do not have to surrender their usernames and passwords, they must list all social media accounts and permit an interviewer to review the contents of their social media accounts during the interview process.21 The ACLU also highlighted a blog posting showing a photograph that allegedly depicted an application form for a clerical position at a North Carolina police department. The form featured a line that asked, “Do you have any web page accounts such as Facebook, Myspace, etc . . . ? If so list your username and password.”22

At a Michigan elementary school, a teacher’s aide was fired for refusing to provide her Facebook password to the school district.23 A parent complained to the school that the aide posted a photograph on Facebook of a co-worker with pants around her ankles.24 School administrators asked the employee for her Facebook password to investigate the complaint. After she refused, the school district informed her that “in the absence of you voluntarily granting Lewis Cass ISD administration access to you[r] Facebook page, we will assume the worst and act accordingly.”25 She was given a ten-day suspension, and placed on administrative leave without benefits.26

Although less invasive but still disturbing, Sears used an alternate means for viewing employee applicant’s Facebook information.27 With an applicant’s approval, it employed a third-party application to view the prospective hire’s

19. Id.
21. Id.
22. Id.
24. Id.
25. Id.
26. Id.
Facebook basic information, without examining the wall content. Given that even basic information might disclose intimate details about an individual, as well as religious and political affiliations and views, Sears could face discrimination complaints if it takes adverse action based upon what the third-party application reveals to it.

B. Academic Institution Actions

More intrusive third-party applications are used by some colleges and universities to monitor athletes, “looking for obscenities, offensive commentary or words like ‘free,’ which could indicate that a player has accepted a gift in violation of N.C.A.A. rules.” Varsity Monitor is a one such application. Its website describes the service it provides as the following: “We monitor the social media interaction of athletes for questionable conduct that could negatively affect their reputation or ‘Personal Brand.’ We monitor for actions that could endanger their future career and sponsorship opportunities as well as damage the brand of their team, league and institution.” Major universities pay between $7,000 and $10,000 each year to Varsity Monitor to track their athletes. Given that many athletes are forced to consent to such monitoring in order to keep playing on their university’s sports team, Varsity Monitor’s purported interest in personal brands and individual reputations seems a little insincere and paternalistic.

As an alternative, a university might require an athlete or student to provide a coach or administrator access to his or her social media account by “friending” the coach or administrator. For example, the University of North Carolina handbook states the following: “Each team must identify at least one coach or administrator who is responsible for having access to and regularly monitoring the content of team members’ social networking sites and postings. The athletics department also reserves the right to have other staff members monitor athletes’ posts.”

Given that academic institutions and employers only recently began demanding access to social media accounts of applicants, students, and employees, the courts have not dealt with many complaints seeking redress for

28. Id.
31. Thamel, supra note 29.
such demands under traditional information privacy and freedom of speech theories. Regardless, aggrieved individuals are likely to find that existing laws protecting privacy and speech are inadequate to protect interests in social media accounts.

III. HOW INTRUSIONS BY EMPLOYERS AND ACADEMIC INSTITUTIONS COULD VIOLATE INFORMATION PRIVACY AND FREE SPEECH RIGHTS AND LEAD TO UNANTICIPATED LIABILITY

A. Information Privacy Rights

Since Samuel Warren and Louis Brandeis published their famous Right to Privacy33 article in 1890 recognizing the emergence of the “the right to be let alone,” the right to information privacy has evolved exponentially. Today, it encompasses privacy torts under state common law, federal and state constitutional law, federal and state statutory law, evidentiary privileges, criminal law, and international law.34 Given the nature of today’s society, where our movements are tracked when we use our credit cards, drive with a toll-paying device in our cars, post comments and photographs to social media accounts, or simply carry a cell phone, the right to privacy has become less of a right to be let alone and more of a right to control information we consider to be private.35

Traditional invasion of privacy torts36 will likely prove to be inadequate to protect privacy interests of employees or students in their social media sites against prying employers or academic institutions. The main reason for this is that the harm redressed by most privacy torts is the further dissemination or publication of private information, rather than the intrusion into private matters. The tort of intrusion upon seclusion involves a simple breach of privacy with no further dissemination required, but a social media site user’s consent to be monitored or his or her voluntarily surrender of an account password would likely defeat any action under this tort, because the intrusion must be unauthorized to be actionable. Additionally, it might be difficult to demonstrate how one can hold a privacy interest in information shared on social media sites, given its public nature.

34. See DANIEL SOLOVE & PAUL SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2-3 (2011).
36. The invasion of privacy torts are public disclosure of private facts, intrusion upon seclusion, false light, and appropriation of name of likeness. SOLOVE & SCHWARTZ, supra note 34, at 2.
This is an unfortunate and absurd result. As noted by Senator Charles Schumer: “Employers have no right to ask job applicants for their house keys or to read their diaries – why should they be able to ask them for their Facebook passwords and gain unwarranted access to a trove of private information about what we like, what messages we send to people, or who we are friends with?”37

Even so, the law has not yet developed to a point that it recognizes an expectation of privacy in social media accounts akin to the expectation of privacy afforded to people’s homes or personal diaries.

If the employer or academic institution is public, then the Fourth Amendment might apply when the social media account of an individual is accessed without consent, without a warrant based upon probable cause, or under exceptional circumstances that do not require a warrant.38 However, in most contexts, employers and universities are obtaining consent of the social media account user before accessing or monitoring his or her account. Therefore, the Fourth Amendment would provide no protection, unless the consent was not voluntarily obtained.

Additionally, it could be difficult to prove that an individual had a reasonable expectation of privacy in a social media account, due to the “third party doctrine.”39 Under this doctrine, once a person exposes information to a third party, he or she can no longer expect privacy in that information. Given that most information on social media sites is exposed to any number of other people, the third party doctrine would apply. Only in an exceptional case would the Fourth Amendment provide protection to information contained in social media accounts.

With the passage of the Electronic Communications Privacy Act (ECPA),40 Congress afforded privacy protection to electronic communications in a broader range of cases than the Fourth Amendment protects, especially in cases in which the third party doctrine would otherwise apply. The ECPA amended the Wiretap Act,41 which in its current form provides stringent requirements that must


38. See, e.g., O’Connor v. Ortega, 480 U.S. 709 (1987) (recognizing the special needs doctrine as an exception to the warrant requirement); Harris v. United States, 390 U.S. 234 (1968) (recognizing the plain view doctrine as an exception to the warrant requirement).

39. See Smith v. Maryland, 442 U.S. 735 (1979) (holding that there was no reasonable expectation of privacy in the numbers dialed on a telephone); United States v. Miller, 425 U.S. 435 (1976) (holding that there was no reasonable expectation of privacy in bank records).


followed before intercepting electronic communications in passage. The Wiretap Act would not protect most social media site content from viewing or monitoring by employers or universities, because much of the electronic communications they would be accessing are stored, rather than in passage.

However, the ECPA also included a new act, the Stored Communications Act (SCA),\(^\text{42}\) that would apply to the viewing and monitoring of stored information by employers and academic institutions. The SCA prohibits anyone from intentionally accessing communications that are in electronic storage without authorization or in excess of an authorization.\(^\text{43}\) Additionally, if a government entity seeks disclosure of communications in electronic storage, the authorization required for it to do so varies depending upon the length of time that the communications have been stored.\(^\text{44}\) If the communications have been stored for 180 days or less, a court order based upon probable cause is required.\(^\text{45}\) If they have been stored for over 180 days, and prior notice is given to the internet subscriber, then the government must obtain a court order or subpoena based upon specific and articulable facts;\(^\text{46}\) if no notice is provided to the internet subscriber, the government must obtain a warrant to access the communications.\(^\text{47}\) The SCA provides an exception to these authorization requirements if the internet subscriber consents to access.\(^\text{48}\)

At least one court has considered the issue of whether the SCA applies when an employer accesses an employee’s social media account. In the case of Pietrylo v. Hillstone Restaurant Group, two employees complained about their employer on a password-protected MySpace chat group, intended to be a private forum in which employees could air their grievances without fear of repercussions from management.\(^\text{49}\) Managers learned of the group and convinced another employee, who was also a member of the MySpace group, to give them her username and password to the site.\(^\text{50}\) The employee provided the information, because she felt coerced to do so.\(^\text{51}\) The managers then accessed the site, saw the critical postings, and fired the two employees who made the comments.\(^\text{52}\)

\(^{45}\) Id.
\(^{46}\) Id.
\(^{47}\) Id.
\(^{48}\) Id.
\(^{50}\) Id. at 3.
\(^{51}\) Id.
\(^{52}\) Id.
A jury found that the managers’ actions violated the SCA, and a federal district court upheld the verdict on a motion for judgment as a matter of law, or alternatively, for a new trial. Key to the case was that the employee who provided her password to the managers felt that, had she not done so, she would have “gotten into trouble.” Therefore, it was reasonable for the jury to conclude that the managers’ access to the stored communications on the MySpace chat group was not “authorized” within the meaning of the SCA.

The use of the SCA to protect privacy in social media accounts is novel, and there is little case law that touches upon it. Although the Pietrylo court found that coerced consent is not authorization within the meaning of the SCA, other courts could rule the other way.

For example, in State v. Poling, an Ohio Municipal Court considered whether a mother violated the SCA when she accessed emails of her sixteen-year-old daughter without permission. The mother was concerned that an adult male, who had been dating her minor daughter and was subsequently issued a civil protective order prohibiting further contact with the girl, was contacting her daughter via email. The mother viewed and printed some of her daughter’s MySpace emails, after the girl had left the house but was still logged in to her account on a family computer.

The case arose, because the adult male in fact had been emailing the daughter, in violation of the protective order. After he was charged with violating the protective order, he challenged the use of the emails against him in his criminal trial as a violation of the SCA and asked that they be suppressed.

Although the SCA does not provide for exclusion of evidence obtained in violation of it – as the exclusionary rule provides for Fourth Amendment violations – the court considered the lawfulness of the mother’s actions nonetheless. The court stated that her “conduct did not violate the SCA, as her conduct would seem to be authorized, at least implicitly, given her status as parent and how she observed the e-mails on the family computer without the use of her daughter’s password.”

The Poling case demonstrates the possibility that other courts could use a theory of implied or express consent to find that employers, who condition an offer of employment or continued employment upon a grant of access or the

53. Id.
54. Id. at 4.
56. Id. at 1120.
57. Id.
58. Id.
59. Id. at 1119.
60. Id. at 1120-21.
61. Id. at 1123.
ability to monitor the social media accounts of job applicants and employees, have acted legally. Therefore, relying on the SCA to curb intrusive actions of employers and educational universities is, at best, a dicey course of action.

Also, litigation under the SCA is unlikely to generate any immediate change in the behavior of employers and academic institutions, because the numbers of cases brought will be small, and they will take a fair amount of time to be resolved. Most employees and students who hesitantly turn over their social media account access information will not face adverse action. Only the few who do experience negative repercussions will sue. However, all employees and students subjected to these intrusions have experienced an invasion of their right to information privacy.

B. Freedom of Speech Rights

The First Amendment might offer some protection from public employers and academic institutions taking adverse action against an employee or student based upon content posted to social media sites. However, “it does not shield private employees, and rights afforded to public employees are limited to speech regarding matters of public concern, which are balanced against their employers’ business interests.” Furthermore, the Supreme Court has found that, if an employee’s speech “cannot be fairly considered as relating to any matter of political, social, or other concern to the community, government officials should enjoy wide latitude in managing their offices, without intrusive oversight by the judiciary in the name of the First Amendment.”

Other federal and state laws might provide greater protections than the First Amendment, covering speech that is not in the public interest. For example, “social networking sites provide an additional venue for employees to engage in communications that are protected by [Equal Employment Opportunity] or whistleblower laws.” Additionally, some states may prohibit “taking an employment action against an employee based on political activities, affiliations, or legal off-duty conduct.” California, Colorado, Connecticut, New York, and North Dakota have passed statutes to protect employees for adverse employment action in response to lawful, off-duty conduct.

In the April 2012 edition of Arizona Attorney, two attorneys who practice in the areas of labor and employment and commercial litigation wrote an article

62. U.S. CONST. amend. I.
63. Abril, Levin, & Del Riego supra note 13, at 85.
66. Id.
67. Abril, Levin, & Del Riego, supra note 13, at 93.
regarding recent actions of the National Labor Relations Board (NLRB) against employers who disciplined employees for social media content.\textsuperscript{68} Although the employees’ postings at issue occurred outside of the work place, the content was work-related.

The article highlights guidance that the NLRB’s Office of General Counsel distributed to its regional offices regarding this emerging area of the law that lacks legal precedent. The guidance emphasizes that “an employee’s comments on social media are generally not protected if they are mere gripes not made in relation to group activity among employees,” and that “employer policies should not be so sweeping that they prohibit the kinds of activity protected by federal labor law, such as the discussion of wages or working conditions among employees.”

One case in which the NLRB was involved concerned a Connecticut ambulance company employee who was fired for making derogatory comments about her employers on Facebook.\textsuperscript{69} She sued for wrongful termination, and the NLRB agreed to settle with her. The NLRB stated that, because the employer wrote the comments at home, off-duty, and on her personal computer, they were considered protected speech. As a result of this lawsuit and settlement, the ambulance company agreed to revise its social media and internet policies so as not to restrict its employees’ rights to discuss wages, working conditions, and other protected speech.

\textbf{C. Potential for Unanticipated Liability}

Employers and academic institutions who pry into the online activities of potential and current employees or students might face unanticipated liability based upon adverse action they take in response to content they view on social media accounts, their failure to act or warn in response to information discovered, or their failure to disclose to the social media account user the specific information gleaned from the user’s account that was used to make employment or educational decisions. Information that an employer or academic institution accesses on a social media site may reveal that an individual is a member of a protected group, based upon age, disability, marital status, religion, race, or national origin, for example. If the employer takes adverse action against a prospective or current employee after discovering the information, the employer might violate, or appear to violate, Title VII of the Civil Rights Act of 1964,\textsuperscript{70} the Age Discrimination Act in Employment Act of 1967,\textsuperscript{71} Titles I and V

\begin{itemize}
\item \textsuperscript{68} See Carrie Pixler Ryerson & John Balitis, Jr., Social Media’s Lessons, 48 APR ARIZ. ATT’Y 17 (Apr. 2012).
\item \textsuperscript{69} Jolie O’Dell, Employee Fired Over Facebook Comment Settles Lawsuit, MASHABLE (Feb. 8, 2011), http://mashable.com/2011/02/08/facebook-employment-speech-lawsuit/.
\item \textsuperscript{70} Pub. L. No. 88-352, 78 Stat. 241 (1964).
\end{itemize}
of the Americans with Disabilities Act of 1990,72 or other federal and state anti-
discrimination laws.

If an employer discovers criminal or harassing behavior or indicia of
violence when reviewing an employee or job applicant’s social media account,
the acquisition of such knowledge may give rise to a duty to warn or protect. If
this employee then harms someone, the employer could be liable under several
common-law tort theories available for third-party actions, including “a
voluntary assumption of a duty to protect, negligent security, negligent failure to
warn, negligent hiring, negligent retention, negligent supervision and other
potentially expensive torts, on which there is no financial cap.”73

Finally, “even if the social networking screening is proper, employers may
be required to disclose any results from the search obtained or used in
employment decisions under the Federal Fair Credit and Reporting Act or a state
equivalent.”74 Such disclosure could result in discrimination complaints
described above, if the information fairly involves the employees or students’
membership in a protected group.

IV. ENACTED AND PROPOSED LEGISLATION ADDRESSING SOCIAL MEDIA SITE
ACCESS AND MONITORING AND THE WAY-AHEAD

As a result of all of the past two years’ media attention given to the issue of
employers and academic institutions requiring access to private social media
accounts, some state and federal legislators have requested investigation of the
allegations.75 Additionally, legislators in California, Delaware, Illinois,
Maryland, Michigan, and New Jersey have enacted laws aimed at prohibiting
intrusion into social media accounts of employees and/or students.76 The U.S.
Congress has also considered a bill, and many state legislatures have proposed
legislation aimed at protecting the privacy of employers, students, or both.

73. Donald F. Burke, When employees are vulnerable, employers are too, NAT’L L.J., Jan. 17,
74. Abril, Levin, & Del Riego, supra note 13, at 88.
75. Would You Give an Employer Your Facebook Password? THE GUARDIAN UK (Mar. 26,
2012 3:17 PM), http://www.guardian.co.uk/commentisfree/cifamerica/poll/2012/mar/26/employer-
facebook-password-poll?goback=%2Egmp_4135130%2Egde_4135130_member_103812815;
Maryland Becomes First to OK Password Protection Bill, supra note 2 (Democratic U.S. Senators
Chuck Schumer of New York and Richard Blumenthal of Connecticut asked Attorney General Eric
Holder to investigate whether asking for log-in information during job interviews violates federal
law.).
A. Enacted State Laws and Proposed Legislation

Most of the enacted and proposed state laws prohibit employers and academic institutions from requesting or requiring disclosure of social media usernames, passwords, or other account access information and prohibit taking adverse action if an applicant, employee, or student refuses to disclose such information. Some address a practice known as “shoulder surfing,” where an


applicant, employee, or student is required to access a social media account in the presence of the employer or faculty member to allow the observer to scan the contents of the social media user’s profile or account.79 A few of the enacted and proposed laws prohibit employers and academic institutions from requiring employees and students to “friend” a representative of the company or school on their social media sites80 or prohibit even inquiring as to whether the employee or student has a social media account.81 A handful of the laws anticipate and close potential loopholes with prohibitions on accessing social media profiles or accounts indirectly through any other person who is a social media contact of the


applicant, employee, or student, seeking a waiver of laws that protect privacy in social media accounts, or requiring a change in social media privacy settings.

The social media privacy laws contain several exceptions, the most common of which permits employers and academic institutions to monitor or access accounts, services, devices, or technology issued by the employer or academic institution and promulgate policies governing the use of such items. Some states would allow employers and academic institutions to access information about applicants, employees, and students that is in the public domain.


84. For proposed state legislation regarding employers, see: S. 195, 63rd Leg. (Mont. 2013).


Sensitive to employers in the financial industry, Michigan’s law “does not prohibit or restrict an employer from 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 section 3(a)(26) of the security and exchange act of 1934.” 87 Finally, some of the laws allow an employer or academic institution to request access information for social media accounts to conduct an investigation into illegal activity or misconduct, such as an employee transferring the employer’s proprietary information without authorization. 88

B. Proposed Federal Legislation

Congress has considered legislation that was drafted in response to the allegations of employers and academic institutions prying into private social media account content. Representative Ed Perlmutter of Colorado proposed an amendment to the Federal Communications Commission Process Reform Act of 2012. 89 The amendment was intended to prevent an employer from demanding that a prospective or current employee reveal a confidential password to a social media account as a condition of employment. 90 The text of the amendment is as follows:

Nothing in this Act or any amendment made by this Act shall be construed to limit or restrict the ability of the Federal Communications Commission to adopt a rule or to amend an existing rule to protect online privacy, including requirements in such rule that


90. Id.
prohibit licensees or regulated entities from mandating that job applicants or employees disclose confidential passwords to social networking websites.91

The House of Representatives rejected the proposed amendment by a vote of 236 to 184, with only one House Republican voting in support of the amendment and only two House Democrats voting against it.92 Republicans have indicated they are willing to work on new legislation in the future that is similar to the proposed amendment.93 They rejected the amendment, however, because they viewed it as a partisan delay tactic used in relation to the entire Federal Communications Commission Process Reform Act of 2012.94

C. A Proposed Way-Ahead for Federal Law

While the efforts of individual states in trying to protect privacy in social media accounts are positive steps, Congress needs to pass a comprehensive solution to this problem, much like it did with the passage of the ECPA. The legislation should seek to incorporate all of the well-reasoned prohibitions and exceptions found in the enacted state laws and bills that are under consideration in state legislatures.

While the draft legislation will need to include a comprehensive “definitions” section, as most state bills incorporate, the operative language of the legislation should prohibit an employer from:

- Requesting an employee or an applicant for employment to disclose access information associated with the employee’s or applicant’s personal social media account in order to gain access to the employee’s or prospective employee’s account or profile on a social media website or to demand access in any manner to an employee’s or applicant’s account or profile on a social media website;
- Discharging, disciplining, failing to hire, or otherwise discriminating against an employee or applicant for employment for failure to disclose access information associated with the employee’s or applicant’s personal social media account.
- Requiring an employee or an applicant to add any person or any other person’s personal account to a list of contacts associated with a personal social media account;

92. Purwal, supra note 89.
93. Id.
94. Id.
• Requiring an employee or an applicant to change the privacy settings associated with a personal social media account; and
• Requiring an employee or an applicant for employment to waive or limit any protection granted under this law.

The legislation should include exceptions to permit an employer to promulgate and maintain lawful workplace policies governing the use of the employer’s electronic accounts, services, devices, and technology, and to monitor usage of such items. Exceptions should also allow an employer to access publicly-available information and to request access to personal social media accounts to ensure compliance with federal securities laws and to conduct investigations into illegal activity and misconduct.

The draft legislation should contain similar prohibitions and exceptions applicable to academic institutions regarding their relations with students and applicants for admission. The goal of this draft language is to protect privacy interests in social media accounts against intrusions by employers and academic institutions in contexts where prospective and current employees or students have virtually no power to resist. It also recognizes that employers and academic institutions have legitimate needs to monitor their own networks and equipment and to protect their proprietary and financial data.

V. CONCLUSION

Although the reference to George Orwell’s Big Brother organization usually refers to an overzealous government, it is now an appropriate reference for public and private employers and academic institutions that have evidenced a voracious appetite for more and more private information regarding the intimate details of their employees’ and students’ lives. Given today’s competitive market where employment opportunities are limited, employees and students with hopes for future employment may simply cower to the power of these entities and grudgingly provide their social media account access information.

The existing federal and state privacy, freedom of speech, and employment laws are insufficient to stop the intrusive actions of employers and academic institutions. Additionally, as pointed out by an ACLU attorney, “It’s going to take some years for courts to decide whether Americans in the digital age have the same privacy rights [as previous generations.]”

This emerging problem calls for new federal legislation to keep pace with ever-changing technology. Congress answered such a call in 1986 with the passage of the ECPA. It needs to do so again with comprehensive legislation to prohibit employers and academic institutions from invading privacy interests in

95. Klimas, supra note 37.
social media accounts. If it does not, the next generation may become numb to such practices, allowing for the infliction of even greater blows to basic rights of privacy and freedom of speech.
FROM UNIVERSAL EXCLUSION TO UNIVERSAL EQUALITY:  
REGULATING ABLEISM IN A DIGITAL AGE

Paul Harpur*

I. INTRODUCTION

The United Nations Convention on the Rights of Persons with Disabilities ("CRPD") is the first human rights convention expressly to protect the rights of persons with disabilities. The preamble to the CRPD explains that the United Nations adopted the CRPD based on twenty-five key facts. One of the facts is "that the majority of persons with disabilities live in conditions of poverty," thus creating a "critical need to address the negative impact of poverty on persons with disabilities." Today, persons with disabilities make up approximately twenty percent of the world’s poorest in developing countries. Many of the world’s 650 million persons with disabilities will have their human rights violated on a daily basis. This discrimination has resulted in persons with disabilities living in poverty even in developed countries. Indeed, research has found that persons with disabilities are more impoverished in the U.S. than any other developed nation. While there is no silver bullet to reverse ableism in the

* BBus (HRM), LLB (Hons), LLM, PhD, Solicitor of the High Court of Australia, Lecturer with the TC Beirne School of Law, The University of Queensland. I would like to extend my thanks to Professor Rick Bales, Professor Graeme Orr, A/Professor Carrie Basas and Mr. Jamie Teh. I also thank the participants in the Northern Kentucky University 2013 Symposium for their insightful comments.

2. Id. at Preamble(t).
3. Id.
community, recent law reforms have arguably created a new disability politics. The introduction of the CRPD and the disability human rights paradigm has substantially altered the benchmark for how states treat persons with disabilities. The new disability human rights paradigm has built upon existing scholarship and promotes a focus on substantive realization of rights.

This article argues that traditional anti-discrimination laws in the United Kingdom and United States do not meet state obligations under the new paradigm introduced by the CRPD. This article contends that emergent regulatory vehicles represent a positive trend towards greater rights compliance and that such new equality models should be applauded and expanded. To illustrate the limitations with traditional civil rights models and the potentiality with emergent models, this article uses regulatory theory to analyse how laws protect persons with disabilities’ access to the digital commons.

Part II of this article will introduce the concept of digital commons and how public policy paradigms have regulated persons with disabilities’ rights of access. This part will map early models which focused on curing and excluding persons with disabilities. Later public policy models focused on integration and how society disables people with impairments. This article will argue that the disability human rights paradigm cemented by the CRPD substantially advances the rights of persons with disabilities. The CRPD and the human rights paradigm require states to go beyond relying on traditional anti-discrimination laws. States are obliged now to seek new regulatory models to protect persons with disabilities rights.

Part III will analyse how existing civil rights laws protect persons with disabilities rights to access digital commons. This part will draw from existing

09.pdf. ("The U.S. has a higher income poverty rate for people with disabilities (using a standardized measure set at 60 percent of median adjusted disposable income and adjusted for price differences) than any other nation in Western Europe as well as Australia and Canada. A handful of nations - again mostly Nordic - have eliminated the disparity in poverty rates between people with disabilities and those with no disabilities.") (citing data collected by Organization for Economic Cooperation and Development); Mark C. Weber, Disability Rights, Welfare Law, 32 CARDOZO L. REV. 2483, 2486 n.11 (2011).


9. Eve Hill & Peter Blanck, Future of Disability Rights Advocacy and "The Right to Live in the World" 15 TEX. J. C.L. & C.R. 1, 29-30 (2009). Hill and Blanck contend that "the implementation of the Convention will succeed or fail depending on whether it is implemented as merely a technical standard, or recognized as a roadmap for transformation." Id.

scholarship and use regulatory theory to demonstrate the limitations of relying upon negative rights and victim enforcement.

Part IV and Part V will introduce dynamic new regulatory models that promote the rights of persons with disabilities in the United States and United Kingdom. The U.S. Twenty-First Century Communications and Video Accessibility Act of 2010 ("21st Century CVAA") expands the parties regulated by equality duties and introduces limited positive duties. Part IV of this article contends that the 21st Century CVAA is a significant development as it is not limited by the narrow scope of relationships that are regulated under traditional anti-discrimination laws. This new approach focuses more on the causes of discrimination in society and targets regulation at the root cause of technological inequalities.

Part V will analyse the positive duties under the Equality Act 2010 (U.K.). This model moves away from simply prohibiting discrimination. The positive duties in the UK embrace a form of management-based systems approach. This approach requires public agencies to seek out and remove inequalities. This part will draw from regulatory theory to ascertain the potential of these positive duties and argue that the CRPD now requires states to move beyond traditional negative duties found in anti-discrimination laws. The operation of the 21st Century CVAA and the positive duty in the Equality Act 2010 represent moves by law makers to find new and innovative ways to promote equality. This article applauds such interventions and encourages law makers to expand the operation of such regulatory vehicles.

II. THE COMMONS AND THE NEW DISABILITY HUMAN RIGHTS PARADIGM

A. Technology Opening the Door to Equality: The Digital Commons

Over the centuries the commons has been the forum where society transacted much of its business. People met in the commons for markets, for cultural functions, political activities, and for official state activities.11 Essentially, access to the commons represented access to community and political life. While the physical commons remains an important part of the community, the growth of the internet has resulted in the growth of digital commons. Digital commons operates as a platform for social media, retail, employment, and

politics and touches on most aspects of community life.\textsuperscript{12} The digital commons have been founded on the notion of equality and are premised on the notion that people should be able to access this resource regardless of their nationality, wealth, or resources.\textsuperscript{13}

People with disabilities may have impairments which reduce their ability to participate in the physical commons. For example, some impairments reduce the capacity of people to leave their homes and transact business in the physical commons. The growth of the digital age has the potential of empowering persons with disabilities.\textsuperscript{14} A person who is unable to leave their bedroom can surf the internet and interact with people across the globe. Effectively, the digital commons has the potential of contributing to the emancipation of persons with disabilities from the charity model.

This article contends that the digital age can be an accessible age if society lets people with disabilities participate.\textsuperscript{15} Ellis and Kent have observed that “increasingly, people with disability rely on the medium [the internet] to provide more independence, work opportunities, and social interactions.”\textsuperscript{16} Persons with disabilities utilize a range of adaptive technologies to operate computers.\textsuperscript{17} For example, persons with low vision or blindness use screen readers to provide an audio-description of what is on the computer screen.\textsuperscript{18} While people with print disabilities are unable to read standard print, the growth of EBooks and other digitizing of information means that millions of works are now potentially available.\textsuperscript{19} Whether or not persons with disabilities will continue to be disabled

\textsuperscript{12} See The Digital Public Domain: Foundations for an Open Culture (Melanie Dulong de Rosnay and Juan Carlos De Martin eds., 2012).

\textsuperscript{13} Jonathon W. Penney, Virtual Inequality: Challenges for the Net's Lost Founding Value 10 NW. J. TECH. & INTELL. PROP. 209, 211 (2012).

\textsuperscript{14} Victor Finkelstein, Attitudes and Disabled People: Issues for Discussion, 37 (1980). Finkelstein argues that "disability" is an oppressive social relationship. Its focus is attitudes towards "disability." Prevalent attitudes, however, are only uncovered as a result of research or social analysis. It is argued that those who carry out research or social analysis of necessity participate in the "disabling social relationship." Finkelstein contends that what we know about attitudes, therefore, cannot be separated from the conditions in which they are uncovered. Id.

\textsuperscript{15} Regulating the digital commons creates various regulatory burdens beyond this article. See Nicolas Suzor, The Role of the Rule of Law in Virtual Communities, 25 BERKELEY TECH. L.J. 1817 (2010) (proposing a framework based upon rule of law theory through which to better conceptualize virtual community governance and suggests appropriate regulatory responses).

\textsuperscript{16} Katie Ellis & Mike Kent, Disability and New Media 59 (2011).

\textsuperscript{17} Nic Suzor, Paul Harpur, & Dylan Thampapillai, Digital Copyright and Disability Discrimination: From Braille Books to Bookshare, 13 MEDIA & ARTS L. REV. 1 (2008).

\textsuperscript{18} For example, the world's most popular open source screen reader is Non-Visual Desktop Access. Non-Visual Desktop Access, www.nvda-project.org, (lasted visited Jan. 27, 2013).

will hinge upon the decision of designers or manufacturers to block or enable accessibility features.

While the potential for technology to transform the lives of persons with disabilities exists, reluctance of key stakeholders to implement accessible websites and other mediums has substantially reduced the enabling potential of the digital revolution. The barriers confronting persons with disabilities in taking advantage of technological advances can be grouped into three general areas. The first issue is the cost of adaptive technologies. When inclusive design is not mainstreamed as part of the product, persons with disabilities need to purchase software and/or hardware to enable them to utilize computers, cell phones, and other resources. Where retrofitting is possible, this process can be expensive and can result in inefficient use of the product. After a person with a disability has acquired the necessary software and hardware, the second barrier is training. Often there are no expert trainers available to run courses on both the adaptive technology and on the standard software or hardware. For example, if a person with a disability is using an adaptive technology to use a specialised computer program at work, the trainers for the adaptive technology are likely to be unfamiliar with the specialist workplace software and the workplace trainers may be unfamiliar with the adaptive technology. This creates a training vacuum that can be difficult for some persons with disabilities to surmount. The final barrier arises due to the way in which software and hardware is designed. As most designers and manufacturers do not consider universal design or accessibility, a large number of barriers are unnecessarily created. For example, security form fields on WebPages can be created in an accessible or inaccessible manner. Both approaches are equally secure, yet many sites adopt the inaccessible approach. Accordingly, it is critical for disability rights advocates and researchers to continue to ensure that accessibility remains on the political radar.

B. Established Disability Public Policy Paradigms

There have been monumental changes in how public policy paradigms treat persons with disabilities. United States laws used to ban people with disabilities

---

22. Id.
23. Id.
24. Id.
25. Id.
26. Id.
from the physical commons. The so called “Ugly Laws” criminalised disability.\textsuperscript{27} The ugly laws were enacted through unsightly beggar ordinances in various cities across the United States. The first unsightly beggar ordinance containing Ugly Law provisions commenced operation in San Francisco in 1867. Ugly Laws were subsequently enacted by numerous cities across the United States and remained operative until after World War I.

Unsightly beggar ordinances sort to regulate who was permitted to seek charity on the streets. By virtue of appearing as a person in need of charity, a person was deemed to be undesirable. Within this regime, people with disabilities were regarded as charitable cases and held to be undesirable. A person who breached the Ugly Laws by appearing in public could be fined $25 (a sizable fine in the 19th century) and/or be incarcerated for 25 days. The Ugly Laws anticipated that some people with disabilities may in fact have a justified reason to seek charity on the streets. If the person was sufficiently impaired, the court could waive the fine and substitute a mandatory stay in an almshouse. If a person is incarcerated in an almshouse, that person may be detained for an indefinite period with no effective right of appeal. Accordingly, being disabled could practically result in a more serious penalty than people who were “undesirable” on other grounds.\textsuperscript{28}

The public policy paradigm that guided regulations impacting upon persons with disabilities through the 20th century embraced some of the worst aspects of the Ugly Law paradigm. The so called “medical model” discounts the rights of persons with disabilities through adopting a medical hierarchal model.\textsuperscript{29} Under the medical model, the parties with the most power are medical practitioners and other professionals who are trained to focus unnaturally on one aspect of people’s needs.\textsuperscript{30} Rather than considering wider issues, policies under the medical model regard impairment as the trigger for disempowerment, institutionalisation, hospitalisation, and for the denial of rights.\textsuperscript{31}

\begin{thebibliography}{10}
  \bibitem{schweik} For a comprehensive discussion of the ugly laws see \textcite{schweik:ugly-1}. "The Ugly Laws" were not the actual name of the laws but a short hand phrase coined to describe the focus of the laws (prohibiting "ugliness" in public) and the ethical stance of the laws (which is ugly). \textsuperscript{Id.} at 23.
  \bibitem{schweik:ugly-2} \textsuperscript{Id.}
  \bibitem{koenig} The medical model is also used to describe other variations from the construction of normality. For example, medical model scholarship has been used to describe discrimination based upon gender reassignment. \textcite{koenig} (detailing the distributive consequences of the medical model with respect to trans persons).
  \bibitem{areheart} See id.
\end{thebibliography}
Medical model supporters regard an impairment as a trigger for disempowerment. Proponents of the medical model encourage regulators to devote resources to reducing people’s divergence from an artificially-constructed notion of normality rather than promoting the realization of human rights. The underlying premise of medical model scholarship is that a person with an impairment can be “fixed” which will then enable them to participate in society. Medical model scholars operate on the basis that until people can be “cured,” their quality of life and potential for success should be discounted. Accordingly, medical model scholarship focuses on obtaining greater resources to develop cures for impairments, so people with disabilities can have their degraded status in society addressed. This has resulted in persons with disabilities being institutionalised in virtual prisons, abused, degraded, and discounted while medical researchers attempt to find a “cure.”

The medical model remains extremely popular in medical schools, with the medical research lobby, and with other people who benefit financially from the disempowerment of persons with disabilities. It has fallen out of favour with persons who are concerned with the wellbeing and human rights of persons with disabilities. Disability rights scholars regard public policy agendas that primarily focus on trying to “cure” disabilities as misguided and often harmful. Rather than focusing upon the impairment and denying people their inalienable rights, social model scholars deconstructed disability discrimination to identify the most significant cause of disablement. Social model scholars identified that to be effective, both domestic and international disability rights must adopt a disability human rights paradigm).

32. Lisa Waddington & Matthew Diller, Tensions and Coherence in Disability Policy: The Uneasy Relationship Between Social Welfare and Civil Rights Models of Disability in American, European and International Employment Law, in DISABILITY RIGHTS LAW AND POLICY: INTERNATIONAL AND NATIONAL PERSPECTIVES 241, 244 (Mary Lou Breslin & Silvia Yee eds., 2002), available at http://www.dredf.org/international/waddington.html. Waddington and Diller analyse the relationship between the social welfare/medical model and civil rights model of disability policy and consider whether the dissonance between the two can be resolved or reduced, to what extent the tension is a problem, and whether a new disability policy model is needed. Id.

33. Anita Silvers, Formal Justice, in DISABILITY, DIFFERENCE, DISCRIMINATION: PERSPECTIVES ON JUSTICE IN BIOETHICS AND PUBLIC POLICY 13, 85 (Anita Silvers et al. eds., 1998). Silvers demonstrates that what is deemed by society to be a dysfunction is often more accurately described as atypical, anomalous, or diverse modes of functioning or the product of an inhospitable physical or social environment. Id.


35. See SAMUEL R. BAGENSTOS, LAW AND THE CONTRADICTIONS OF THE DISABILITY RIGHTS MOVEMENT 7-13 (2009) (describing “the endorsement of a social rather than a medical model of disability” as “the one position that approaches consensus within the movement”).
it is not an impairment that causes disablement, but how society is constructed that causes exclusion to occur.36

Social model scholars have focused on identifying interventions that will reduce society disabling people who have impairments.37 Professor Michael Oliver explains that the “core of the social model” aims for the ideal that “[i]t is society that has to change not individuals.”38 Some early disability rights scholars adopted a radical agenda to reverse this exclusion. Radical social model scholars contended that the growth of capitalism created a culture that disabled people with impairments.39 Radical social model scholars regarded the class struggle as inherently disabling and employed Marxist theories to address the economic exclusion of persons with disabilities.40 Other social model scholars adopted a non-radical agenda to address society’s disabling of persons with impairments.41 Early scholars, such as Professor Jacobus TenBroek, promoted the notion of “integrationism—that is, a policy entitling the disabled to full participation in the life of the community and encouraging and enabling them to

---


38. Michael Oliver, Understanding Disability: From Theory to Practice 37 (1996) (discussing issues related to the fundamental principles of disability, citizenship and community care, social policy and welfare, education, rehabilitation, and the politics of new social movements and the international context.).


40. Finkelstein, supra note 39.

do so."^42 Regardless of how radical the manifestation of the social model, all theorists in this church accept that society is the major cause of the disablement of people with different abilities.

The difference between the medical and social models can be illustrated by considering a person in a wheelchair. Medical science has not been able to “cure” paraplegia despite centuries of effort. Is being a wheelchair inherently disabling, though? What is stopping a person in a wheelchair from climbing the steps to access a train or building? What is preventing a person in a wheelchair from entering through a narrow doorway or from using the restrooms in a building? The cause of this exclusion is not the fact the person is in a wheelchair but the decision by society to use steps instead of ramps or lifts, to have narrow doorways, and to not install wheelchair accessible restrooms.^43 Key stakeholders in society have decided that people with a constructed norm are the people that will use certain venues and acted on this erroneous assumption.

C. The Paradigm Shift in Practice: The Rights Regime

In 2001, the United Nations General Assembly established an Ad Hoc Committee to report on the possibility of the United Nations adopting a disability-specific human rights convention.^44 Following years of transparent negotiations with disability persons organizations and other stakeholders, a draft convention was put before the United Nations General Assembly in December 2006.^45 Eight days later, the General Assembly unanimously adopted the CRPD. Following sufficient ratifications, the CRPD entered into force on May 3, 2008.^46

---

^42. Jacobus tenBroek, The Right to Live in the World: The Disabled in the Law of Torts, 54 CALIF. L. REV. 841, 843 (1966) (recognizing the connection between inclusion on the one hand and the participation of persons with disabilities in society); Michael Stein and Janet Lord have noted that "Professor tenBroek's 'right to live in the world' –the ability of persons with disabilities to have equally meaningful contact with the population at large—became a central feature of the values underlying the United Nations Convention on the Rights of Persons with Disabilities."

^43. Adam Samaha, What Good Is the Social Model of Disability?, 74 U. CHI. L. REV. 1251, 1258-59 (2007) (claiming that the social model has essentially no direct policy implications and arguing that the impact of the social model depends on normative commitments developed by some other logic, such as membership in the disability rights movement or adherence to versions of libertarian, utilitarian, or egalitarian theory that are triggered by the model's causation story).


A significant number of provisions in the CRPD promote policies that support social model interventions. Perhaps the most express recognition in the CRPD, that society is the cause of disablement, can be found in the CRPD’s preamble. Paragraph (e) of the CRPD preamble explains that the State parties enter the convention “[r]ecognizing that disability is an evolving concept and that disability results from the interaction between persons with impairments and attitudinal and environmental barriers that hinders their full and effective participation in society on an equal basis with others.” Paragraph (e) confirms the accuracy of the social model of disability and, accordingly, provides express recognition to the body of disability scholarship that has been focusing upon the role of society in disabling people with impairments.

The CRPD goes further than just recognising the fact society disables people with impairments. The CRPD promotes a new disability human rights paradigm, which advances a more holistic public policy agenda. One of the limitations with the social model was that it ignored the additional needs that may arise with certain impairments. The social model focused on removing physical barriers to inclusion. This resulted in advocacy to enable persons with disabilities to use ramps at the front of buildings rather than going around the back to a tradesman’s entrance by trash cans. Through enabling persons with disabilities to enter through the front door, the social model has arguably advanced the rights of many persons with disabilities. However, physical access will not ensure equality. Persons with disabilities may require medical support to enable them to exercise their rights. The social model targeted environmental barriers but has not promoted a holistic agenda.


46. Melish, supra note 45.
47. CRPD, supra note 1, at Preamble (e).
48. Id.
49. Id.
51. See Michael Ashley Stein & Penelope J.S. Stein, supra note 31, at 1223.
52. For examples of some impairments which require continuous medical support: Diabetes mellitus type 1 requires constant blood glucose testing, injections and the care of an endocrinologist; chronic airway diseases (such as asthma) and autoimmune disease lead to chronic kidney disease which requires both dialysis and constant drug intervention; Most individuals with myelomeningocele will need periodic evaluations by a variety of specialists, including: Orthopedists to monitor growth and the development of bones, muscles, and joints; Neurosurgeons perform surgeries at birth and manage complications associated with tethered cord and hydrocephalus; Neurologists to treat and evaluate nervous system issues, such as seizure disorders; Urologists to address kidney, bladder, and bowel dysfunction - many will need to manage their urinary systems with a program of catheterization. Bowel management programs aimed at
The disability human rights paradigm provides that states are required to regulate for the removal of environmental barriers, as well as proactively enable persons with disabilities to exercise their rights. The operation of the disability human rights paradigm can be evinced by analysing persons with disabilities right of access. The CRPD creates a right to access. The CRPD recognises that the right to access is critical for persons with disabilities to exercise their fundamental rights, including rights to social, economic, and cultural equality, health, education, information, and communication.

The right to access requires state signatories to “ensure” persons with disabilities equal access “to the physical environment, to transportation, to information and communications, including information and communications technologies and systems.” Rather than attempting to wrestle with the issues related to all forms of access, this article will focus on how persons with disabilities’ right to accessible communication technologies facilitates their access to the digital commons. Where providing access to public transport may cost billions to alter existing infrastructure, altering software and hardware at the design and manufacture stage is often inexpensive.

To protect the right to access, the CRPD adopts a two-pronged regulatory approach. The first prong focuses on rendering communication systems accessible at the design and manufacturing stage. Where universal design is adopted, many access barriers are not created in the first place and thus the need to engage in retrofitting is reduced or eliminated. The importance of universal inclusive design can be evinced by how widely it is referred to in the CRPD. The focus on inclusive design also appears with reference to “inclusive education,” workplaces that are “open, inclusive and accessible” to persons improving elimination are also designed: Ophthalmologists evaluate and treat complications of the eyes; Orthotists design and customize various types of assistive technology, including braces, crutches, walkers, and wheelchairs to aid in mobility.

53. Michael Ashley Stein and Penelope J.S. Stein, supra note 31, at 1223.
54. CRPD, supra note 1, at art. 9. This right of access impacts on various other rights, for example, the right to participate in political public life and the right to vote found in CRPD, id at art. 29. See also Ron McCallum, Participating in Political and Public Life: A Challenge for We Persons with Sensory Disabilities, 36 ALT. L.J. 80 (2011).
55. CRPD, supra note 1, at art. 9. This right of access impacts on various other rights, for example, the right to participate in political public life and the right to vote found in CRPD, id at art. 29. See also Ron McCallum, Participating in Political and Public Life: A Challenge for We Persons with Sensory Disabilities, 36 ALT. L.J. 80 (2011).
56. CRPD, supra note 1, at Preamble (v).
57. CRPD, supra note 1, at art. 1(1).
59. Microsoft Corporation, Engineering Software For Accessibility (Ben Ryan, Devon Musgrave, Lynn Finnel, eds., 2010).
60. Id. at art. 24(1).
with disabilities,\textsuperscript{61} and ensuring that international development programs are “inclusive of and accessible to persons with disabilities.”\textsuperscript{62}

Universal design does not mean universal access. The definition of “universal design” in the CRPD acknowledges that inclusive access cannot always be provided. Under universal design, access should be provided “to the greatest extent possible.”\textsuperscript{63} Where universal design cannot be achieved, the second prong becomes relevant. The second prong to protect the right to access in the CRPD requires states to ensure that “reasonable accommodations” are made to enable persons with disabilities to obtain access.\textsuperscript{64} This will involve requiring non-state actors, such as telecommunication providers, employers, educators and the like, to enable persons with disabilities to obtain access. In addition to engaging in positive conduct, state actors are required to provide funding and facilitating the development of assistive technologies.\textsuperscript{65} The duty to accommodate persons with disabilities requires states to strive for substantive equality for persons with disabilities.\textsuperscript{66}

III. THE REGULATION OF EQUALITY: COMMAND AND CONTROL, UNDER ANTI-DISCRIMINATION LAWS

The United States has developed a civil rights anti-discrimination model that has been adopted around the world.\textsuperscript{67} The primary operative statutes in the United States are the Rehabilitation Act of 1973\textsuperscript{68} and the recently amended Americans with Disabilities Act (“ADA”).\textsuperscript{69} Following recent reviews, anti-discrimination statutes in the United Kingdom have been harmonised in the

\textsuperscript{61} Id. at art. 27(1).
\textsuperscript{62} Id. at art. 32(1)(a).
\textsuperscript{63} Id. at art. 2.
\textsuperscript{64} Reasonable Accommodation is used: in the definition of disability discrimination in CRPD, id. at art. 2; to promote equality and non-discrimination in CRPD, id. at art. 5(3); to ensure the liberty and security of the person in CRPD, id at art. 14(2); to ensure the right to education in art, CRPD id at art. 24(2) & (5); and to exercise their right to work in art. id. art. 27(1)(i).
\textsuperscript{65} Johan Borga, Stig Larssona and Per-Olof Östergrena, The Right to Assistive Technology: for Whom, for What, and by Whom?, 26 DISABILITY & SOC’Y 2 (2011) (analysing the assistive technology content of the CRPD from a basic human rights perspective).
\textsuperscript{69} 42 U.S.C. §§ 12101-12117 (2012).
Equality Act 2010. Despite cultural and content differences, the anti-discrimination regimes in the U.K. and U.S. are both based on the social model. Traditionally, the duties under the U.K. and U.S. regimes have relied upon negative duties supported by weak control mechanisms. As negative duties remain the primary way in which discrimination is combated in the U.K. and U.S., this part will analyse the operation of those laws.

This part will analyse whether traditional anti-discrimination laws posit commands that promote digital equality and have sufficient controls to ensure compliance. Under the classic command and control regulatory model, the content of the command is critical. The command will alter conduct and achieve the objective of the intervention. This command can be phrased as either rules or standards. The direction must target people who can influence the desired result, require those parties to take the necessary steps to achieve the desired outcome, and avoid unintended consequences.

The ADA has been identified as an exemplar of the social model. The social model focused on removing barriers to inclusion without clearly defining what steps states needed to take. The authoritative statement on the disability human rights paradigm provides guidance on how states should alter conduct to enable persons with disabilities to exercise their rights. Do the commands in the ADA and Equality Act achieve the outcomes prescribed in the CRPD? Presuming persons with disabilities are able to access the anti-discrimination regime, then the remaining two steps focus on relationships that are regulated and the content of duties. Following the ADA Amendments Act, the issue of

70. The Equality Act, 2010, c. 15 (U. K.) has moved to replace a number of legislative regimes covering gender, race, disability, religion or belief, sexual orientation and age. The acts that have been replaced by the Equality Act 2010 include the: Equal Pay Act, 1970, c. 41 (U.K.), Sex Discrimination Act, 1975, c. 65 (U.K.), Race Relations Act, 1976, c. 74 (U.K.) and Disability Discrimination Act, 1995, c. 50 (U.K.).


72. See Lisa Heinzerling, Selling Pollution, Forcing Democracy, 14 STAN. ENVTL. L.J. 300, 302 (1995) ("In a command-and-control system, the government dictates the technology that must be installed to control pollution."); Cass R. Sunstein, Problems with Rules, 83 CAL. L. REV. 953, 1019 (1995) ("All industries must adopt the same control technology.").


74. Some scholars have argued that the introduction of anti-discrimination duties have caused employers to reduce their hiring of persons with disabilities. For a discussion of this debate see Bagenstos, supra note 6.

75. Michael Ashley Stein and Penelope J.S. Stein, supra note 31, at 1204.

76. In a series of judgments, the United States Supreme Court substantially read down the meaning of "disability" to the extent that the scope of the ADA was extremely limited. The three United States Supreme Court opinions are: Murphy v. United Parcel Serv., 527 U.S. 516, 519
who has a disability is less contentious in the United States. Because many other jurisdictions interpret who has a disability widely, this article will focus on who is regulated and the content of those regulations. This part will first analyse if this duty applies to various relationships connected with access to the digital commons and will then analyse the prohibition against discrimination under traditional negative duties.


A. Who Attracts Duties?: Designer and Manager of Digital Commons

The anti-discrimination regimes in the U.K. and U.S. prohibit discrimination in defined relationships. People who do not fall within prescribed relationships can lawfully engage in discrimination. The Equality Act 2010 contains anti-discrimination duties to regulate a prescribed range of relationships. The focus in the United Kingdom regime, but for limited circumstances, is on parties who may have direct contact with persons with disabilities. Those regulated in the United Kingdom include employers, educators, providers of goods, services, and public transport, operators of public premises, managers of sporting activities, and public transport operators.

The ADA adopts a different structure to the United Kingdom anti-discrimination regime. The ADA is divided into five titles. Title I prohibits discrimination in the employment context; Title II pertains to discrimination by public entities; Title III covers various types and services of private entities engaged in commerce (in “places of public accommodation” and “commercial facilities”); Title IV mandates the availability of telecommunications devices and relay services for persons with hearing impairments; and Title V contains miscellaneous provisions to assist in interpreting and enforcing Titles I-IV.

Do United Kingdom and United States anti-discrimination regimes regulate parties who design and manage digital commons? The issue of disability discrimination caused by inaccessible websites and databases has attracted considerable litigation and judicial division. The jurisdiction with the clearest legislative position is the United Kingdom. Under the now repealed Disability Discrimination Act 1995 (U.K.), businesses had an obligation to ensure equality and non-discrimination to “access ... and use of means of communication.” The Equality Act 2010 has expanded this duty and now deems any person concerned with the “provision of an information society service” an “information society service provider.” This creates duties under the Equality Act 2010 as a

80. Id. at § 39
81. Id. at § 88.
82. Id.
83. Id. at Pt §§ 35-37.
84. Id. at §§ 29,195.
91. Disability Discrimination Act, 1995, c. 50, § 19 (U.K.). This provision was introduced in 1999.
The agency charged with enforcing the Equality Act 2010, the Equality and Human Rights Commission, explains the scope of this duty:

If you provide services through a website – such as online shopping, direct marketing or advertising – you are known as an Information Society Service Provider (ISSP). This applies whether you have a one-page website which you maintain yourself or a very sophisticated website maintained by a professional web design company and covers anything in between.

The Equality Act 2010 Schedule 25 extends the definition of Information Society Service Provider to include any commercial website or internet based provider based in Europe that has commercial relationships touching the United Kingdom. However, this duty does not extend to internet service providers who only act as a conduit for the transmission of information.

Unlike the United Kingdom, where the statute clearly extends to websites, the regime in the United States has mixed application. Websites run by local, state, and federal agencies are required to be accessible by Title I of the ADA and the Rehabilitation Act of 1975. The situation is far more complicated with respect to privately-owned, privately-run websites. Courts have attempted to expand public access duties to cover digital environments. ADA Titles III and IV address website accessibility. Title III focuses on access to public accommodations and Title IV presents guidelines to ensure that people with disabilities enjoy full and equal access to telecommunications.

To sue a website for breaching the ADA, a complainant would need to either establish that the website was a place of public accommodation, or that there is a sufficient nexus between the service provided by such a place of public accommodation and the website. Plaintiffs will confront substantial difficulties in establishing that all digital commons are places of public accommodation. The United States District Court for the Southern District of Florida, in Access Now, Inc. v. Southwest Airlines Co., considered whether an airline’s on-line...

93. See id.
ticketing website was a place of public accommodation. 100 The court observed that Title III was plain and not ambiguous, 101 and that “the plain and unambiguous language of the statute and relevant regulations does not include websites among the [twelve specifically enumerated categories defining] ‘places of public accommodation.’” 102 As websites are not expressly mentioned in the ADA or regulations, for a website to be a “place of public accommodation,” it must be connected to a “physical, concrete structure.” 103 Accordingly, purely nonphysical establishments cannot be places of public accommodation. 104

The leading case on the Title III nexus test is the judgment of the U.S. District Court for the Northern District of California in National Federation of the Blind v. Target Corp. 105 Target, a retail chain, used websites as an integral component of their physical stores. Unfortunately, the websites were not accessible for blind persons using screen readers. The National Federation for the Blind and others sued Target for breaching Title III. In response, the Target Corporation filed a motion to dismiss the claims on the basis there was an insufficient nexus. Target argued that their inaccessible website did not limit persons with disabilities’ ability to physically access their stores and therefore did not breach the ADA.

According to the nexus approach, the court held that a website of a place of public accommodation must accommodate persons with disabilities. 106 The court advised that the ADA entitled people with disabilities to access “the services of a place of public accommodation, not services in a place of public accommodation.” 107 As a result, a website need not deny physical access to a building. A website that forms part of the service of a place of public accommodation is required by the ADA to be accessible. 108

Scholars have criticised United States courts’ narrow reading of what websites are regulated by the ADA. 109 Kenneth Kronstadt has argued that “[t]he

---

101. Id. at 1317.
102. Id. at 1318.
103. Id. at 1318.
104. Id. at 1319.
105. 452 F. Supp. 2d 946 (N.D. Cal. 2006).
106. Id. at 956.
107. Id. at 956.
108. Id. at 956.
The legislative history behind the ADA’s enactment supports the view that Congress did not intend to limit Title III’s reach to only those entities that are physically accessible for the purchase of goods and services. The nexus approach has the absurd outcome where a retail store like Target attracts duties under Title III, but purely on-line commercial operations, such as “amazon.com or buy.com would not need to make any accommodations because they have no facilities deemed places of public accommodation.”111 Nikki Kessling illustrates the absurd outcome of the nexus test using a hypothetical example:

Jill is profoundly visually impaired but otherwise self-sufficient. Because she cannot operate a car or navigate a busy city on foot without assistance, shopping for groceries (or anything else) is a difficult task. Jill’s city has four stores. Store A has a physical storefront only. Store B has a physical storefront as well as a website; shoppers can buy items via the store or the website. Store C has a physical storefront and a website, but regularly offers special “online-only” deals that apply only to website purchases. Store D has no physical storefront at all; a website is its sole method of selling its goods to the public.112

The nexus test means that only the portions of the store that directly relate to a physical store attract duties under the ADA. If businesses structure their websites to avoid linking them to their physical stores, they will avoid duties under the ADA to ensure their websites are accessible.

Arguably, the need to find a nexus between a physical location and a website unnecessarily limits the scope of the ADA. The nexus test goes against the bright-line rule adopted by the United States Department of Justice.113 The bright-line rule adopted by the Department of Justice provides that the ADA applies to websites. This approach recognizes that significant business is performed on the internet. As persons with disabilities are less mobile than the wider community, internet access even more critical. Limiting the ADA to

110. Kenneth Kronstadt, Looking Behind the Curtain: Applying Title III of the Americans with Disabilities Act to the Businesses Behind Commercial Websites, 81 S. Cal. L. Rev. 111, 133 (2007) (suggesting an approach that ensures title III will apply to the types of businesses Congress enumerated, even if such businesses conduct transactions exclusively via the Internet).
111. Id. at 130.
112. Nikki D. Kessling, Why the Target "Nexus Test" Leaves Disabled Americans Disconnected: A Better Approach to Determine Whether Private Commercial Websites are "Places of Public Accommodation," 45 Hous. L. Rev. 991, 992 (2008) (illustrating the various issues disabled Americans face in attempting to use the Internet, the magnitude of the problem of web inaccessibility, and the primary ways people can make websites accessible to those with disabilities).
websites that have a nexus with a physical shop substantially limits the operation of this remedial statute. If anti-discrimination law does not regulate parties who create barriers to inclusion, then it is likely that market forces will fail to pressure such parties to adopt inclusive design.\(^{114}\) The failure to regulate all website designers and operators has reduced the capacity of persons with disabilities to enjoy equal access to digital commons.

**B. The Prohibition against Discrimination: Regulating for Equality through Reasonable Adjustments**

The statutory regimes in the United Kingdom and United States each bifurcate the prohibition against discrimination into two categories.\(^{115}\) In the United Kingdom, the categories are referred to as direct\(^{116}\) and indirect discrimination.\(^{117}\) In the United States, the categories are called disparate treatment and disparate impact.\(^{118}\) While there are significant differences in interpretation and drafting, these statutes prohibit broadly similar conduct.

A discriminator engages in direct discrimination or disparate treatment where the discriminator treats or proposes to treat a person less favourably because that person has a disability. This requires a comparison between the treatment a person received with a disability and the treatment they would have received if they were not disabled. To establish direct discrimination in the United Kingdom, plaintiffs need to compare their treatment against an actual or a hypothetical comparator.\(^{119}\) United States courts have been comparatively hostile to plaintiffs, requiring them to find an actual comparator who is almost the twin of the plaintiff to prove the existence of disparate treatment.\(^{120}\)

---

115. This legislative approach accepts that there is market failure pertaining to persons with disabilities. Michael Ashley Stein, *Labor, Markets, Rationality, and Workers With Disabilities*, 21 Berkeley J. Emp. & Lab. L. 314 (2000) (analysing how market failure results in certain employers from reaching rational labor market decisions by creating a "taste for discrimination," in which the costs of including people with disabilities in a workforce are perceived as being greater than they really are).
119. For a discussion of this process see Hepple, supra note 78, at 99.
120. Suzanne B. Goldberg, *Discrimination by Comparison*, 120 Yale L.J. 728 (2011) (proposing that the comparator methodology has retained its popularity in large part because it serves entrenched judicial-legitimacy preferences that favour clearly-defined and identifiable categories and, relatedly, disfavour sociologically-oriented inquiries); Charles A. Sullivan, *The
The second category of discrimination is indirect discrimination or disparate impact. The concept of the disparate impact theory was first articulated by the United States Supreme Court in *Griggs v. Duke Power Co.*, and was later adopted in anti-discrimination statutes across the globe.\(^{121}\) Indirect discrimination or disparate impact prohibits facially neutral policies that have a discriminatory impact upon persons with disabilities.\(^{122}\)

Under both categories of discrimination, duty holders are required to make reasonable adjustments to render digital commons accessible to persons with disabilities in limited situations.\(^{123}\) The United States and the CRPD label this duty to make alterations as “reasonable accommodation,”\(^{124}\) and the United Kingdom labels it “reasonable adjustments.”\(^{125}\)

Reasonable accommodations involve making alterations to environments to enable persons with disabilities to operate.\(^{126}\) Professor Bob Hepple explains that there are three broad categories of reasonable adjustments.\(^{127}\) The first category concerns changing how things are done. This might involve providing sign language interpreters. The second category focuses on changes in the built environment, such as the installation of ramps. The third category concerns the

---

\(^{121}\) 401 U.S. 424 (1971); For example, the Civil Rights Act of 1964 and associate case law were extremely influential when Australia was drafting its anti-discrimination regimes. NEIL REES, KATHERINE LINDSAY AND SIMON RICE, AUSTRALIAN ANTI-DISCRIMINATION LAW 3-5 (2008).

\(^{122}\) For a discussion of barriers in the education of persons with vision impairments see Paul Harpur and Rebecca Loudoun, *The Barrier of the Written Word: Analysing Universities’ Policies to Include Students with Print Disabilities and Calls for Reforms*, 33 J. HIGHER EDUC. POL’Y & MGMT. 153 (2011) (using a combination of survey data and policy searches, the paper examines whether Australian universities are enabling students with print disabilities to take advantage of technological advances). Results revealed that Australian Universities are not ensuring that students with print disabilities have timely access to textbooks required for their university studies as a result of a combination of factors including inefficiencies caused by the statutory agency which regulates copyright, and by some universities having policies to provide minimal support to these students. *Id.*


\(^{124}\) See 42 U.S.C. § 12112(b)(5) (2012). For use of this term regarding the right to work see CRPD, *supra* note 1 at art. 27(1)(c).


\(^{126}\) Carrie Griffin Basas, *Back Rooms, board rooms--Reasonable accommodation and resistance under the ADA*, 29 BERKELEY J. EMP. & LAB. L. 59 (2008) (arguing that reasonable accommodations under the ADA are at the centre of the integration of people with disabilities into mainstream work environments).

\(^{127}\) *Hepple, supra* note 78, at 75.
duty holder providing auxiliary aids, such as installing screen readers on computers.

The factors that will determine whether an adjustment is unreasonable are broadly similar in the United Kingdom and United States. These factors include the cost of the adjustment when compared to the resources of the duty holder, the impact of the adjustment on the duty holder, and the position and relationship of the place where the adjustment is to be made. Professor Mark Weber has observed that significantly, the reasonable accommodation test “is not a cost-benefit comparison, but rather a cost-total budget comparison.” In an employment scenario, in one case a reasonable accommodation could be over ten percent of the employee’s annual wage and in another case it might be below this figure. Consequently, there are no fixed criteria to determine whether an adjustment is reasonable or unreasonable.

When balancing the competing factors courts focus on the cost of the adjustment to the duty holder, rather than on the benefit to the individual with a disability or to the community at large. Christopher Brown argues that failing

---

128. However, U.S. courts adopt a more narrow view of when a accommodation is linked to a disability. See Cheryl L. Anderson, What is "Because of the Disability" under the Americans with Disabilities Act? Reasonable Accommodation, Causation, and the Windfall Doctrine, 27 BERKELEY J. EMP. & LAB. L. 323 (2006) (analysing how a number of courts have required reasonable accommodations to be linked to narrowly identified aspects of a person's disability). Anderson concludes that US courts have used causation requirements to avoid evaluations on the merits of accommodations claims. Id.


130. Mark C. Weber, Unreasonable Accommodation and Due Hardship, 62 FLA. L. REV. 1119, 1136 (2010). Weber analyses the authoritative sources concerning the ADA Act accommodation requirement and concludes: (1) Reasonable accommodation and undue hardship are two sides of the same coin. The statutory duty is accommodation up to the limit of hardship, and reasonable accommodation should not be a separate hurdle for claimants to surmount apart from the undue hardship defense. There is no such thing as "unreasonable accommodation" or "due hardship." (2) The duty to accommodate is a substantial obligation, one that may be expensive to satisfy, and one that is not subject to a cost-benefit balance but rather a cost-resource balance; it is also subject to increase over time. (3) The accommodation duty entails mandatory departure from neutral workplace rules, effectively creating a preference for workers with disabilities, but one not to be confused with the affirmative action concept found in other anti-discrimination regimes. Id.

131. For a discussion of the ten percent figure see House Committee on the Judiciary, H.R. Rep. No. 101-485(III), at 41 (1990); Weber, supra note 130, at 1136.

to consider the positive externalities of an adjustment distorts the assessment. Brown argues that courts should adopt a net social benefit model, which assesses all the costs and benefits associated with an adjustment. This approach means that duty holders are not burdened with high adjustment costs where the benefit to an individual is moderate. The individual case-by-case approach largely ignores the situation where an adjustment has a high cost but may benefit thousands of individuals who are not in regulated relationships.

Even if macro issues were considered, the reasonable accommodation model responds after systems are created. Discussing the United States regime, Dr. Beth Ribet has criticised how anti-discrimination laws ignore employers’ conduct in creating barriers to employment, saying, “[t]he culpability of the employer or entity in the production of the disability itself is not conceived within the terrain of the law, when considering or weighing what its burden should be.” The retrofitting focus of anti-discrimination laws can create substantial barriers for inclusion.

It is often difficult or impossible to retrofit systems to render them accessible. Arguably, a system which focuses upon retrofitting will not create an accessible society. The CRPD calls upon states to promote universal design where possible. Under this approach, reasonable adjustments and accommodations operate where it is difficult or expensive to implement universal design. Relying upon the reasonable adjustment and accommodation model can reduce many barriers to inclusion, but it is far from creating equality. Equality can only be achieved where states promote universal design and embrace reasonable accommodations and adjustments where inclusive design is impractical.

C. Is Victim Enforcement a Viable Vehicle for Control?

The main vehicle to ensure that regulated parties comply with a command is through control. Generally, prohibitions standards are difficult to enforce. It is extremely difficult to hold duty holders accountable if they are being investigated for noncompliance because they can adopt any procedures they desire to satisfy the standards. The law does not impose a prescribed process

---


134. Id. at 341.


136. CDRC, supra note 1, at art. 5.

that duty holders need to follow to satisfy their duty. This means different duty holders may adopt different processes to achieve prescribed outcomes. While this flexible style of regulation enables duty holders to modify processes to their individual circumstances, this makes it difficult for regulators and complainants to determine if a breach has occurred. To determine if there has been noncompliance, the person enforcing the laws must evaluate each duty holder’s process to evaluate the level of compliance. This is expensive and complicated for regulators and even more difficult for complainants from oppressed groups.

Anti-discrimination laws rely upon victim enforcement as the primary enforcement vehicle.138 The civil rights approach has empowered survivors of discrimination to protect their own rights. There are definitely positive aspects to enabling people to enforce their rights.139 Despite the benefits, scholarship has concluded that victim enforcement lacks a sufficient level of enforcement to ensure regulatory compliance.140 Scholarship has identified that many disputes never become legal disputes. William Felstiner, Richard Abel, and Austin Sarat have identified that disputes are social constructs that move through several stages.141 The first stage occurs when an unperceived injurious experience is perceived as an injurious experience. While a lawyer may easily identify conduct as injurious, the capacity of the wider population to name conduct can be confounded by a lack of information, internalised oppression, and other anthropological variables.142 If an individual has named conduct as injurious, the next stage towards litigation involves transforming the named injury into a grievance. Transforming a named injury into a grievance involves an individual attributing blame to a particular party or parties. Once an individual has mentally attributed blame, the third stage involves turning a grievance into a claim against the blamed party. The term “claim” here refers to the act of approaching the blamed party to obtain redress for the individual’s injury and should not be confused with the originating documents in civil litigation of the


142. Id. at 633.
same name. If the blamed party expressly or implicitly refuses the claim of the individual, then a dispute exists. Following the above three stages, the individual may transform their dispute into litigation. While there is no primary research applying Felstiner, Abel and Sarat’s model to disability discrimination, it is reasonable to presume that many disputes are not transformed into legal disputes.

Reportedly, there is a chronic under-enforcement of anti-discrimination laws. Relying on victim enforcement is an ineffective control vehicle. The limitations of relying on victim enforcers can be evinced by the strategic choices of “cause lawyers” in the United States responding to the difficulties in pursuing parties who control access to digital commons. Cause lawyers can be defined as “attorneys who spend a significant amount of their professional time designing and bringing cases that seek to benefit various categories of people with disabilities and who have formal connections with disability rights organizations.” The National Federation for the Blind (“NFB”) is one of the world’s largest advocacy groups for persons with low vision and it often engages in strategic litigation with the aid of cause lawyers. In order to combat discrimination by websites that have no nexus to a physical location, the NFB has attempted to target end users who have ADA requirements.

The barrier that the NFB is targeting is the accessibility features on the Kindle reader. While the Kindle Reader is not a website, it is an extremely important communication device. The Kindle Reader is the EBook reader that enables customers to read EBooks purchased from Amazon.com. When the Kindle was first released, it included a screen reader and was accessible for persons with low vision and blindness. Following pressure from publishing houses, Amazon decided to turn the accessibility feature off. This decision prevented persons with low vision and blindness from being able to read the books on the Kindle. Due to the nexus requirements under Title III of the ADA, it would be difficult to prosecute suit against Kindle for discrimination.

144. Michael Ashley Stein et. al., Cause Lawyering for People With Disabilities, 123 Harv. L. Rev. 1658, 1661 (2010).
146. Id.
147. Id.
148. Id.
Without accessibility features enabled, the Kindle is now being used by educational institutions.¹⁴⁹ The move by Kindle into the education market has created additional duties under a range of statutes.¹⁵⁰ Educational institutions are prima facie prohibited from creating facially neutral policies which discriminate against persons with disabilities.¹⁵¹ As a test case, the NFB has sued Arizona State University to prevent the university from deploying Amazon’s Kindle to distribute electronic textbooks to its students because the device is inaccessible.¹⁵² While the approach of the NFB may create commercial pressure to alter Amazon’s conduct, arguably this is a less than ideal regulatory solution. Even if the NFB is successful, this case only concerns the operation of the Kindle Reader in education. This means persons with disabilities who would like to use the Kindle Reader to exercise their rights to engage in work, cultural life, politics and the like may still be denied access. Arguably, anti-discrimination laws should create a duty directly upon designers and manufacturers of technological devices.

IV. SETTING A NEW BENCHMARK FOR PERFORMANCE: 21ST CENTURY COMMUNICATIONS AND VIDEO ACCESSIBILITY ACT

One of the problems with the traditional anti-discrimination laws is that they fail to focus upon all parties that can influence inclusion. In particular, people who create digital commons may not attract any anti-discrimination duties in the U.S. Even where such duties exist, website designers are not required to use accessible software products. Even where a digital environment is accessible for persons with disabilities, barriers can be created by hardware that does not embrace universal design.

Recognising that persons with disabilities were not fully benefiting from technological advancements, United States lawmakers enacted the 21st Century Communications and Video Accessibility Act (“CVAA”). This law does not


¹⁵¹. ADA and Section 504 of the Rehabilitation Act also apply to the education of people with disabilities. All private educational institutions come within the definition of title III of the ADA, and public educational come within title II. As most institutions receive federal funding, most will also be subject to §504 of the Rehabilitation Act.

alter obligations discussed above under the ADA. In effect, the 21st Century CVAA creates a new regulatory regime to further promote equality. This part will analyse the operation of this dynamic law and examine the potential for increased accessibility created by expanding the regulatory pie by placing performance duties on certain designers and manufacturers.

A. Regulating the Digital Commons in the US: The 21st Century CVAA

The 21st Century CVAA promotes equality by creating new obligations upon people in the United States who produce material to be broadcast on the internet or television to people inside the United States. The duties in the 21st Century CVAA are contained in two broad titles. Title I enshrines universal design with respect to communication devices for the deaf, blind, and generally for persons with disabilities.\(^\text{153}\) Some of these provisions create a general right. Section 104, for example, creates a right to access to internet-based equipment and services:

> With respect to equipment manufactured after the effective date of the regulations established pursuant to this section, and subject to those regulations, a manufacturer of equipment used for advanced communications, including end user equipment, network equipment, and software, shall ensure that such equipment that such manufacturer offers for sale or otherwise distributes in interstate commerce shall be accessible to and usable by individuals with disabilities, unless soothe requirements of this subsection are not achievable.\(^\text{154}\)

Even where it is not economically viable to include accessibility features in a product, designers and manufacturers have duties not to create products which prevent people with disabilities from using adaptive technologies to use those products. “Each provider of advanced communications services has the duty not to install network features, functions, or capabilities that impede accessibility or usability of advanced communications services.”\(^\text{155}\) These duties are not absolute. The duty is to make reasonable efforts and should not be read to require “every feature and function of every device or service [to be rendered] accessible for every disability.”\(^\text{156}\)

Some of the provisions in Title I provide more disability-specific protections. An example of a specific protection for persons with deafness is


\(^{154}\) Id. at §§617(a)(1) (Supp. V 2011).


found in 21st Century CVAA §102. Section 102 requires designers and manufacturers who create telephones to ensure that they are accessible for people using hearing aids. The United States Federal Communications Commission (“FCC”) explains that, in the future, designers and manufacturers of smart phones will be required to ensure that they are accessible to people with blindness and deafness.

Title II of the 21st Century CVAA focuses on increasing people with disabilities’ access to video programming broadcast on the internet and television. One of the primary ways the 21st Century CVAA increases accessibility is by requiring film producers to comply with audio and text captioning guidelines. The introduction in the 21st Century CVAA of video description, captioning, telecommunications relay services, and other film accessibility features will arguably make “media and telecommunications more accessible to people with disabilities.”

B. Improving Accessibility through Universal Design: The 21st Century Communications and Video Accessibility Act

One of the regulatory vehicles proposed by the CRPD to reduce discrimination is the adoption of universal design principles. Article 2 of the CRPD defines universal design as "the design of products, environments, programmes and services to be usable by all people, to the greatest extent possible, without the need for adaptation or specialized design." Universal design can be distinguished from reasonable accommodations or adjustments. Reasonable accommodations occur where an inaccessible environment is altered to enable persons with disabilities to use the environment. Universal design does not involve modifications to environments after it has been developed. Universal design focuses upon creating an environment that is fully inclusive from the outset.

State parties agree to “ensure and promote” all the rights contained in the CRPD by adopting all necessary legislative and policy vehicles to implement the
This includes regulatory vehicles targeting any “person, organization or private enterprise” that can promote or detract from the realization of the rights of persons with disabilities.

The significance of the 21st Century CVAA is that it adopts a universal design model to removing equalities in society. The 21st Century CVAA does not wait until a product is created to make reasonable adjustments. The 21st Century CVAA recognises that many of the barriers in society can be best removed by the people who create them at the design and manufacture stage. On signing this act into law, President Obama observed that the 21st Century CVAA:

will make it easier for people who are deaf, blind or live with a visual impairment to do what many of us take for granted from navigating a TV or DVD menu to sending an email on a smart phone...set[ting] new standards [98] so that Americans with disabilities can take advantage of the technology our economy depends on.  

The regulatory premise underpinning the 21st Century CVAA is that society should attempt to avoid creating inequalities where it is economically reasonable to do so.

Where anti-discrimination laws largely only focus upon parties who have a direct relationship with people with disabilities, the 21st Century CVAA embraces the notion that in certain situations, people have obligations to promote equality even if they never have direct contact with a person with a disability. Traditional anti-discrimination laws rely on prohibiting discrimination through the use of negative duties. The 21st Century CVAA utilizes performance standards that require positive conduct. Performance standards set a desired outcome and let duty holders determine how to achieve the prescribed performance. Performance standards can achieve positive outcomes, as they encourage duty holders to seek out and identify strategies to achieve desired performance targets. While the performance targets set in the 21st Century CVAA may not be perfect, enacting such targets represents a positive step by the legislature to set equality targets and to expand the regulatory pie.

162.  Id. at art. 4(1)(a).
163.  Id. at art. 4(1)(e).
C. Enforcing the 21st CCVA

The transformational potential of the 21st Century CVAA could be reduced by issues of enforcement. As the designers and manufacturers in the 21st Century CVAA do not have direct contact with people with disabilities, this creates a problem of who has standing to sue for noncompliance. Section 104 of the 21st Century CVAA introduced a complaints mechanism to the FCC.\(^\text{167}\) Under this regime, people can make formal and informal complaints to the FCC. After receiving a complaint, the FCC must resolve the complaint within 180 days.\(^\text{168}\)

If the FCC determines that there has been a breach, then the FCC can require a designer or manufacturer to remedy the breach.\(^\text{169}\) The FCC cannot bring legal sanctions against a designer or manufacturer, nor can a complainant seek damages. While the enforcement mechanisms in the 21st Century CVAA may reduce the effectiveness of the intervention, this regime does provide a model of how laws can promote equality by expanding the parties that attract duties.

V. REGULATING FOR SYSTEMIC EQUALITY: GENERAL DUTIES UNDER THE EQUALITY ACT 2010

The problem with the structure of traditional anti-discrimination laws is that duty holders are focused on avoiding prohibited conduct and not upon avoiding discrimination. Leading scholars have identified that traditional anti-discrimination laws lack the capacity to significantly address systemic inequalities.\(^\text{170}\) The limitations of regimes relying upon negative duties and the

---

168. Id. at § 618 (3)(B).
169. Id. at § 618 (3)(B)(i).
170. Martin Malin, *Do Cognitive Biases Infect Adjudication? A Study of Labor Arbitrators*, 11 U. PA. J. BUS. & EMP. L. 175, 176-78 (2008) (arguing that stereotypes are unconscious habits of thought that link personal attributes to group membership and presenting a study of whether irrelevant characteristics of a grievant in an arbitration conducted pursuant to a collective bargaining agreement affect the outcome of the grievance); Deborah Rhode, *The Subtle Side of Sexism*, 16 COLUM. J. GENDER & L. 613, 617 (2007) (arguing that there is a subtle side of sexism, a cluster of social expectations and practices that reinforce sex-based inequality); Susan Sturm, *Second Generation Employment Discrimination: A Structural Approach*, 101 COLUM. L. REV. 458, 556-64 (2001) (arguing that cognitive bias, structures of decision making, and patterns of interaction have replaced deliberate racism and sexism as the frontier of much continued inequality and exploring the potential for a de-centered, holistic, and dynamic approach to these more structural forms of bias). For a discussion of positive duties in Australia see Paul Harpur, *A Proactive Duty to Eliminate Discrimination in Victoria*, 19 AUSTL. J. ADMIN. L. 180 (2012) (analysing Australia’s first positive legislative duty protecting persons with disabilities in the Equal Opportunity Act 2010). This duty requires more of duty holders. Under Part 3, duty holders must, through a proactive audit process, seek out and eliminate structural inequalities where it is reasonable and proportionate to do so.
benefits of proactive duties were considered in a report published by Professors Bob Hepple, Mary Coussey and Tufyal Choudhury.\textsuperscript{171} Hepple, Coussey and Choudhury recommended a structural approach to ensuring equality. These authors argued that laws should create four new duties upon parties: “(1) a positive duty on public authorities to advance equality; (2) proactive duties on private sector employers to achieve employment equity or fair participation; (3) proactive duties on employers to introduce pay equity schemes; and (4) the use of contract and subsidy compliance as a sanction and incentive.”\textsuperscript{172}

The recommendations in the Cambridge Report were grounded upon considerable targeted case studies of employers across the United Kingdom and United States. The Cambridge Report led directly to a private members bill by Lord Lester of Herne Hill QC which was not enacted into law.\textsuperscript{173} Seven years later, however, a watered down version of the 2003 private members bill was enacted into law becoming the Equality Act 2010. This part will analyse the capacity of the public sector positive duties contained in the Equality Act 2010 Part 11, Chapter 1 to facilitate persons with disabilities’ access to the digital commons.

A. Positive Duties Advancing Rights: The Equality Act 2010

The equality duty in the Equality Act 2010 requires public authorities to give “due regard to the need to . . . eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under this Act.”\textsuperscript{174} Parties that develop and manage digital commons in the United Kingdom attract duties not to discriminate. The equality duty requires public authorities to take proactive conduct to eliminate access discrimination on their own websites. However, the equality duty is not limited to digital commons that public authorities control. To discharge the equality duty, a public authority is required to “remove or minimise disadvantages” and “take steps” to increase participation in public life.\textsuperscript{175} Accordingly, the equality duty requires public authorities to

\begin{enumerate}
\item Hepple, supra note 78, at 127.
\item Equality Act, 2010, c. 15, § 149 (U.K.). For application of this section see Ashley Bowes, R. (Luton) v Secretary of State for Education: A Case Note, 16 JUD. REV. 156 (2011) (considering the Administrative Court decision in R. (on the application of Luton BC) v Secretary of State for Education on whether, by cancelling the Building Schools for the Future (BSF) school refurbishment programme launched in 2003 by the New Labour administration, the Secretary of State had: (1) acted irrationally; (2) fettered his discretion under the Education Act 2002 s.14(1); and (3) breached the substantive and procedural legitimate expectation of schools that were in the process of applying for funding).
\item Equality Act, 2010, c. 15, § 149(3) (U.K.).
\end{enumerate}
focus on what they can do to eliminate discrimination and not to focus exclusively upon their own internal operations.

While public authorities have a duty to seek to eliminate discrimination in the wider community, the coverage of the equality duty is clearly a limitation. The coverage of the equality duty differs markedly from that of traditional anti-discrimination duties. Unlike direct and indirect discrimination, the positive duty in the Equality Act 2010 only applies to public authorities. While this is a limitation, the existence of the equality duty follows a trend of expanding proactive anti-discrimination duties in the United Kingdom. The United Kingdom has a history of expanding the operation of positive duties. The Fair Employment (Northern Ireland) Act 1989 (U.K.) included positive duties upon large employers to reduce tension between Catholic and Protestant communities by achieving fair participation at work.176 The Northern Ireland Act 1998 (U.K.) extended employers’ positive duties to promote equality in respect of religion, age, disability, race, religion, sex, marital status, and sexual orientation.177 Now, the Equality Act 2010 has included positive duties upon public authorities to give due regard to the need to eliminate discrimination, harassment, victimisation, and other conduct prohibited under this regime. If the positive duty in the Equality Act 2010 is an effective regulatory vehicle, then it is possible that this duty will be expanded to other relationships.

B. A Regulatory Analysis: How Positive is the Equality Duty?

There is a scholarly consensus that positive duties are more effective than traditional negative duties in ensuring equality.178 The regulatory challenge is to convert the intent of the statute to results on the ground.179 Frank Dobbin and Alexandra Kalev tested the claim that a structural approach is necessary to combat the prevalence of structural discrimination.180 They found, not surprisingly, that simply having anti-discrimination policies will not reduce discrimination. To be effective, equity programmes must be institutionalised and

180. Frank Dobbin and Alexandra Kalev, Multi-Disciplinary Responses to Susan Sturm’s the Architecture Of Inclusion: The Architecture Of Inclusion: Evidence from Corporate Diversity Programs, 30 Harv. J.L. & Gender 279 (2007) (exploring the generalizability of some of Sturm’s findings to the corporate world using unique data from a longitudinal study of diversity efforts at more than 800 American firms over thirty years).
have an expert leading the programme. Second, there must be public accountability and support for the implementation of these equity plans. This accountability must contain a punishment for noncompliance and provide duty holders with guidance about the processes they should follow to combat discrimination. This part will now use regulatory theory to test whether the equality duty is likely to be institutionalised and whether the enforcement vehicles are likely to promote compliance.

The Equality Act 2010 contains a number of steps that public authorities should adopt to give due regard to promoting equality. With respect to promoting the rights of persons with disabilities, the Equality Act advises that: “The steps involved in meeting the needs of disabled persons that are different from the needs of persons who are not disabled include, in particular, steps to take account of disabled persons’ disabilities.” If the steps in the Equality Act 2010 were implemented, then this would arguably promote the rights of persons with disabilities and increase their access to digital commons.

The regulatory challenge is to turn well-intentioned objectives into substantive changes on the ground. One of the most effective processes to achieve continuous change is through management systems. In their seminal work, Cary Coglianese & David Lazer explained the regulatory criteria for effective systems-management processes. An effective system-management process will contain processes to identify hazards, processes to mitigate the hazards identified, procedures for monitoring and correcting problems, training policies for workers, and measures for evaluating and refining the system.

While the Equality Act 2010 and the associated regulations do not prescribe a management-systems approach, a form of this approach has been recommended in non-binding Equality and Human Rights Commission guidelines. The essential guide to the public sector equality duty explains that the equality duty “requires equality to be considered in decision-making, in the design of policies and in the delivery of services, including internal policies, and for these issues to be kept under review.” Unfortunately, the essential guide to the public sector equality duty does not clarify how agencies should consider and...
review processes. Whether considerations and reviews will achieve significant change will depend upon the criteria that guides these processes.

C. Priorities and the Equality Duty: Public Authorities’ Conduct and Access to Digital Commons

The equality duty can only be said to have made a difference if public authorities go further to promote equality than they would have done under existing traditional anti-discrimination duties. The potential impact of positive duties can be emphasised by contrasting them with traditional negative duties. Traditional anti-discrimination duties require duty holders to respond to access when they are confronted by a person with a disability. This means that most work systems are created without considering the needs of persons with disabilities. For example, under direct and indirect discrimination provisions, employers’ duties limit what is reasonable by deciding what adjustments would impose an unjustifiable hardship on the employer once the work system has been established. In relation to employers’ duty, Hepple explains that “an employer is not required to anticipate the needs of potential disabled employees or job applicants.”188 Employers only have duties to make reasonable adjustments if they have actual or imputed knowledge of a person with a disability as an employee or job applicant.189 The fact employers need not be proactive is one of the greatest limitations with traditional anti-discrimination laws. Arguably, laws that fail to assess the cost of reasonable adjustments at the development stage permit the creation of new barriers and effectively endorse discriminatory practices.190

To accurately map the impact of the equality duty is a project in itself. However, it is possible to obtain an understanding of how public authorities are devoting equality resources. Public authorities’ obligation under the equality duty applies to all protected attributes in the statute. This includes discrimination based upon age; disability; gender reassignment; marriage and civil partnership; pregnancy and maternity; race, religion, or belief; sex; and sexual orientation.191 It is probable that with so many attributes to protect, that the efforts of public authorities may focus upon instances of discrimination that

188. Hepple, supra note 78, at 77; Equality Act, 2010, c. 15, sch. 8 (U.K.).
190. Baker & Godwin, supra note 57, at, 59 (analysing the Canadian Supreme Court judgment Council of Canadians with Disabilities v. VIA Rail Canada Inc. [2007] 1 S.C.R. 650 (Can.). In this case, the defendant knowingly purchased railway cars that were not accessible to persons with disabilities. The defendant then argued that it would be too expensive to render the cars accessible.).
attract particular public attention. Due to this problem, less vocal issues or attributes may receive inadequate attention.

The operation of the Equality Act 2010 (Specific Duties) Regulations 2011 (U.K.) means it is possible to determine the extent to which public authorities are considering disability-related issues and issues related to access to digital commons. After following the procedures in the Equality Act 2010, the Equality Act 2010 (Specific Duties) Regulations 2011 (U.K.) became binding law. Under the Equality Act 2010 (Specific Duties) Regulations 2011 (U.K.), public authorities are required to publish how they have complied with the equality duty on an annual basis. The publication must contain details on the conduct they have taken to promote equality that have impacted upon their employees and upon the wider community. These publications provide raw data, which facilitates public debate on how the equality duty is enforced. Scholars and disability person organizations will need to utilize these public reports to critically analyse the nature of government conduct and the effectiveness of the regulatory regime.

D. Enforcing the Equality Duty

The equality duty under the Equality Act 2010 does not create a private right of action. Rather than relying upon victim enforcement, the Equality Act 2010 relies upon the offices of the Equality and Human Rights Commission to ensure compliance. This section will analyse the three vehicles the Equality and Human Rights Commission use to enforce compliance with the equality duty.
The Equality and Human Rights Commission can decide to conduct an inquiry on its own motion.\textsuperscript{199} The purpose of these investigations is not to detect noncompliance of individuals. Indeed, if during the course of an inquiry the “the Commission begins to suspect that a person may have committed an unlawful act,” then the Commission must, “so far as possible, avoid further consideration of whether or not the person has committed an unlawful act.”\textsuperscript{200} If the Commission uncovers evidence that may indicate there has been a breach of the law, then this evidence can be used in a subsequent formal investigation into the individual in question.\textsuperscript{201}

Own motion reports have limited capacity to alter conduct. In releasing a report on an own motion inquiry, the Commission cannot state, “whether expressly or by necessary implication,” that a person has committed an unlawful act.\textsuperscript{202} Furthermore, the findings of such an investigation are not legally binding upon named people, however, courts may take such findings into consideration.\textsuperscript{203} The limited role of own motion investigations reflects a trend in the U.K. against such investigations.\textsuperscript{204}

If the Equality and Human Rights Commission desired to name a specific party or enforce sanctions against them, then the primary vehicle to do this is through a formal investigation. These formal investigations enable the Commission to investigate whether a person has committed an unlawful act or has breached an unlawful act notice under section 21 of the Equality Act 2006.\textsuperscript{205} The Commission can only commence a formal investigation where it has a reasonable suspicion that the relevant person has perpetrated an unlawful act.\textsuperscript{206} Bob Hebble has observed: “A single complaint of unlawful conduct is unlikely to suffice as the basis for initiating an investigation, but a series of complaints over time might be sufficient. The suspicion may (but need not) be based on the matters arising in the course of an inquiry.”\textsuperscript{207} As most digital platforms are publically available, or available once an account has been established,


\textsuperscript{199} Equality Act, 2006, c. 3, § 16 (U.K.).

\textsuperscript{200} Id. at § 16(2)(a).

\textsuperscript{201} Id. at §§ 16(2)(b) & (c).

\textsuperscript{202} Id. at § 16(3)(a).

\textsuperscript{203} Id. at sch. 2, ¶ 17.

\textsuperscript{204} For a discussion of this trend as it applies to the Commission for Racial Equality see Mary Coussey, \textit{The Effectiveness of Strategic Enforcement in the Race Relations Act 1976, in Discrimination: The Limits of Law 37–40} (Bob Hepple and Erika M. Szyszczak, eds., 1992).

\textsuperscript{205} Equality Ac, 2006, c. 3, § 20(1) (U.K.).

\textsuperscript{206} Id. at § 20(2). The requirement that the Commission holds a reasonable belief has been set as the standard of conduct by the executive and not by statute. Hepple, supra note 78, at 152 (citing Equality and Human Rights Comm’n, The Government’s Response to Consultation ¶ 38 (2004)).

\textsuperscript{207} Hepple, supra note 78, at 152; Equality Act, 2006, c. 3, § 20(3) (U.K.).
determining whether there is a barrier to inclusion is relatively easy. However, it may be more difficult to ascertain whether or not a public authority has given due regard to ensuring such platforms are accessible.

If the Commission performs a formal investigation and concludes that a person has breached the law, then the Commission can issue an unlawful act notice. An unlawful act notice is a declaration that the person in question has been found to have breached equality laws. In addition to some procedural points, the unlawful act notice may: “(a) require the person to whom the notice is given to prepare an action plan for the purpose of avoiding repetition or continuation of the unlawful act; or (b) recommend action to be taken by the person for that purpose.”

Under section 22, a person who is required under an unlawful act notice to create an action plan must find strategies within their organization to ensure the unlawful conduct ceases. This plan is then given to the Commission who may approve the action plan or may reject the action plan and recommend alterations. If a person fails to comply with an action plan, an order can be made to a court which can impose a fine.

There is a good probability that the action plan model under the Equality Act 2006 will facilitate significant reductions in discrimination in the U.K. The ideal vehicle to enforce meta-regulation is through the process of encouraging duty holders to develop their own plans and having these plans authorised and enforced by a regulator. This approach generally encourages regulated parties to focus more on systemic problems than box ticking or complying with prescriptive regulations. This regulatory approach finds support in anti-discrimination scholarship. Susan Sturm has recommended that employers and private consultants could work collaboratively to identify the best methods of removing structural discrimination. These parties would share their findings with courts to empower judicial officers to more effectively scrutinize employer

209. Id.
210. Id.
211. Id. at § 22.
212. Id.
214. See generally CHRISTINE E. PARKER, THE OPEN CORPORATION: EFFECTIVE SELF-REGULATION AND DEMOCRACY (2002) (setting out a blueprint for effective corporate self-regulation). Examining the conditions under which corporate self-regulation of social and legal responsibilities is likely to be effective. Id.
215. Sturm, supra note 170, at 556-64.
VI. CONCLUSION

The CRPD has introduced a new human rights paradigm. Part I of this article analysed how this new model has increased obligations to ensure rights. The CRPD clearly articulates persons with disabilities’ rights and imposes on states an obligation to adopt a more holistic public policy agenda. This agenda requires states to first seek to regulate for universal design. Where universal is not practical, then states are required to ensure that reasonable adjustments are made to enable persons with disabilities equal access to the physical environment, to transportation, and to information and communications, including information and communications technologies and systems.

Traditional anti-discrimination laws in the United Kingdom and United States will not meet state obligations under the new paradigm introduced by the CRPD. Part III used the CRPD to critically analyse the traditional anti-discrimination regimes in the U.K. and U.S. Traditional anti-discrimination laws did not include commands that could ensure equality and that existing victim enforcement regimes are inadequately enforced.

Parts IV and V introduced new legislative models that have the potential of improving the capacity of persons with disabilities to exercise their rights. Part IV analysed the 21st Century CVAA. This transformational regime expands the parties who are regulated by equality duties and creates limited positive duties. Through introducing limited universal design obligations, the 21st Century CVAA creates a regime that targets barriers to equality before they are created. Part V analysed the positive duties under the United Kingdom’s Equality Act 2010. The positive duties require public sector agencies to give due regard to the need to eliminate discrimination, harassment, victimisation, and any other conduct that is prohibited by or under the Equality Act 2010. If enforced, the positive duties in the 21st Century CVAA and Equality Act 2010 will increase consideration of access issues before barriers to inclusion are created. The introduction of the 21st Century CVAA and the positive duties in the Equality Act 2010 advance the rights of persons with disabilities. This article has analysed the 21st Century CVAA and the positive duty in the Equality Act 2010 before these regimes have developed considerable case law. While the anti-discrimination model has provided benefits to persons with disabilities, this model needs to be reformed to promote equality in a way that is compatible with the human rights paradigm found in the CRPD.

THE ROLE AND EFFECT OF SOCIAL MEDIA IN THE WORKPLACE

Francois Quintin Cilliers*

I. INTRODUCTION

“[B]usinesses need to fully transform to properly address the impact and demands of social media.”1 This article analyzes the role and effect of social media in the modern workplace. Although social media is still a relatively new concept in labour relations, its influence on workplace dynamics could cause difficulties if left unregulated.2 Technological and media advancements provide advantages in labour relations including employment advertisements,3 employee communications,4 workers compensation,5 and collective bargaining.6 Apart from the risks that social media poses in the workplace; it can also positively

---

* Mr. Francois Quintin Cilliers LLB, LLM (UFS) is a lecturer in the Department Mercantile Law at the University of the Free State.

2. David Kelleher, 5 Problems with social networking in the workplace, INFO. MGMT. (Oct. 6, 2009, 11:27 AM), http://www.information-management.com/specialreports/2009_165/social_networking_media-10016208-1.html (explaining that by allowing access to social networking at work an employer may experience problems with: 1) productivity, 2) bandwidth, 3) viruses and malware, 4) social engineering, and 5) reputation and legal liability).
4. Ryan C. Daugherty, Around the Virtual Water Cooler: Assessing, Implementing and Enforcing Company Social Media Policies in Light of Recent National Labor Relations Board Trends, MMLK.COM (2011), http://www.mmlk.com/Around-the-Virtual-Water-Cooler-published-AugSept.pdf (explaining that employee communications on social networking websites may be protected concerted activity under the National Labor Relations Act if these communications relate to the terms or conditions of employment. “Three recent NLRB actions . . . have clarified that social networking communications are on its radar screen, and included in the “concerted activities” it will protect.”).
5. Derek Sanky, Be aware of social media benefits, risks, WINNIPEG FREE PRESS (2012), http://www.winnipegfreepress.com/business/be-aware-of-social-media-benefits-risks-138701469.html (“Evidence from social media sites has also been used in workers’ compensation benefits claims, usually in an attempt to show that the claimant is more able to work than he or she claims.”).
6. Id. (discussing the use of social media in the collective bargaining context to share information, to gain support, and to stop the spread of false rumours).
influence employment. According to a survey of approximately 1,400 college students, "[m]ore than half of college students (56%) [indicated that] if [they] encountered a company that banned access to social media, they would either not accept a job from it or would accept the job and find a way to circumvent corporate policy." Similarly, a survey found that thirty-three percent of young professionals have "Considered the Unrestricted Use of Mobile Devices and Social Media at Work When Making the Decision to Accept or Reject a Job Offer."

Clearly, the use of social media entails some risk on the employer’s side, but it also has an effect on employee interests. Applicants may not expect a prospective employer to do background research using social media, but there are no regulations that allow, restrict, or limit such a possibility. The lack of statutes and regulations regarding the usage of social media in the hiring process

---

7. Kelleher, supra note 2 (describing employers’ benefits from social networking to include: expanding market research, providing a personal touch to clients, improving a company’s reputation, and providing low-cost marketing).

8. CISCO, THE FUTURE OF WORK: INFORMATION ACCESS EXPECTATIONS, DEMANDS, AND BEHAVIOR OF THE WORLD’S NEXT GENERATION WORKFORCE 2 (Nov. 2, 2011), available at http://www.cisco.com/en/US/solutions/ns341/ns525/ns537/ns705/ns1120/cisco_connected_world_technology_report_chapter2_press_deck.pdf [hereinafter CISCO PRESS DECK] (referencing an online survey from May 13, 2011 to June 8, 2011 that included 1,441 college students (age 18–24) in fourteen countries (United States, Canada, Mexico, Brazil, United Kingdom, France, Spain, Germany, Italy, Russia, India, China, Japan, and Australia)).

9. Id. at 6. See also Georgina Terry, "Can We Tweet?" Seems to be the question, 4 LINKAGE 1,18 (2011), available at http://www.amchamtt.com/Downloads/Linkage%20Q4-11.pdf.

10. CISCO, 2011 CISCO CONNECTED WORLD TECHNOLOGY REPORT 17 (2011), available at http://www.cisco.com/en/US/solutions/ns341/ns525/ns537/ns705/ns1120/2011_cisco_connected_worldtechnology_report_chapter_2_report.pdf [hereinafter CISCO REPORT] (referencing an online survey from May 13, 2011 to June 8, 2011 that included 1,412 full-time employees (age 21–29) with college degrees in fourteen countries (United States, Canada, Mexico, Brazil, United Kingdom, France, Spain, Germany, Italy, Russia, India, China, Japan, and Australia)); CISCO PRESS DECK, supra note 8, at 2.

11. Kelleher, supra note 2 ("[T]aking a heavy-handed approach could be counterproductive, indicate a lack of trust in employees . . . and is too restrictive.").

12. Benedict, supra note 3, at 7 ("Most users of social media sites mistakenly believe that the personal information they post for their “friends” to view is private . . . ."). But see Jenna Wortham, A Pair of Social Media Predicaments, N.Y. TIMES GADGETWISE (Nov. 23, 2009), http://gadgetwise.blogs.nytimes.com/2009/11/23/a-pair-of-social-media-predicaments/ ("A recent study conducted by Harris Interactive for CareerBuilder.com determined that 45 percent of employers questioned were using social networks to screen job candidates – more than double from a year earlier, when a similar survey found that just 22 percent of supervisors were researching potential hires on social networking sites like Facebook, MySpace, Twitter and LinkedIn.").

13. See generally Cara R. Sronce, The References of the Twenty-First Century: Regulating Employers’ Use of Social Networking Sites As an Applicant Screening Tool, 35 S. ILL. U. L.J. 499, 500 (2011) ("Because of the many concerns surrounding SNS technology use by employers, some legal scholars advocate laws to regulate employers' use of social-networking site.").
creates uncertainty for employers and employees. There is similar uncertainty regarding employees’ online disclosure of information about their employer and employment conditions. It is unclear how much information an employee may share online before the disclosure constitutes a breach of contract, unfair discrimination, or other misconduct. Will similar use of social network sites outside of the workplace still constitute a labour offense? Could service providers be held liable for an offense created through the disclosure or use of its information systems?

Social media has become a deciding consideration in employment litigation and modern labour relations. “Increased employee use of technology is resulting in greater rates of employee misuse, discipline for such misuse, and, ultimately, litigation.” Most employers have drafted workplace policies to address employees’ use of social media and their potential misuse of employers’ systems. Generally, these policies do not encompass all the applicable aspects and safeguards necessary to create clear, enforceable rules or to ensure that employees comply with the provisions.

14. See, e.g., Wortham, supra note 12 (referencing an applicant’s dilemma: “I’m applying for a new job and there is some unflattering stuff on the Web that I would be really embarrassed if even my parents – let alone a potential employer – were to see. But is it really necessary to delete anything that a potential employer might happen to see online?”).

15. Daugherty, supra note 4 (discussing recent complaints filed by the National Labor Relations Board that signal social media firings as “a new area of concern for employers.”).

16. See Kelleher, supra note 2 (“[O]rganizations need to watch for employees who may be commenting publicly about their employer. For example, one young employee wrote on her profile that her job was boring and soon received her marching orders from her boss. What if a disgruntled employee decided to complain about a product or the company’s inefficiencies in his or her profile?”).

17. See 47 U.S.C.A. § 230(c) (West 2013) (“No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”).

18. Daugherty, supra note 4 (“Social media data has become a notable consideration for employers – as part of the hiring process, as a marketing tool, as a productivity concern – and increasingly as a material factor in employment litigation.”).


20. Id. (“Statistics show that . . . most employers have adopted policies relating to electronic use . . . .”). See also Daugherty, supra note 4 (“Most employers have considered, if not implemented, social media-specific employee policies to complement their pre-existing workplace policies and procedures.”).

21. Kelleher, supra note 2 (discussing that employees may use their employer’s system “to view objectionable, illicit or offensive content.”).

22. See Daugherty, supra note 4 (“It is important for companies to avoid thoughtlessly implementing overly broad or generic social media policies, and to narrowly tailor such policies in light of the National Labor Relations Act, applicable state statutes, and their company goals and peculiarities.”).
employers do not follow through with the monitoring and discipline outlined in their workplace policies. 23

Ensuring productivity in the workplace can be difficult for employers without established rules or policies to provide certainty regarding the proper use of internet facilities and media. 24 “Two-thirds of online American adults (67%) are Facebook users, making Facebook the dominant social networking site in” the United States (“U.S.”). 25 Because most online adults use social media, 26 lack of employer guidance may lead to situations where employees spend the majority of their time socializing on platforms like Facebook or Twitter. 27 Employers and employees need certainty on legal informatics and its role in the workplace, especially regarding the use of social media. 28 As technology and electronic systems advance so too should the applicable labour laws and employers’ workplace policies. 29

23. Thompson, supra note 19, at 284 (“Statistics show that while most employers have adopted policies relating to electronic use, the majority of employers are not following through with appropriate monitoring and discipline.”).

24. See Kelleher, supra note 2 (“If every employee in a 50-strong workforce spent 30 minutes on a social networking site every day, that would work out to a loss of 6,500 hours of productivity in one year!”).

25. PEW RESEARCH CTR., PEW INTERNET & AM. LIFE PROJECT, COMING AND GOING ON FACEBOOK 2, 6-7 (2013), available at http://pewinternet.org/~media//Files/Reports/2013/PIP_Coming_and_going_on_facebook.pdf (referencing a phone survey conducted by The Pew Research Center in December 2012. The survey included 1,006 American adults, and was conducted in English on landline and cell phones. The survey results found 525 Facebook users out of 860 adult internet users.). The Pew Research Center is a nonpartisan fact tank that “conducts public opinion polling, demographic research, media content analysis, and other empirical social science research,” And can be found online at http://www.pewresearch.org/.

26. KATHRYN ZICHUHR, PEW RESEARCH CTR., PEW INTERNET & AM. LIFE PROJECT, GENERATIONS ONLINE 2010 16, 27 (Dec. 2010), available at http://pewinternet.org/~media//Files/Reports/2010/PIP_Generations_and_Tech10.pdf (referencing a phone survey conducted in 2010 by The Pew Research Center. The survey included 2,252 American adults, and was conducted in English on landline and cell phones. The survey results found that 61% of online adults use social network sites.).

27. Kelleher, supra note 2 (“The time spent using social networking applications is one reason why many businesses are reluctant to allow employees to use sites like Facebook, MySpace and LinkedIn during office hours.”). See also Thompson, supra note 19, at 285 (“Employees often use work time and break time to socialize and vent” on social network sites.).

28. See Benedict, supra note 3, at 60 (“To minimize the negative risks for employers, trade unions, and employees, clear and well-drafted social media policies should be implemented, well-advertised within the organization, and consistently enforced.”).

29. See Thompson, supra note 19, at 288, 293 (“Recent case law demonstrates that although employers appear to be getting the message that implementation of policies, monitoring, and discipline are a necessary part of controlling technology, they still have a very long way to go. . . . Policies created even two years ago are likely significantly outdated and thus worthless to address today’s changing technological landscape.”).
II. SOCIAL MEDIA IN GENERAL

Social media can be described as the use of web-based and mobile technology to convert communications into an interactive dialogue.\(^{30}\) Interactive or electronic communication is a form of indirect communication, because communicating parties are not “face-to-face.”\(^{31}\) In South Africa, the Regulation of Interception of Communications and Provision of Communication related information Act (“RICA”)\(^{32}\) defines indirect communication as:

a message or any part of a message, whether –
(a) in the form of –
   (i) speech, music or other sounds;
   (ii) data;
   (iii) text;
   (iv) visual images, whether animated or not;
   (v) signals; or
   (vi) radio frequency spectrum; or
(b) In any other form . . . that is transmitted . . . by means of a postal service or a telecommunication system.\(^{33}\)

According to a study in 2012, the top five social media platforms were Facebook, YouTube, Wikipedia, BlogSpot, and Twitter.\(^ {34}\) The same study found that social networks have thirty-six percent of the total unique visitors on the social media sites sampled.\(^ {35}\) Clearly, indirect communication through social media platforms is readily and easily available.

Some employers restrict the use of social media platforms throughout the working day by using a restricted-access protocol in their electronic systems.\(^{36}\) However, a restricted-access protocol might negatively effect employees’

---

30. See Media Definition, MERRIAM-WEBSTER ONLINE DICTIONARY, http://www.merriam-webster.com/dictionary/social (defining Social Media as “forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content”) (last visited July 14, 2013).
31. See id.
32. Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.
33. Id. at § 1.
35. Id. (including Facebook, Twitter, LinkedIn, and Google+ as social networks).
36. See Kelleher, supra note 2 (“Banning access to social networking sites may be an optimal solution for some organizations . . . .”).
morale\textsuperscript{37} and result in employees finding different ways to connect to social-media platforms.\textsuperscript{38} For example, employees may use mobile phones to connect to restricted sites or to otherwise circumvent an employer’s restrictions on use.\textsuperscript{39}

The availability of social-media platforms on mobile phones makes it difficult to enforce workplace policies that prohibit the use of social media during working hours\textsuperscript{40} as employees’ mobile phones are often not employers’ property.\textsuperscript{41} Because employees often own their mobile phones, there is decreased possibility for employers to monitor or intercept communications.\textsuperscript{42} Even when “employers purchase the technology for work purposes, they cannot fully control how employees actually use it.”\textsuperscript{43} By using a mobile phone, an employee could spend hours online without the employer’s knowledge.\textsuperscript{44}

III. EFFECT IN THE WORKPLACE

“Social Media is about sociology, not technology.”\textsuperscript{45} Social media can be used as a powerful marketing tool.\textsuperscript{46} People have a psychological need to interact with one another\textsuperscript{47} and social media helps to fill this need. Unfortunately, social

\textsuperscript{37} Id. ("[T]aking a heavy-handed approach could be counterproductive, indicate a lack of trust in employees . . . .").

\textsuperscript{38} See CISCO PRESS DECK, supra note 8, at 6 ("More than half of college students (56\%) if [they] encountered a company that banned access to social media, they would either not accept a job from them or would join and find a way to circumvent corporate policy.").

\textsuperscript{39} See Thompson, supra note 19, at 286 (discussing the ability of employees to use mobile phones for both work and personal use).

\textsuperscript{40} Id. ("While employers purchase the technology for work purposes, they cannot fully control how employees actually use it. Employees could just as easily be using the phone for work purposes as they could be text messaging a new love interest, surfing the Internet, emailing a friend, or blogging about politics or even the employer.").

\textsuperscript{41} See CISCO REPORT, supra note 10, at 36 ("Just 3 in 10 End Users Use a Personal Smartphone or Tablet for Work and Are Able to Expense the Mobile Data Subscription Plan.").

\textsuperscript{42} See 18 U.S.C. § 2701 (2012) (In the U.S., it is an offense to “(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.").

\textsuperscript{43} Thompson, supra note 19, at 286 (discussing employees’ use of employer-purchased mobile phones).

\textsuperscript{44} See id. ("Employees could just as easily be using the phone for work purposes as they could be text messaging a new love interest, surfing the Internet, emailing a friend, or blogging about politics or even their employer.").


\textsuperscript{46} Id.

\textsuperscript{47} See Elizabeth Vasiliades, Solitary Confinement and International Human Rights: Why the U.S. Prison System Fails Global Standards, 21 AM. U. INT’L L. REV. 71, 77 (2005) (discussing the impact of solitary confinement on prisoners. “The lack of social contact and environmental stimulation often results in extreme psychological problems, such as extraordinary malaise and increased violent tendencies.”).
media’s easy access also creates problems for employers as social media can become an addiction in the workplace and result in decreased productivity.\textsuperscript{48} The use of electronic systems, the internet, and email is commonplace in most businesses worldwide, and has become a necessity in the modern working environment.\textsuperscript{49} The accessibility of electronic social media creates strategic marketing opportunities for businesses.\textsuperscript{50} However, the use of electronic media must be genuine and participatory in order to properly leverage this communication channel when reaching out to people.\textsuperscript{51}

Workplace productivity can be maintained or improved through low-cost, instant, communication platforms available in social media.\textsuperscript{52} Social media provides employees with the ability to instantly communicate with other employees and clients.\textsuperscript{53} It also provides employees with online meeting capabilities that allow them to attend meetings and consultations without leaving their desks.\textsuperscript{54}

Electronic and social media have contributed to the steady flow of information within the workplace and established channels of communication with clients, co-workers, and peers.\textsuperscript{55} Social media greatly assists in the marketing and advertising aspects of any business that understands the “culture” of the social network platform it intends to use to communicate with its targeted clients.\textsuperscript{56}

\textsuperscript{48} Kelleher, supra note 2 (“One reason why organizations [ban] social networking in the workplace is the fact that employees spend a great deal of time updating their profiles and sites throughout the day.”).

\textsuperscript{49} Thompson, supra note 19, at 286 (“However, the use of technology in the workplace (and beyond) has evolved so significantly from simple computer use that an absolute bar to personal use of technology is not realistic and may actually interfere with employee productivity.”).

\textsuperscript{50} Solis, supra note 45 (“the future of marketing integrates traditional and social tools, connected by successful, ongoing relationship with media, influencers, and people.”).

\textsuperscript{51} Id. (“The conversations that drive and define Social Media require a genuine and participatory approach.”).

\textsuperscript{52} See Thompson, supra note 19, at 283, 286 (“The “virtual office” is now a reality and employers reap the benefits of this new flexible workplace with increased hours and almost unlimited access to employees at any time of the day (or night).” Employers have embraced employees’ use of smartphones “when they serve their own purposes -- increased employee accessibility, productivity, and connectivity . . . .”).

\textsuperscript{53} Id. at 285. (“They do not even need to leave their desks -- they send an e-mail, a link to a Web page, a text message or instant message -- knowing that the recipient will receive the message instantaneously.”).

\textsuperscript{54} Id.

\textsuperscript{55} Id.

\textsuperscript{56} Solis, supra note 45 (discussing the importance of understanding the culture of social networks before marketing to them: “The future of marketing integrates traditional and social tools, connected by successful, ongoing relationship with media, influencers, and people”). See also Kelleher, supra note 2 (describing employers’ benefits from social networking to include: expanding market research, providing a personal touch to clients, improving a company’s reputation, and providing low-cost marketing).
The National Labor Relations Board ("NLRB") has presumably recognized the integral part that social media plays within the modern workplace.\footnote{Daugherty, supra note 4.} As one author has explained, "it is very apparent that the NLRB intends to address social media communications as part of the NLRA, and to treat them similarly to old-fashioned water cooler conversations, regardless of when or where they occur."\footnote{Id.}

The use of social media even extends to collective labour relations.\footnote{Sanky, supra note 5 (discussing the use of social media in collective bargaining to share information, to gain support, and to stop the spread of false rumours).} For example, employers and union representatives have created controlled websites to inform employees and unions of the status of collective bargaining.\footnote{Id.} These websites help to keep workplace relations steady and peaceful, and, simultaneously, put false rumors to rest.\footnote{See id.}

In the current labor market, many prospective employees grew up with electronic systems and the flow of information through these systems as a part of their daily lives.\footnote{The Challenge and Promise of "Generation I", MICROSOFT NEWS CTR. (Oct. 28,1999), http://www.microsoft.com/en-us/news/features/1999/10-28geni.aspx (discussing a speech given in 1999 by Bill Gates, Microsoft's Chairman and CEO, where Bill Gates foreshadowed that the internet would change the way children learn, communicate, and work). Today's workforce has an increasing number of employees that were born in the 1980s and 1990s. Id.} If one considers this fact for a moment, it should become clear how utterly impractical it would be for an employer to prohibit this aspect of daily life within the workplace.\footnote{Thompson, supra note 19, at 286.}

There is a negative side to electronic and social media in the workplace.\footnote{Kelleher, supra note 2.} In general, there is a decline in productivity because employees spend time updating their profiles.\footnote{Id. ("One reason why organizations [ban] social networking in the workplace is the fact that employees spend a great deal of time updating their profiles and sites throughout the day.").} Additionally, employees’ downloading of videos and other online activities may require high levels of bandwidth, thus increasing the employers’ costs.\footnote{Id. ("Although updates from sites like Facebook or LinkedIn may not take up huge amounts of bandwidth, the availability of (bandwidth-hungry) video links posted on these sites creates problems for IT administrators. There is cost to Internet browsing, especially when high levels of bandwidth are required.").} Employers also face additional risks from employees’ usage of social media.\footnote{Id.} These risks may include: viruses infecting workplace
A. Use During the Employment Stage

“Privacy is dead, and social media hold [the] smoking gun.”

Generally, users are under the impression that the information they post on social-media platforms is private based upon their user settings. Users also believe that their right to privacy will protect their information from falling into the possession of unwanted third parties. Many job applicants do not expect that prospective employers will log into social-media platforms to research their online activities when determining whether they should be hired. However,
employers are legally allowed to view information of applicants that includes applicants’ photos and “status updates” on their social media profile.\textsuperscript{76}

Does the right to privacy provide any protection in these instances? Are employers allowed to use information obtained from a social-media platform as a valid and reasonable cause not to hire a particular applicant?\textsuperscript{77}

The Constitution of the Republic of South Africa guarantees the right to privacy to every South African citizen, and specifically states that the right to privacy includes “the right not to have . . . the privacy of their communications infringed.”\textsuperscript{78} The Fourth Amendment to the United States Constitution clearly protects against unreasonable search and seizure; however, it is less clear regarding the protection of the privacy of communications.\textsuperscript{79} In the U.S., if employers have a policy that includes the ability to “audit, inspect, and/or monitor employees’ use of the Internet,” employees do not have a reasonable expectation of privacy for their internet activity at the workplace.\textsuperscript{80} As such, employers may give permission for searches and seizures that would otherwise be illegal.\textsuperscript{81}

Similar to the U.S. and South Africa, the European Union (“E.U.”) has a directive for the “protection of individuals with regard to the processing of
personal data and on the free movement of such data.”82 Because this directive prohibits the transfer of personal data to countries outside of the E.U. that do not meet the E.U.’s adequacy standards for privacy protection, the U.S. Department of Commerce worked with the European Commission to develop the U.S.-E.U. Safe Harbor Framework (“Safe Harbor”).83 The Safe Harbor aims to ensure the free flow of personal information and enables organizations in the U.S. to participate by publicly declaring their compliance with the Safe Harbor Privacy Principles.84 The Safe Harbor is possibly one of the best codes of practice that can be applied in workplace policies when one considers the use and implications of social media during the employment stage. The Safe Harbor consists of the following seven principles:85

[1] Notice
Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.

[2] Choice
Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

[3] Onward Transfer (Transfers to Third Parties)
To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the Safe Harbor Privacy Principles or is subject to the Directive or another adequacy finding . . .


84. Id. See also R. VAN DER MERWE ET AL., INFORMATION AND COMMUNICATIONS TECHNOLOGY LAW 350 (2008).
Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual’s privacy in the case in question, or where the rights of persons other than the individual would be violated.

[5] Security
Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

[6] Data integrity
Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

[7] Enforcement
In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual’s complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization.

Recently, a teacher’s aide in Michigan was suspended for refusing to share her Facebook username and password with her employer. Her employer’s request was made after allegations that she had posted an improper photo on her Facebook profile. In the absence of U.S. legislation to provide clarity on the issue, cases of this nature will contribute to growing uncertainty. In South

86. Id.
88. Id. (posting a photo of a coworker that showed a pair of shoes and pants around the ankles).
89. In this regard, Van der Merwe states that the protection of information is poorly regulated in the United States. See R. VAN DER MERWE ET AL., supra note 84, at 349 (“The United States . . . tends to believe that the information industry should be left to regulate itself . . . . Legislation protecting data privacy in the United States is sectoral and haphazard.”). But see H.R. 537 (2013) (A bill was introduced in the U.S. in 2013 “[t]o prohibit employers and certain other entities from requiring or requesting that employees and certain other individuals provide a user name, password, or other means for accessing a personal account on any social networking website.”).
Africa, this type of request and use of information may result in an infringement of the Employment Equity Act.90

Under the Employment Equity Act, employers cannot unfairly discriminate against employees or applicants for employment based on race, gender, political opinion, religion, sexual orientation, HIV status, pregnancy, and other grounds.91 An applicant's political views and sexual orientation might not have been known to an employer had it not been for the information gained through the applicant's social media page. Regardless of the actual reason for not hiring an applicant, a court may infer that the applicant's sexual orientation or political views evidenced on social media was the employer's reason for not selecting the applicant.

The procurement and improper use of a prospective employee's personal information may have a permanent and damaging effect on the employment relationship.92 Trust may be lost between employees and employers, especially if prospective employees consider employers' actions an infringement of their right to privacy.93 Additionally, if an employer reviews an applicant's social media pages without the individual's knowledge, the employer risks breaching privacy laws in some countries.94

In South Africa, when deciding whether an individual's constitutional right to privacy has been infringed, the Constitutional Court of South Africa considers the following factors: (1) the manner in which the information was obtained;95 (2) the nature of the information;96 (3) the purpose for which the information was

---

91. Id. § 6 (“(1) No person may unfairly discriminate, directly or indirectly, against an employee, in any employment policy or practice, on one or more grounds, including race, gender, sex, pregnancy, marital status, family responsibility, ethnic or social origin, colour, sexual orientation, age, disability, religion, HIV status, conscience, belief, political opinion, culture, language and birth. (2) It is not unfair discrimination to – (a) take affirmative action measures consistent with the purpose of this Act; or (b) distinguish, exclude or prefer any person on the basis of an inherent requirement of the job.”).
92. Benedict, supra note 3, at 7 (“If an applicant learns that a prospective employer has accessed their personal social media site(s), there may be an irreparable loss of trust in the organization based on the perceived moral breach of privacy, even in the absence of a legal breach of privacy.”).
93. Id.
94. See, e.g., id. at 8 (referencing Canadian privacy law).
95. Mistry v. Interim Medical and Dental Council of South Africa, (4) SA 1127 (CC), 53 (1998) (indicating that a constitutional breach of privacy may be found if information is obtained in an intrusive manner).
96. Id. (implying greater constitutional protection for information about intimate aspects of personal life).
originally collected;\(^97\) and (4) the nature and manner of dissemination of the information.\(^98\)

In South Africa, the Electronic Communications and Transactions Act ("ECT") defines personal information as "information relating to race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual."\(^99\) Section 51 of the ECT indicates that "[a] data controller\(^100\) must have the express written permission of the data subject\(^101\) for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law."\(^102\) Thus, the ECT requires that an employer or its appointee obtain the written permission of employee or applicant before collecting any personal information on the employee or application, unless the employer is otherwise permitted or required by law to collect the information. In addition, the ECT states that "[a] data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required."\(^103\) As such, where an employer has the lawful ability to collect personal information on an employee or applicant, the employer can only collect information that is "reasonably necessary" to the lawful purpose. The ECT also prohibits a data controller from disclosing "any of the personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject."\(^104\)

The Promotion of Access to Information Act ("PAIA") aims to give effect to right to information provided for by the South African Constitution.\(^105\) According to the PAIA, an individual may request and gain access to any record

\(^{97}\) Id. (discussing that it may be unconstitutional to collect information for one purpose and use it for another).

\(^{98}\) Id. (considering whether the information was "disseminated to the press or the general public or persons from whom the applicant could reasonably expect such private information would be withheld.").


\(^{100}\) Id. § 1 ("[D]ata controller’ means any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject.").

\(^{101}\) Id. § 1 ("[D]ata subject’ means any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored.").

\(^{102}\) Id. § 51(1).

\(^{103}\) Id. § 51(2).


\(^{105}\) Promotion of Access to Information Act, Act 2 of 2000 (S. Africa) (giving “effect to the constitutional right of access to any information held by the State and any information that is held by another person and that is required for the exercise or protection of any rights; and to provide for the matters connected therewith.”).
access to a third party’s personal information is prohibited if such access unreasonably infringes upon the third party’s rights. Employers must adhere to the PAIA when requesting or seeking an applicant or employee’s personal information. When an employer approaches a data controller to obtain an employee’s personal information, the employee will be considered a third party protected under the PAIA. Additionally, the PAIA states that it is an offense to destroy, damage, falsify, or conceal information with the intent to deny a right of access to the information.

In South Africa, even though private communications are generally protected by the right to privacy, there is uncertainty whether information and communications that would normally be considered private, but which are published on a social-media platform which provides easy access to the public could still enjoy legal protection. After all, this information is added to the social-media platform by users who should be aware of the fact that it can easily be accessed by anyone, unless the user restricts access to only selected individuals.

106. Id. § 11(2) (“A request contemplated in subsection (1) includes a request for access to a record containing personal information about the requester.”).

107. Id. § 1 (“[P]ublic body’ means—(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or (b) any other functionary or institution when—(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or (ii) exercising a public power or performing a public function in terms of any legislation.”).

108. Id. § 11(1) (“A requestor must be given access to a record of a public body if – (a) that requester complies with all the procedural requirements in this Act relating to a request for access to that record; and (b) access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.”).

109. Id. § 34(1) (“[T]he information officer of a public body must refuse a request for access to a record of the body of its disclosure would involve the unreasonable disclosure of personal information about a third party, including a deceased individual.”); § 34(2) (granting exceptions to allow disclosure when 1) an individual consents, 2) individual was informed before giving information to a public body that it might be made available to the public, 3) information is already publicly available, 4) individual is under the care of the requestor and the information relates to such care, 5) individual is deceased and requester is the individual’s next of kin or appointed by the individual’s next of kin, or 6) individual is/was a public official).

110. Promotion of Access to Information Act, Act 2 of 2000 § 90 (“A person who with intent to deny a right of access in terms of this Act – (a) destroys, damages or alters a record; (b) conceals a record; or (c) falsifies a record or makes a false record, commits an offence and is liable on conviction to a fine or to imprisonment for a period not exceeding two years.”).


112. See, e.g., Facebook Legal Terms, supra note 73 (“You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings.”).
There is a possibility that an employer could obtain an employee’s personal information from a telecommunications or internet service provider. The ECT states that service providers113 will not be held liable for any infringement caused from the access or content of this information if it adhered to the industry’s code of conduct,114 acted as mere conduit115 for data messages,116 and only provided storage services or hosting services without knowledge of the content it was hosting.117 The U.S. has adopted similar provisions.118

In Texas, a court held no tort of intrusion upon seclusion occurred when an employer viewed employees’ posts on Facebook and subsequently terminated the employees because of the content in the posts.119 A court in California denied a former employee’s motion to dismiss when his former employer alleged that his continued use of a Twitter account was a misappropriation of trade secrets.120 Thus, employers’ social-media accounts may be regarded as trade secrets and former employees who use or steal these accounts may be guilty of misappropriation.121

114. Id. § 72 (“The limitations on on liability established by this Chapter apply to a service provider only if – (a) the service provider is a member of the representative body referred to in section 71; and (b) the service provider has adopted and implemented the official code of conduct of that representative body.”).
115. Id. § 73(1) (“A service provider is not liable for providing access to or for operating facilities for information systems or transmitting, routing or storage of data messages via an information system under its control, as long as the service provider – (a) does not initiate the transmission; (b) does not select the addressee; (c) performs the functions in an automatic, technical manner without selection of (d) does not modify the data contained in the transmission.”).
116. Id. § 1 (“‘[D]ata message’ means data generated, sent, received or stored by electronic means and includes – (a) voice, where the voice is used in an automated transaction; and (b) a stored record.”).
117. Id. § 75(1) (“A service provider that provides a service that consists of the storage of data provided by a recipient of the service, is not liable for damages arising from data stored at the request of the recipient of the service, as long as the service provider – (a) does not have actual knowledge at the data message or an activity relating to the data message is infringing the rights of a third party; or (b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent; and (c) upon receipt of a take-down notification referred to in section 77, acts expeditiously to remove or to disable access to the data.”).
118. 47 U.S.C. § 230(c) (2012) (“No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”). See also Shiamili v. Real Estate Grp. of N.Y., Inc., 952 N.E.2d 1011, 1017 (N.Y. 2011) (“Service providers are only entitled to this broad immunity, however, where the content at issue is provided by “another information content provider” (47 USC § 230[c][1]). It follows that if a defendant service provider is itself the “content provider,” it is not shielded from liability . . . ”).
119. Sumien v. CareFlite, No. 02–12–00039–CV, 2012 WL 2579525 (Tex. App. July 5, 2012) (Two employees were terminated after posting comments on Facebook related to their employment.).
121. Id.
Employers should not use information gained from a social-media site, like Facebook, during the employment process, unless such information has a realistic bearing on the decision to hire an employee or has a reasonable implication for the employee’s continued employment.\textsuperscript{122} Employees should be informed of any personal information that is in the possession of the employer and granted access to said information, when one considers the provision of South Africa’s ECT and PAIA.\textsuperscript{123}

**B. Effect after Employment**

People lose their inhibitions online and say things they would not normally say, look at things they would not necessarily want others to know they were looking at, and reveal things about themselves that normally would be private. Disgruntled current and former employees have not been able to resist the temptation to leak the employer’s confidential information online, or misappropriate such information for themselves or for a future employer.\textsuperscript{124}

The use of technology in the workplace is a given in today’s “Information Age.”\textsuperscript{125} Technology can not only improve productivity,\textsuperscript{126} contribute to effective marketing campaigns,\textsuperscript{127} improve communication in the workplace between employees, clients, and suppliers,\textsuperscript{128} but it can also ruin employment relations and the company’s image\textsuperscript{129} without regulation of employees during working hours. During working hours, employees can spend a lot of time online watching videos on YouTube,\textsuperscript{130} updating their status on Facebook,\textsuperscript{131} or browsing the internet searching for other employment opportunities.\textsuperscript{132} The possible negative implications of this behavior do not stop once the working day.

\textsuperscript{122} Stonce, supra note 13, at 513 (Otherwise, employers risk discriminating against applicants “based on race, age, marital status, sexual orientation, and many of the other personal characteristics easily discoverable on these pages.”).

\textsuperscript{123} See generally Electronic Communications and Transactions Act 25 of 2002 § 1(a) (S. Africa); Promotion of Access to Information Act, Act 2 of 2000 (S. Africa). See also 2009 Protection of Personal Information Bill (A South African bill that provides for the lawful collection and use of personal information.).

\textsuperscript{124} Thompson, supra note 19, at 286.

\textsuperscript{125} See id. at 283 (“Technology pervades American life both in and outside of the workplace.”); id. at 298 (“Interconnectivity through various technological media is the reality of the changing workplace.”).

\textsuperscript{126} Id. at 286.

\textsuperscript{127} Solis, supra note 45.

\textsuperscript{128} Thompson, supra note 19, at 285.

\textsuperscript{129} Benedict, supra note 3, at 5 (Employees can misuse social media “to the detriment of the employer-employee relationship in addition to the reputation of the business generally.”).

\textsuperscript{130} Thompson, supra note 19, at 285.

\textsuperscript{131} Kelleher, supra note 2.

\textsuperscript{132} Thompson, supra note 19, at 285.
There have been many instances where employees were dismissed due to remarks made on their personal blogs, Facebook, Twitter, and other social media platforms. The increased use of technology by employees will ultimately result in an increase in the misuse of information systems and litigation. Clearly, the modern employer is faced with challenges when deciding whether to allow the use of social media and, if allowed, how to regulate and use it in employment. One should not lose sight, however, of the employee’s duties and obligations that arise from the employment contract and common law. The employee’s duties are “to make his personal services available [to the employer], to “warrant” his competence and reasonable efficiency, to obey the employer, to be subordinate to the employer, to maintain bona fides, to exercise reasonable care when using the employer’s property, and to refrain from misconduct.” An employee’s unauthorized use of electronic systems to visit pornographic sites, to make defamatory remarks of the employer or workplace, or to spend hours on social media sites will probably constitute a breach of the majority of these duties.

Defamation is “the intentional publication of words or behaviour concerning another which has the tendency to undermine such a person’s status, good name or reputation.” In this sense, “publication” can include “posts” on social-media sites, and employees can be held liable for defamatory remarks posted on social-media sites.
Possible risks that can be incurred from employees misuse or ignorance of electronic systems and policies include:

- Disclosure of valuable and confidential information;
- Vicarious liability of employers;
- Increased costs;
- System inefficiency or delays in the use of the business e-mail systems;
- Dissemination of computer viruses or malicious code;
- Loss of productivity and system inefficiency due to the use of social networking sites;
- Reputational risk from negative publicity.

Employers can be held vicariously liable for an employee’s wrongful act; including defamation and any offense connected with child pornography, perpetrated by their employees if an employment relationship existed at the time the act was committed and the wrongful act was committed in the scope of employment. Can employers monitor employees’ communications and information on their computers at work?

According to RICA in South Africa, the monitoring and surveillance of communications are generally prohibited; however, RICA does provide that any person may authorize or give written permission to monitor or intercept any data communication, unless it is for unlawful purposes. RICA includes statutory exemptions to the prohibition of interception:

---

144. *See id.*
145. *Cyberlaw @ SA III, supra note 70, at 255.*
146. Kelleher, *supra note 2* (“There are also serious legal consequences if employees use these sites and click on links to view objectionable, illicit or offensive content. An employer could be held liable for failing to protect employees from viewing such material. The legal costs, fines and damage to the organization’s reputation could be substantial.”).
147. *Cyberlaw @ SA III, supra note 70, at 255.*
148. The Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 § 2 (S. Africa) (“[N]o person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission.”).
149. *Id. § 5* (“Any person, other than law enforcement officer, may intercept any communication if one of the parties to the communication has given prior consent in writing to such interception, unless such communication is intercepted by such person for purposes of committing an offence.”). *See also Cyberlaw @ SA III, supra note 70, at 282-83.* This includes electronic consent through express written electronic consent or by way of a “pop-up” screen where the employee need only agree to the employer’s electronic communication policy. In the case of the latter, this policy should be easily accessible to the employee.
150. The Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 § 3 (S. Africa).
[1] Where the intercepting party is also party to the communication.\footnote{151} Considering that the employee might use the property of the employer to log onto social media sites and post damaging information, the employer could possibly be regarded as a party to the communication, as the scope of a person’s privacy only extends to those issues where the person has a legitimate expectation of privacy, which may not include e-mail and internet use on the workplace’s assets.\footnote{152}

[2] Where a party to a communication has provided prior written consent to the interception.\footnote{153} A policy included in the employee’s employment contract (and consistently implemented in the workplace) would probably give effect to this exception.

[3] Where interception occurs in the carrying on of business.\footnote{154} This is also known as the “business interception” and may only be carried out with the consent of the system controller, for the purpose of obtaining evidence during an investigation of unauthorised use of a communication system which is mainly used for business purposes.\footnote{155} However, the users (employees) have to be notified of that “indirect communications transmitted by means thereof may be intercepted.”\footnote{156}

[4] Where interception prevents serious bodily harm\footnote{157} or determines the location of a person in the case of an emergency.\footnote{158}
Where the interception takes place in prison.159
Where monitoring takes place for the purposes of maintenance or installation of telecommunication equipment.160

In South Africa, the Basic Conditions of Employment Act (“BCEA”) states that “[e]very employee has the right to . . . discuss his or her conditions of employment with his or her fellow employees, his or her employer, or any other person[.]”161 Employees will enjoy protection where any information shared is concerned with only their conditions of employment, nothing more.162

In the U.S., the National Labor Relations Act contains a similar provision that protects employees’ “concerted activities,” which include situations where employees act together to improve working conditions.163 Recent actions by the National Labor Relations Board (“NLRB”) indicate that concerted activities may also include employee discussions using social media.164

an oral interception direction; and (c) the sole purpose of the interception is to prevent such bodily harm.”).

158. Id. § 8 (A telecommunication service provider must intercept any communication from the sender or determine the location of the sender when a law enforcement officer orally requests this information. A law enforcement officer can request this information when responding to an emergency, “[i]n circumstances where – (a) a person is a party to a communication; (b) that person, as a result of information received from another party to the communication (in this section referred to as the “sender”), has reasonable grounds to believe that an emergency exists by reason of the fact that the life of another person, whether or not the sender, is being endangered or that he or she is dying or is being or has been seriously injured or that his or her life is likely to be injured or that he or she is likely to die or be seriously injured; and (c) the location of the sender is unknown to that person.”).

159. Id. § 9 (“Any communication may, in the course of its occurrence or transmission, be intercepted in any prison as defined in section 1 of the Correctional Services Act, 1998 (Act No. 111 of 1998), if such interception takes place in the exercise of any power conferred by or under, and in accordance with any regulations made under that Act.”).

160. Id. § 10 (“Any person who is lawfully engaged in duties relating to the – (a) installation or connection of any equipment, facility or device used, or intended to be used, in connection with a telecommunication service; (b) operation or maintenance of a telecommunication system; or (c) installation, connection or maintenance of any interception device used, or intended to be used, for the interception of a communication under an interception direction, may in the ordinary course of the performance of those duties, monitor a signal relating to an indirect communication where it is reasonably necessary for that person to monitor that signal for the purposes of performing those duties effectively.”).


162. Id.

163. 29 U.S.C. § 157 (2012) (“Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection, and shall also have the right to refrain from any or all of such activities except to the extent that such right may be affected by an agreement requiring membership in a labor organization as a condition of employment as authorized in section 158(a)(3) of this title.”).

164. Daugherty, supra note 4 (discussing recent arguments by the NLRB that protected concerted activity includes employee discussions with co-workers about their jobs and working
However, in Daniel Phillip Neethling v. Southern African Fruit Terminals, an employer obtained information in a folder marked “personal” from an employee’s work computer in the absence of an ECP permitting the employer to do so. The Commissioner held that “employees were entitled to use their computers for personal purposes” and that “the evidence . . . obtained from invading the applicant’s privacy must be disregarded.”

C. Dismissal

Posting comments about an employer on a website (Facebook) that can be seen by an uncontrollable number of people is no longer a private matter but a public comment . . . . A Facebook posting, while initially undertaken outside working hours, does not stop once work recommences. It remains on Facebook . . . for anyone with permission to access the site to see . . . . It would be foolish of employees to think they may say as they wish on their Facebook page with total immunity from any consequences.

The use of electronic systems to gain access to social-media sites always leaves a trail or “history.” The same is true when it comes to posts made on social-media platforms. Once it has been posted and read, it’s difficult to ever truly erase. It is important to note that electronic data may be used as evidence during litigation in the U.S. and in South Africa. An employee may be held

---


166. Id. at 10-11.

167. Fitzgerald v. Dianna Smith t/as Escape Hair Design, FWA 7358 (2010) (An Australian court held a dismissal to be unreasonable when a hairdresser was dismissed for posting the following comment on Facebook “Xmas ‘bonus’ along side a job warning, followed by no holiday pay!!! Whoooooo! The Hairdressing Industry rocks man!!! AWSOME!!! [sic].”).


169. Fed. R. Civ. P. 34(a)(1)(A) (“A party may serve on any other party a request . . . to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party’s possession, custody, or control . . . any designated documents or electronically stored information – including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations – stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form.”).

170. ECT § 11 (“(1) Information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message. (2) Information is not without legal force and effect merely on the grounds that it is not contained in the data message purporting to give rise to
liable for defamatory remarks made on social-media sites that infringe upon the good name or reputation of the employer or the workplace.171

In South Africa, the termination of an employment contract (or dismissal) will only be fair and enforceable if it is substantively and procedurally fair,172 as opposed to the principle in the U.S. of “at will-employment.”173 A dismissal will be substantively fair when the reason for the dismissal is related to the incapacity or poor work performance of the employee, the operational requirements of the employer (retrenchment), or the misconduct of the employee.174

The improper or unauthorized use of the workplace’s electronic resources can be seen as insubordination175 and, considering that the misuse of these systems can incur costs to the employer or damage the workplace’s network systems, damage to the employer’s property, both of which fall under the ambit of misconduct.

Schedule 8 of the Labour Relations Act, which contains a Code of Good Practice on Dismissal, states the factors that must be taken into consideration when deciding on whether an employee is guilty of misconduct. These include the employee’s awareness of the rule that was contravened, the reasonableness of this rule, and whether this rule was consistently applied in the workplace.

If an employer instituted a reasonable electronic communications policy (“ECP”) and enforced the policy consistently, any contravention of the policy will constitute misconduct on the part of the employee and would be a substantively fair reason for dismissal.176 The eventual dismissal will then only be (entirely) fair once a proper investigation into the matter, followed by a hearing, is held in order to comply with procedural fairness.177

---

171. See generally CYBERLAW @ SA III, supra note 70, at 252-56.
172. Labour Relations Act 66 of 1995 § 188 (S. Africa) (A dismissal “is unfair if the employer fails to prove – (a) that the reason for the dismissal is a fair reason . . . and (b) that the dismissal was effected in accordance with a fair procedure.”).
174. Labour Relations Act 66 of 1995 § 188 (A fair reason for dismissal is “(i) related to the employee’s conduct or capacity; or (ii) based on the employer’s operational requirements[,]”).
175. As where an employee refuses to obey a reasonable instruction from the employer.
176. Cronje v. Toyota Mfg, 3 BALR 213, 224-25 (CCMA) (2011) (finding dismissal of an employee that distributed a racist cartoon at work to be substantively fair when an employer had a policy that prohibited the distribution of racist material.).
177. See id. at 226 (“In determining whether a dismissal is fair or not, commissioners must have regard to principles laid down by superior courts, and when courts have held that it is fair to
The existence of an ECP is not necessarily the “smoking gun” for cases of alleged employee misconduct. In *Warren Thomas Griffith v. VWSA*, the Commission for Conciliation Mediation and Arbitration (“CCMA”) held that an employee may be dismissed for disobeying a lawful instruction and abusing company facilities (the unauthorized use of internet and e-mail systems). It was the Commissioner’s view that “a person with the employee’s intelligence and experience” should appreciate the fact that intentional disregard of the employer’s instructions would constitute misconduct and that an ordinary person would understand the meaning of “undesirable” and that pornography would fall into this realm.

The law seems clear enough on this issue, if an employee posts defamatory or derogatory comments on any social-media platform that bring the employer or workplace’s good name and reputation into disrepute, whether this is done during or after working hours, the employee can face dismissal. “Not every employee comment regarding their employment or their workplace, using social networks, amounts to an attack and justifies dismissal.” The employer must prove that any damage it has suffered was caused by or was the result of the employee’s electronic communications.

---

178. *Warren Thomas Griffith v. VWSA*, CCMA case no. KN EC 16174, 9-11 (unpublished) (finding dismissal of an employee for abuse of internet and telephone to be substantively fair when the employee previously received warnings to limit his personal calls and avoid accessing undesirable websites).

179. *Id.* at 8-11.

180. See *Sedick & another v. Krisray (Pty) Ltd.*, 20 CCMA 8.7.1 and 8 BALR 879 (CCMA) (2011) (finding dismissal to be substantively fair when employees posted comments on an unrestricted Facebook page that brought management into disrepute and had potential for damage among customers, suppliers, and competitors); *Fredericks v. Jo Barkett Fashions*, JOL 27923 (CCMA) (2011) (finding dismissal to be substantively fair when employee posted derogatory statements on an unrestricted Facebook page about the company and general manager that negatively impacted the image of the company and general manager). See also *Johnson v. City of Marseilles*, No. 06 CV 0955, 2008 WL 94803, *2, 9 (N.D. Ill. Jan. 8, 2008)* (using sexually explicit email communications as evidence to overcome summary judgment on a claim for sexual harassment in the workplace); *SACCAWU obo Haliwell v. Extrabold t/a Holiday Inn Sandton*, 3 BALR 286, 3, 10 (CCMA) (2012) (upholding a dismissal as substantive fair when the employee refused to accept a position transfer, sent a disrespectful email to management, and posted negative comments on Facebook about her manager). But see *Mahoro v. Indube Staffing Solutions*, 20 KVBA 8.18.6, 9-11 (2011) (finding an employee’s dismissal to be substantively unfair when the employer “failed to establish that the Facebook communication by the applicant to an undisclosed recipient had an adverse effect on the business of the respondent and created unharmonious working relationship amongst its employees in the workplace”).


182. See *id.* See also *Fitzgerald v. Dianna Smith t/as Escape Hair Design*, FWA 7358 (2010).
IV. CONCLUSION

“[D]on’t say anything online that you wouldn’t want plastered on a billboard with your face on it.”183 Employers should communicate this basic principle to their employees. The use of electronic communication and social media is increasing and the modern workplace needs to adapt to ensure that the employees adhere to their employers’ lawful instructions as well as their duties, whilst their rights are consistently respected by the employer.

Considering all the legislation and case law discussed and referenced in this article, employers should take the following steps and update their ECP to minimize the risks of social media in and out of the workplace, to possibly use it as a tool, and to ensure continued productiveness:

[1] Restrict access during working hours to only approved websites and other electronic communications systems that are concerned with the activities and business of the workplace. This gives employees a breather and would allow them to access social networking sites during their lunch break as well as before and after working hours.184 “Web filtering software gives administrators the ability to implement time-based access to these and other sites.”185

[2] Educate and train staff on how the use of electronic and social media can cause security issues for the organization.186 Explain that clicking on suspicious links and giving out personal details online can result in malware and viruses entering the workplace’s electronic systems or in identity fraud, which could damage their own or their employer’s reputation. In this regard, inform employees that any conduct that can disgrace their employer’s reputation can result in their dismissal.188

183. Wortham, supra note 12 (quoting Erin Bury, the community manager of Sprouter, a social media site for entrepreneurs (http://sprouter.com/)).
184. Kelleher, supra note 2 (recommending that employers use web filtering software to implement time-based restrictions on their employees access to social networking sites during working hours while allowing “access to social networking sites during their lunch break, before and after office hours”).
185. Id.
186. Id. (“Most employees are not aware how their actions online can cause security issues for the organization.”).
187. Id. (“Tell them in a language they understand how a simple click on a link they receive or an application they download can result in malware infecting their machine and the network. Additionally, tell them not to click on suspicious links and to pay attention when giving out personal details online. Just because employees are clever enough to have an online profile does not mean they are technically savvy or that they have a high level of security awareness.”).
188. See id. (“Have all employees sign any policies related to the use of the Internet at work, access to social networking sites and what they are allowed to say or do during office hours. Monitoring of all Web activity is important, and employees should be aware that their actions are being recorded and that failure to adhere to company policy can result in disciplinary action and/or dismissal.”).
[3] Convey that any information or comments posted online with some bearing to the business, the workplace, the employer, or another employee should be accurate, non-confidential and not harmful to the continued employment relationship. Remind employees to pay attention to the terms and conditions of social media platforms and related websites.

[4] Emphasize the confidentiality obligations of employees. Remind them of the non-disclosure and confidentiality clauses (that should be) in their employment contracts. This includes non-disclosure of the personal information of co-workers. Require employer-approval for any statement made to the media (or via electronic media).

[5] “Set security and usage policies. Have all employees sign any policies related to the use of the Internet at work, access to social networking sites and what they are allowed to say or do during office hours.”189 Allow personal use of the employer’s electronic systems, but remind employees that personal messages will be treated similar to work messages and management will have access to such personal messages without regard to consent. Employees should thus refrain from using the electronic communication systems to transmit information that they would not want to be accessed by a third party.

[6] Monitor online activity.190 “[E]mployees should be aware that their actions are being recorded and that failure to adhere to company policy can result in disciplinary action and/or dismissal.”191 Employees should also be made aware of the fact that the employer will have the right of access to certain information.192 Although employees may be given a password to access the workplace’s system, employees should be aware that this system belongs to the employer and the content of e-mail communications will be accessible to management for any business purpose.193

By implementing these steps and introducing a comprehensive ECP in the workplace, an employer can satisfy its needs without having employees feel that their rights are being infringed. This should also reduce employees’ desire to defame their employer or co-workers online.

189. Kelleher, supra note 2.
190. Id. (“Monitoring of all Web activity is important.”).
191. Id.
192. Thompson, supra note 19, at 288 (“Inform employees that the company not only has the right to, but will, inspect, monitor, and review employee use of employer provided or paid for technology, including but not limited to e-mail, Internet, and cell phone records – including text messages (if paid for by the employer).”)
193. Id. at 287-88 (“An Electronic Use policy also served to place employees on notice that their use of technology has no expectation of privacy.”).
EMPLOYER SURVEILLANCE VERSUS EMPLOYEE PRIVACY: THE NEW REALITY OF SOCIAL MEDIA AND WORKPLACE PRIVACY

Saby Ghoshray*

Privacy is dead, and social media holds the smoking gun.1

I. INTRODUCTION

Scenario 1: The morning after Super Bowl Sunday 2013, Lee is hung over. Yet, he has an important client filing to complete. His boss needs him desperately, but, his mind is foggy from the excessive drinking the day before. Lee picks up the telephone and calls in sick. This greatly upsets his boss. Although his boss knows Lee is a compulsive social media user, he did not think anything suspicious, until he stumbled onto a late afternoon tweet from Lee. “Just waking up, heading for the beach. What a game last night!” The infuriated boss walked downstairs to chat with the Human Resource (“HR”) department. While Lee is out enjoying the beach, the HR manager contemplates her next step – whether to initiate an action to discharge, discipline, or penalize Lee.

Scenario 2: Melissa is a front line analyst at an investment bank, working on a sophisticated trading model that has huge upside for the company. Although her manager sees potential in her, of late, she finds her distracted and making uncharacteristic mistakes. The supervisor also knows that she is an avid social media user with many followers. She also knows Melissa does not like to disappoint her followers, who salivate for her regular updates. The manager stumbles onto Melissa’s recent update, which was open to the public as she had no privacy setting. He was shocked to read a long posting hinting at the

* Dr. Ghoshray’s scholarship focuses on subsets of International Law, Constitutional Law, Cyberspace Law, Technology and Fourth Amendment, among others. His work has appeared in a number of publications including, Albany Law Review, ILSA Journal of International and Comparative Law, European Law Journal ERA-Forum, Toledo Law Review, Georgetown International Environmental Law Review, Temple Political & Civil Rights Law Review, Fordham International Law Journal, Santa Clara Law Review, Michigan State International Law Journal, Loyola Law Journal and Washburn Law Journal, among others. The author would like to thank Jennifer Schulke for her assistance in legal research and typing of the manuscript. Much love to his beautiful children, Shreyoshi and Sayantan, for their patience and understanding. I offer appreciation to the members of the Northern Kentucky Law Review Editorial Board for their diligence in the editorial process. Dr. Ghoshray can be reached at sabyghoshray@sbcglobal.net.

proprietary methodologies she is working on. Flustered and alarmed, the manager walks into the office of his own supervisor. Is Melissa giving away trade secrets unknowingly? Immediately, the supervisor is on an intense conference call with the HR representative. Should Melissa be disciplined or let go for her social media update?

**Scenario 3:** Shawn is a middle level executive at a Big Four firm. Shawn is an excellent employee, and a devoted father of three. He uses social media very sparingly. He does not have a fan following, but, he frequently exchanges messages with his wife while at work. Shawn has no privacy setting. His wife is an avid Facebook user and she uses a privacy setting. Only individuals within her designated community can view her communications. Shawn’s supervisor finds his productivity slipping. As she engages in an online search, she discovers the family problems he is having through the posted exchanges with his wife on nights he stayed late in the office. Based on personal information gained through the online search, the supervisor made negative recommendations on his upcoming promotion. Can the supervisor influence Shawn’s promotion because of his social media communications?

The scenarios presented above are hypothetical. But, they are symptomatic of an emerging reality unfolding in America’s workplace as employers are ramping up surveillance of their employees. Thus, these hypothetical snapshots act as important vignettes through which to see and examine how our social media behavior may be slowly eroding our expectation of privacy. This article is an exploration towards uncovering that new reality, and using the employee-employer bilateral relationship as a contextual lens to process such reality.

Manifested in the hypothetical scenarios above is the reality of a digitally immersed contemporary society, where an overwhelming number of individuals live their lives connected and mediated via social media at all times. In living their lives inside the electronic confines of social media, these individuals leave their digital footprints in cyberspace. Digital footprints convey meaningful information about an individual. Employers have become increasingly interested in accessing such footprints of its employees. As this search has become a new functionality in the evolving employee-employer relationship, both sides continue to grapple with its adverse consequences. Prompted by surveillance results, as employers make decisions on their employees’ future, today’s labor market has awoken to a slew of legal uncertainties.

For every one of the hypothetical scenarios above, an abundance of real life scenarios are unfolding at the corporate conference rooms. As employment disputes have begun to trickle through courtrooms and administrative tribunals, the judges and administrators are waking up to this new reality. In this reality, both the paucity of settled law and the scarcity of precedence make evaluation of
legal implications of social media relationships very difficult. Yet, these
decision-makers have been placed into an unenviable role of making decisions
about people’s lives and livelihoods based on the interplay of law and social
media.

Let us consider one of the inaugural social media based employment
termination cases recently reviewed by the National Labor Relations Board
(“NLRB”). The NLRB was thrust into this first of a kind - Facebook meets
labor law case, after having made its way through appeal from an administrative
law judge (“ALJ”) decision. The employee, a former BMW salesman, had
taken pictures of an event sponsored by his employer, a dealership. The
employee had posted sarcastic comments and photos related to the event on his
Facebook page. As more people viewed his posts, his supervisor learned the
contents of his page, resulting in the salesman’s termination from the
dealership. On appeal, the ALJ ruled in favor of the dealership. In justifying
the ruling, the ALJ found posting photos and comments at the employee’s sole
discretion and without any consultation from workplace to be an employment
violation. Arguing the employee’s Facebook posting to be an unprotected form
of expression, the ALJ refused to review the legality of the content itself. The
NLRB agreed with the ALJ’s determination.

The NLRB decision upholding an employee’s termination from employment
represents an individual outcome of contemporary society’s immersion in social
media. It further highlights how social media behaviors may have tangible

2. See Facebook Post Gets Worker Fired, ESPN.COM (Mar. 9, 2009, 5:41 PM),
http://sports.espn.go.com/nfl/news/story?id=3965039 (“A Facebook post criticizing his employer,
the Philadelphia Eagles, cost a stadium operations worker his job . . . According to the newspaper,
Leone posted the following on his Facebook page: ‘Dan is [expletive] devastated about Dawkins
signing with Denver . . . Dam Eagles R Retarted [sic]!!!’”); see also David Kravets, AP Reporter
Reprimanded for Facebook Posts; Union Protests, WIRED.COM (June 9, 2009, 4:40 PM),
http://www.wired.com/threatlevel/2009/06/facebooksword; see generally Raffi Varoujian, Legal
Issues Arising from the Use of Social Media in the Workplace, HELIUM.COM (July 28, 2011),
workplace (discussing current tensions which exist between the law and the capabilities of the
Internet that have yet to be fully addressed by the law) (last updated June 21, 2012).

3. The National Labor Relations Board (NLRB) is an independent federal agency. Its duties
include the oversight and protection of employee’s rights, as well as suggesting the need for union
representatives for employees. See the NLRB’s page, http://www.nlrb.gov/nlrb-process, for an
overview of the NLRB process and organizational setup.

28, 2012).

5. Id. at 170.
6. Id.
7. Id. at 171 (noting he was terminated on June 22, 2012).
8. Id. at 174.
9. Id.
11. Id. at 164.
adverse impacts on lives. As the cases of employer surveillance of their employees trickle through the court system, complex legal issues are surfacing. In particular, the intersecting rights of employee and employer and their evolving relationships continue to invite attention. How these relationships might shape the constitutional contours of either First Amendment speech right or the Fourth Amendment privacy right is of grave uncertainty. This prompts a series of questions that require deterministic paradigms.

How might an employee’s First Amendment right be impacted by an unprovoked surveillance? Should an employer prohibit all employees from social media activities at work? Must an employer train its employees in acceptable workplace social media etiquette? Does an employee leave her free speech right through social media at the corporate door? Can an employee expect a reasonable level of privacy from employer’s surveillance in her social media communication? Most of these questions relate to how employee’s individual rights get impacted on account of leaving her digital footprints in cyberspace. The queries, indeed get further complicated in the following scenario.

Let us examine the case of Janis Roberts, a former Texas helicopter paramedic working for CareFlite. Ms. Roberts felt frustrated with the attitude of a patient she assisted. Upon completion of her emergency call, the flight paramedic vented her feelings by posting a comment on her co-worker’s Facebook page complaining about a certain unruly patient. She did not stop at just a mere complaint. Her Facebook exuberance continued on as she expressed the desire to slap that patient. Janis Roberts’ protracted Facebook exchange with her fellow flight paramedic soon found the roving eye of their supervisor. As a result, she was terminated for being unprofessional and insubordinate. The ensuing appeal against the employer’s decision soon made its way to the Second District Court of Appeals, who upheld the Tarrant County judge’s decision observing that the terminated employee’s Facebook rant is “not within the zone of her seclusion, solitude and private affairs.” By providing an example of how an individual’s social media exchange can influence employer surveillance, this case highlights potential legal consequences of contemporary society’s deep social media immersion. Moreover, this case serves as a harbinger of many future cases to show how individual social media behavior

---

13. Id. at *1.
14. Id.
15. Id.
16. Id. at *2.
17. Id. at *5.
can cut across multiple legal dimensions of employer surveillance, wrongful termination, and invasion of privacy.

On the surface, privacy in the social media era seems to be heading towards annihilation. In reality, it has metamorphosed into a complex phenomenon, as the scope and legal protection of privacy has been evolving with society’s behavioral norms and changing expectations. For example, workplace frustration is a common occurrence and venting this frustration is a typical human response. However, as facts of the above case reveal, the two co-workers held a differing view of the act. The terminated employee, Janis Roberts felt she was within her privacy right to a secluded conversation in posting derogatory comments about her workplace condition. The employee with whom Ms. Roberts exchanged Facebook messages felt such communication may be outside the purview of private conversation. Yet, based on the actual outcome, it may appear that the employee does not have any privacy right. After all, she was simply exhaling her frustration on Facebook like so many others do, only to find her employment terminated. Perhaps a comparison of how an analogous scenario might have unfolded a couple of decades back will shed some interpretive gloss on this phenomenon. Imagine a similarly frustrated employee in an earlier decade. She would have either called a co-worker to vent or shared her frustration in a face-to-face conversation during a break. This would have invited neither a supervisor’s review nor termination. These period-specific dichotomous outcomes of analogous events are indicative of how technology enabled social media behavior may be shaping individual’s expectation of privacy in the workplace, as evaluated in the observations below.

First, society’s pervasive digital immersion is manifested in individual’s enhanced ability in contemporaneous and instant information exchange with multiple other individuals. As a result, a single one-to-one information exchange mediated through social media can instantly become a many-to-many communication. Such information, by virtue of its underlying digital exchange mechanism, can now be stored for future review and decision making based on the content. On the contrary, the telephone era’s analogous private exchanges between co-workers traveling through physical communication lines would not be so conducive to instant storage and surveillance. Thus, such communication mechanisms would be difficult to rely on for monitoring employee behavior, unless the targeted employee’s telephone was wiretapped upon finding probable cause.

Second, ease of instant communication and access to its stored content within social media may provide stronger rationale for surveillance. Thus, the

19. Id. at *2.
contemporary individual may be sacrificing an essential liberty component, individual privacy, on account of widespread digital immersion in the social media. Admittedly, having a digital footprint adversely impacts an employee’s right to privacy in personal communication. But, this article examines whether the broader scope of employer intrusion into an individual’s private affairs at work is necessarily consistent with the Fourth Amendment.

Employer surveillance of an employee’s zone of private seclusion to uncover personal details is a disturbing trend. Recognizing this emerging phenomenon, this article sets out to examine whether über-surveillance of an employee may indeed be an outgrowth of the employee’s digital immersion. Thus, the article ponders whether the seduction of social media may have become a driver in eroding individual’s privacy on the pretext of protecting her employer’s legitimate business interest. Furthermore, a paucity of legislative guidelines might have underscored the growing disconnect between digital immersion and law’s inability to track such immersion. In this context, distillation from various court proceedings reveals the two occasions when the search for employee digital footprints is conducted: (i) during the cyber-vetting of an employee prior to employment, and (ii) during the actual employment. This article examines the second thread in detail while responding to a growing need for providing guidance in law.

The article proceeds with Part II examining the current landscape of digital immersion in contemporary society. This examination will reveal the background that facilitated the emergence of this newer social media exuberance. Although the linkages between social media exuberance and employer surveillance has not been established as a matter of law, their relationship would be informative to analyze. Part II also analyzes the reasons and examines the societal factors that have given rise to the legal evolution in this direction.

Part III examines how the current Fourth Amendment jurisprudence can be applicable in identifying how individual behaviors may be framed within the confines of settled jurisprudence. The article arrives at this conclusion by analyzing the aspiratory dimensions of an older case and finds analogues

20. See, e.g., Eli R. Shindelman, Note, Time for the Court to Become “Intimate” with Surveillance Technology, 52 B.C. L. Rev. 1909, 1914 (2011) (noting the struggle courts have to protect privacy in the age of technology); see, e.g., Lyria Bennett Moses, Recurring Dilemmas: The Law’s Race to Keep Up with Technological Change, 2007 U. ILL. J.L. TECH. AND POL’Y 239, 241 (2007) (noting that the law has fallen behind technology); see generally Raffi Varoujian, supra note 2 (discussing current tensions which exist between the law and the capabilities of the Internet that have yet to be fully addressed by the law).

behavior in the post-modern era. This analysis will develop a better understanding of the current penchant for employer’s über-surveillance.

Part IV examines individual behavior in social media, which may have a definite link in abrogating individual’s subjective expectation of privacy. By developing a set of fundamentals, Part IV drives home the point that the contemporary society’s digital immersion is a fundamental yearning for symmetry, which may in turn work against individual’s search for privacy at workplace. Finally, Part V concludes that the Fourth Amendment jurisprudence may still be robust enough to address complexities arising out of social media behavior and its implications in employee-employer bilateral relationship.

II. THE LANDSCAPE OF EMPLOYER – EMPLOYEE RELATIONSHIP

Social media has induced a new behavioral paradigm amongst individuals that has prompted an evolving pattern in employer-employee relationships. Two decades back, it would be rather unconscionable to contemplate an employer continuously monitoring an employee conversation. On the contrary, a continuous surveillance of an employee’s digital key strokes may be the new norm. This is because a search of an individual’s digital footprint in cyberspace would reveal multiple behavioral signatures that might assist an employer in making decisions about the employee’s continued viability within the organization. Although a very sensitive area, this phenomenon has implications for both the employer’s rights and the employee’s rights, because an employer’s surveillance of its employees opens up to uncharted legal trajectories with limited precedence. In this new social landscape, by generating numerous behavioral signatures, an employer may discipline, penalize, and terminate an employee – each of these outcomes could result in legal implications along a multitude of dimensions. This article focuses on the landscape created within the employer-employee relationship once the employee accepts a position. This event could trigger a diversity of signatures, each of which would require fact-specific legal analysis. I will address a few of these in this context.

22. See generally Matthew E. Swaya and Stacey R. Eisenstein, Emerging Technology in the Workplace, 21 LAB. L. 1, 9 (2005) (discussing how the rapid advancement in surveillance technology has allowed a proliferation of various keystroke logging devices that can track and store employee activities on the internet).


New technology has enabled behaviors which the law is not yet prepared to address. Legislative enactment to address gaps in the law must address deterministic complexities. Therefore, the legality of employer surveillance in a search of an employee’s digital footprint must depend on the scope and contour of the search. For example, legitimacy of surveillance may depend on how the employer conducted the search. As a matter of law, for a surveillance to be legitimate, its scope must be determined based on employee’s protection threshold. An employee’s protection threshold is much lower in instances where such surveillance is undertaken on an employer-issued computer than in instances where a search for an employee’s social media footprints is conducted during off hours on a private personal computer. Certainly, digital footprints created in an employee’s personal machine must have a higher threshold of Fourth Amendment privacy protection. This very same Fourth Amendment protection, however, can be turned on its head in favor of an employer, if the employer searches for an employee’s digital footprints created on an employer-issued computer during work hours.

The above scenario is somewhat akin to the shared rights developed between a tenant and a landlord within a lease framework. While the tenant has the right to be left alone, the landlord retains the right to a periodic inspection and can penalize the tenant based on observed violation(s). Similarly, an employer may not engage in continued surveillance of an employee’s every key stroke, but can review contents of his or her accessed websites based on a probable cause of a violation. Thus, in matters related to employer-issued machines, an employer has a much lower threshold to trigger surveillance of an employee’s social-media adventures.

The ownership of the conduit, such as a personal computer or a smartphone on which employees create their digital footprints, may be an element for

25. Id.
26. James D. Phillips and Katharine E. Kohm, Current and Emerging Transportation Technology: Final Nails in the Coffin of the Dying Right to Privacy, 18 RICH. J.L. & TECH. 1, 10 (2011) (arguing that advances in technology have led to Supreme Court decisions that have created confusion in Fourth Amendment privacy law). Technology-enabled communication has moved beyond the point-to-point communication of yesteryear to a combination of distributed transmission and third-party-enabled communication, where various third-party providers are not only storing data but also processing it to make the system more efficient as well as to enhance the experience of users. See Connie Davis Powell, “You Already Have Zero Privacy. Get Over It!”, Would Warren and Brandeis Argue for Privacy for Social Networking?, 31 PACE L. REV. 146, 146 n.2 (2011) (noting details on various third-party mechanisms in communication, social media, and Internet); see also 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, 371 (2011) (describing how a Facebook account stores private content in which a user manifests an expectation of privacy, as opposed to “envelope” information).
27. Id.
28. Id.
delineating and structuring the shared rights of privacy and surveillance. Thus, delineating rights and identifying factors influencing such delineation would shape acceptable behavior for both parties in the context of social media exchanges at the workplace.

A. Issues That Impact an Employer

The hypothetical scenarios and the judicial determinations discussed earlier present an interesting, yet, converging snapshot of how various employer interests could be at stake on account of employee behavior in social media. Recognizing this new technology-enabled distraction of an employee, a set of acceptable employee norms could be prescribed in the employee handbook. In developing such a handbook, an employer can take into account its own objectives – such as, legitimate business interests, compliance obligations, and insulation from liabilities against employees. This would also provide a reference for an employer to fall back on in times of dispute. This will, therefore, allow for the law’s contour to evolve in a deterministic way to adequately balance employer surveillance with employee conduct that warrants such surveillance.

1. Employer’s Legitimate Business Interests

Employee productivity is recognized as one of the central drivers for a business’ continued viability. It might thus be argued, that this drive for remaining viable gives an employer a legitimate right to extract productivity from its employees. Therefore, in an environment where an individual is continuously wired, it may become vitally important to monitor employees. Anecdotal evidence gleaned from pertinent literature survey is replete with the growing trend of employees sacrificing workplace productivity due to the drive

---

29. See Varoujian, supra note 2.
30. Id.
31. Here I draw attention to the employers’ genuine concern for its employees’ loss of productivity on account of engaging in non-work related activities during work. In this sense, an employer can assert enhancement of productivity of its employees as a legitimate business interest, especially in the current social landscape, where employees are prone unbridled digital excursion on employer time. While employee digital immersion has been causing employer concern ever since internet and email use has become widespread, such concern has become heightened as the rampant use of social media at workplace has added another new layer of employer concern
32. See Kendra Rosenberg, Location Surveillance by GPS: Balancing an Employer’s Business Interest with Employee Privacy, 6 WASH. J. L. TECH. & ARTS 143, 152 (2010).
33. Id.
to constantly communicate via social media, where constant status updating is not only the norm, but almost required.

Thus, this growing necessity of having some employee surveillance in effect would require us to determine the scope of such surveillance and to consider how much employee privacy could be allowed in their online activities in the workplace. Should surveillance be a legitimate part of doing business? Should such surveillance be conducted as an ad hoc reactive response to sagging productivity? The following section illuminates these concerns.

2. Ensuring Compliance

In an era of instant messaging and continuous status updating, a typical employee is in constant communication mode. In the frenzy of frequent status updates, often the employee is not paying careful attention to the delineation amongst time, place, and context. In such evolving paradigm of pervasive digital immersion, the line between home and office gets blurred. As the digital environment and its non-digital counterpart fall within a continuous unregulated space, a typical employee forgets the limits of social media exchange, triggering unrestrained communication during work hours while utilizing employer’s machine. Yet, such violations of compliance related to social media communication may not be easily apparent to a supervisor, as it may only be identified either through tracking or through third-party reporting. Thus, the way an employer may become privy to a compliance violation is through surveillance of employees. The pertinent question is therefore, for how long should an employee be put under surveillance? Although surveillance may be the only way to ensure compliance, must there be scope limitation as to the scope and duration

---


36. Harmon.ie Press Release, supra note 35 (“Two out of three users will interrupt a group meeting to communicate with someone else digitally, either by answering email (48%), answering a mobile phone (35%), chatting via IM (28%), updating their status on a social network (12%) or tweeting (9%).”).

37. Id.


of such surveillance? Despite the positive outcomes an employer may derive, unbridled surveillance without probable cause must still be recognized as a violation of fundamental privacy. Therefore, the scope of surveillance should be predicated on a trigger based on an employee violation. Clearly, establishing when to initiate such surveillance is still up for debate.

3. Employer Liability in Implicating Others

An employer’s legal liability from its employee’s social media exchanges can emerge through various pathways. Commentators have already noted how an employer could be subject to liability on theories of tort, contract, or copyright violations because of employee social-media exchanges. The content of such exchanges could range from dissemination of an employer’s trade secret to derogatory exchanges addressed towards a co-worker. A set of scenarios can illuminate the potential danger lurking for an unsuspecting employer.

First, if conducted during work hours, or communicated from an employer-owned machine, the employer could be liable for causing injury to an employee or an affected person. Second, unless careful, an employee could inadvertently share trade secrets with the general public while updating a Facebook status. If such inadvertent sharing takes place with members of a rival firm, it may cause irreparable economic harm to the employee’s business on account of revenue loss or sudden drop in market share.

Second, an employee could engage in social media outbursts to give vent to momentary frustration at work. Other possible scenarios may include, exchanges deliberately targeted towards other employee, exchanges that might be deemed derogatory or determined to be in violation of business regulations. In all such instances, the employer could face liability as a matter of law.

41. Id.
42. Id.
43. See Michelle Sherman and Robert S. Gerber, Protecting Trade Secrets in the New Social Media World, A.B.A., available at http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2012_hot_topics_in_ip_lit/2012aba_panel2_protecting_trade_secrets_in_the_new_social_media_world.authcheckdam.pdf (discussing aspects of social media and the creation of accounts, profiles and associations during the time of employment. The author ponders on who owns those created profiles, “the plaintiff former employer, or the defendant former employee?”) (last visited July 10, 2013). From precedent rulings, it would seem the employers are faring better in litigation but it is a costly affair.
44. Kravets, supra note 2.
45. GLYNN, supra note 23, at 273-319.
These anecdotes exemplify how apparently innocuous Facebook update could mushroom into a potential nightmare for the employer.

Finally, despite presenting a stronger rationale for allowing employer surveillance, highlighted incidents above do not shed revelatory light on the more probing issues of how long, how often, and when the employer should conduct its surveillance. A full explication of such query will necessitate a decoupling from the context of surveillance to the more fundamental issue of individual privacy. This requires engaging in a discussion of individual employee’s expectations of privacy – privacy that is recognized within the broader society’s reasonable expectation.

B. Issues That Impact an Employee

Contemporary employees are products of society - a society where smartphones, Facebook, and Twitter each represent dimensions through which such post-modern employees communicate, exhibit emotions, and form communities. In this concept of living connected, continuously uploaded, and streamed online, the fulfillment of all the promises of life for an individual also means displaying private snapshots to their self-selected digital community. Although life’s journey may require recognizing privacy as an essential element to fulfill life’s promises, post-modern individual’s constant-digital immersion may have brought an attendant cost of living – an unexpected abrogation of privacy.

Privacy is a fundamental liberty component and an essential element to the life of a free man. Yet, post-modernity’s digital immersion recognizes the contour of an individual’s privacy through the prism of an individual’s behavioral norm. In other words, how far an individual’s privacy contour will be allowed to evolve would depend on what behavioral norm such individual exhibits in a relevant and an analogous context. Thus, while we may lament the

47. Id. (describing the multitude of ways Americans use technology in their everyday lives).
48. See Julia Angwin, How Much Should People Worry About the Loss of Online Privacy?, WALL ST. J. (Nov. 15, 2011, 3:56 PM), http://online.wsj.com/article/SB10001424052970204190704577024262567105738.html (panel discussion regarding the impact the Internet has had on daily life and why protecting the privacy of that activity is important).
49. Id. (“Our founding fathers experienced life without privacy protections under the British, when writs of assistance permitted searches of homes at the whim of customs agents. Life without privacy laws was hell under the British, and it would be even worse now, given the powerful surveillance technologies that governments around the world now possess.”).
individual privacy space shrinkage at an alarming rate, we cannot decouple ourselves from the root of such an abrogation—the role of an emerging communication paradigm.

As communication has changed from telephone conversation to exchanging computer messages, the frequency, content, and the reach of communication has truly metamorphosed. Individuals are able to communicate with more people, with the enhanced capability to communicate simultaneously and more frequently. The ultra-connected nature of today’s communication has created a scenario where employee surveillance can go beyond the relevant employer-employee relationship, as technologically enhanced communication has opened up the possibility of employer surveillance impacting the privacy of more individuals. A few significant observations are noteworthy to consider here.

With technology’s capability to expand in various dimensions, the ambit of employer surveillance has expanded. Although employer surveillance is


53. See generally Cashmore, supra note 1. Other authors contends that, “The large amount of time spent at the organization during the workweek may also mandate that personal business be brought to and engage/resolved at work during normal business hours. Examples could include banking, medical appointments, child related issues, etc. Thus, privacy would be of large importance as having personal items on your work computer would/could offer information that the public usually is not privilege too.” Sherri Coultrup and Patrick D. Foutain, Effects of Electronic Monitoring and Surveillance on the Psychological Contract of Employees: An Exploratory Study, 19 J. BUS. & BEHAV. SCI. 219 (2012), available at http://asbbs.org/files/ASBBS2012V1/PDF/C/CoultrupS.pdf.

54. The contemporary social media technologies are replacing the former telephone and the facsimile machine as modes of communication between co-workers, business colleagues or even friends. Instead, the communication is done via text updates, chat message, or blog posting, which allows a single post or updates to connect with mass amounts of ‘friends’ or casual browsers of that publicly open posting. See generally Gini Dietrich, Social Media to Replace Traditional Media Says CEO Study, SPINSUCKS (May 23, 2012), http://spinsucks.com/entrepreneur/social-media-to-replace-traditional-media-says-ceo-study/; see also Six degrees of mobilization Technology and society: To what extent can social networking make it easier to find people and solve real-world problems?, ECONOMIST TECH. QUARTERLY, Sept. 1, 2012, available at http://www.economist.com/node/21560977.

55. Swaya & Eisenstein, supra note 22, at 9.
indexed at the bilateral employee-employer dimension, society’s digital immersion forces a secondary effect. As the targeted employee is connected with many members within her digital community, such surveillance impacts others within the broader scope of a one-to-many relationship. Thus, apparently simple bilateral employee-employed surveillance may mushroom into a multi-lateral surveillance, affecting the privacy of individuals beyond the employee in question.

Clearly, generic employee surveillance has a shaping effect on the privacy right of individuals that are not employees. These individuals have neither consented to such surveillance, nor agreed to bare intimate details of their lives to the prying eyes. Mass acclimatization of social media and society’s pervasive digital immersion has opened up totally uncharted areas of privacy violations, where a contractually bound bilateral relationship – that between an employer and employee – may open up a Pandora’s Box of social uncertainty and legal indeterminacy.

Despite the existence of an emerging trend, this discussion does not address the issue of an employer demanding personal information from their prospective employees. Driven by a desire to identify and evaluate the digital persona of its prospective employees, employers routinely subject job applicants to furnish their personal account information, including passwords to view their social media activities. This area is currently gaining a sustained focus of inquiry, driven in part due to growing litigation, and in part owing to pending legislative efforts at both the state and federal level. Recognizing that some of these intrusions may be unreasonable and unacceptable invasions of privacy, law-makers are contemplating new statutory protections. However, given the complexities and nuances involved within this interaction between law and technology, uniformity in state-wide legislative enactments could take time. Therefore, while the landscape of statutory protections is yet to mature and get harmonized across the country, the path to prudent employer behavior can still be envisioned within the enduring principles enshrined in the existing Fourth Amendment protections.

57. Id.
59. Khaki, supra note 58.
60. Id.
III. FOURTH AMENDMENT PROTECTION AGAINST UNREASONABLE SURVEILLANCE

Post-modern individuals’ digital immersion forces them to leave digital footprints at almost every waking moment, virtually through every exchange within the society. Residing within these digital footprints is personal, private information related to the individual. Therefore, a search for those footprints will invariably intrude upon an individual’s personal confines. Yet, society’s behavioral norm has been structured in such a way that an individual cannot escape from digital immersion. As a result, technology enhanced surveillance enables access to those individual’s digital footprints.

Although such erosion of individual privacy conflicts with liberty interests, the scenario is somewhat different within the context of employee-employer relationships. Technological advancement has allowed rapid enhancement in the functional aspects of information acquisition, sensor capacity, data streaming and data storage and retrieval in the digital environment. Mediated through the use of HDTV, smartphones, the internet and other devices, technology has allowed pervasive use and acclimatization of digital communication, empowering individuals to disseminate an unedited and non-discriminatory collection of personal information in the cyberspace. This allows entities outside of the original intended recipient to access and investigate an abundance of personal information by following the digital trails of a person’s online exchanges, enabling various entities to reconstruct a new locus of online identity. By digital footprint, I refer to this locus of online identity an individual leaves behind in cyberspace created through that individual’s online interactions that ranges from shopping, email communication, cyberspace chat, social media interaction, sharing YouTube videos, etc. See Kieron O’Hara, et al., *Lifelogging: Privacy And Empowerment With Memories For Life*, 1 IDENTITY INFO. SOC’Y 156, 159 (2009), available at http://eprints.soton.ac.uk/267123/ (observing the various modes and modicums of individual exchanges in cyberspace enabling the development of emerging culture of online social presence where individual sheds personal privacy in documenting their lives in front of strangers).

62. Here I draw attention to the emerging social dynamics, where creating online social media profile to keep in touch, communicate, and search for lost friends, relatives, and acquaintances has become the social norm. Often times, individuals prefer to communicate by posting messages on social media sites that can be shared with and viewed by more than one recipient, as opposed to traditional two-way communication. In this new way of social media communication, a two-way conversation, often times, become a conversation with multiple forum with an initial two-way communication becoming a many-to-many discussion. In this emerging social landscape, individuals are encouraged to become active in social media in order to have meaningful conversations within a community forum. Often times, individuals are encouraged to assimilate in this all-pervasive social media immersion by interjecting an element of fear in the minds of those lagging behind in adoption of such media. See Danah Boyd, *Whether the Digital Era Improves Society is Up to Its Users – That’s Us*, GUARDIAN (Apr. 21, 2012, 5:00 EDT), http://www.guardian.co.uk/commentisfree/2012/apr/21/digital-era-society-social-media (noting how the existing attention economy introduces the culture of fear in adopting newer social practices, one of them being immersion in social media usage).

63. The sanctity of privacy as a fundamental right has illuminated the U.S. Constitution for more than century. The core privacy fundamental emerged from a much deeper right-to-life interpretation with its roots embedded in the conception of liberty. Therefore, individual privacy is recognized as an essential component of liberty. See generally Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193-95 (1890) (discussing the need for
relationship. Here, the surveillance right of an employer would be better determined against a framework of an individual’s subjective expectation of privacy. Commenting on linkages between an individual’s expectations of privacy in contemporary society with such individual’s digital immersion, the Supreme Court noted:

Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . . Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy.

The Court’s pithy observation above animates its view on the individual’s subjective expectation of privacy. While unclear what direction the Court

privacy as technology developed in 1890). Long before the technological onslaught of the post-modern era, Justice Warren and Justice Brandeis invoked a deeper fundamental right to privacy that has since been muted somewhat under the attack of states’ heightened interests. See id. at 193.

64. I had argued elsewhere that, premised on an exigency of situation framework, privacy as a liberty interest has been muted under superior state interests. This has resulted in significant abrogation of individual privacy in furtherance of state’s law enforcement related objectives. See Saby Ghoshray, Privacy Distortion Rationale for Reinterpretation of the Third-Party Doctrine of the Fourth Amendment, 13 FLA. COASTAL L.J. 33, 81(2012) [hereinafter Ghoshray, Privacy Distortion Rationale]. A rapidly shrinking privacy paradigm is inconsistent with Warren and Brandeis’ privacy concept discussed earlier, in that, their privacy calls for recognizing the sacrosanct realms “of private and domestic life.” See Warren and Brandeis, supra note 63, at 195. This broader connotation of the right to be left alone must be understood against an increasing threat to privacy in contemporary society, as privacy must be recognized for an individual’s inherent right of privacy within the confines that an individual creates. Extrapolating this right to privacy would imply that these sacrosanct fundamentals would equally extend to the interior of the home-like community of connected individuals—be it within the Twitter community, the Facebook community, the MySpace community, or any other online community. Just because technology has allowed the quantity and frequency of information to skyrocket does not necessarily preclude individuals from exercising their right to be left alone. See Chip Walter, A Little Privacy, Please, SCI. AM. (June 17, 2007), http://www.scientificamerican.com/article.cfm?id=a-little-privacy-please.


66. See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). While referring to Justice Harlan’s famous test in Katz, Peter Winn observed that:

[In] Justice Harlan’s concurrence on its merits, we have seen that in working on the reasonable expectation of privacy test, he refined the test in his own way, adding both a subjective and an objective component. Perhaps he thought that the subjective component was needed to clarify that, although an objective expectation of privacy might exist, a subjective expectation might not, as when a person in his (objectively private) home is overheard intentionally speaking in a loud voice out of on open window. . . . Perhaps Justice Harlan felt the subjective component of the test was still needed to mirror the old trespass element that an intrusion lack permission. However, when applying the test in
itself must follow, it may be hinting at a trajectory based on two underlying principles. The first formulates the scope and the contour of individual’s expectations of privacy by indexing it at what the Court views as the broader society’s expectation of an acceptable behavior framework. In the second, the Court further modulates individual’s privacy expectation based on finding a necessary ingredient within a broader spectrum of individual self-expression. Although far removed from a discussion of the employee-employer bilateral relationship, the Court’s observation here is prudential. The Court views individual’s digital immersion and resulting communicating modes as part of a set of fundamental needs for the individual’s ability to express himself or herself, an area I have discussed in detail elsewhere. Although the Court’s observation above might tilt the balance in favor of restriction in employer surveillance to protect individual privacy from erosion, the full impact of the Court’s dicta may become attenuated when measured in light of employer’s legitimate business concern.

Subsequent cases, even Harlan himself only referenced the objective component.


67. Taking a renewed look at the fundamentals of the privacy interests under the *Katz* holding, an individual’s subjective expectation of privacy must be evaluated at the next level of abstraction that requires evaluating the scope qualitatively and quantitatively. The means of evaluation is dependent on identifying society’s reasonable expectation of privacy—an objective framework. Therefore, the crux of the issue relies on identifying society’s recognizable, reasonable expectations.

68. Updating personal social media accounts like Facebook, using Twitter, and texting to express ranges of emotions are essential and integral activities of a contemporary individual living within a wired social fabric. Just like the inside of the private dwelling provides an inner sanctum for that individual to evolve into her desired existence, updating Facebook and Twitter and texting provides that self-expression outlet for the post-modern existential being. Therefore, like the individuals evolving inside the private dwelling has the Fourth Amendment privacy right despite the deleterious influence of law enforcement paradigm and technology based intrusion, individuals interacting within Facebook, MySpace, and Twitter also possess the right to privacy in their self-expression. This desire for protecting an individual’s self-expression must be recognized in construing right to privacy for an individual in a bilateral relationship like that within an employer-employee relationship.

69. *Quon*, 130 S. Ct. at 2630

70. See Ghoshray, *Privacy Distortion Rationale*, supra note 64, at 67-68.

71. The Court’s observation in *Quon* is in the context of a public employee’s Fourth Amendment right against his employer’s “unreasonable searches and seizures.” See *Quon*, 130 S. Ct. at 2627. Applying this standard might provide an employee a much higher protection against employer surveillance, as the *Quon* Court recognized the employee as an individual who had a right to self-expression in the social media.

72. The *Quon* Court’s observation, however, is applied in the context of a public employee-employer relationship, which is a rather restrictive scenario. An employee’s privacy protection in the workplace varies as a function of the nature of the bilateral employee-employer relationship that defines the contour of the “operational realities of the workplace.” See O’Connor v. Ortega, 480 U.S. 709, 717 (1987) (linking employee right to privacy with the operational realities of the
On the contrary, however, in an environment where unprecedented advancement in surveillance technology has empowered an employer with a superior ability to track every digital footprint of an employee, it is important to have a protectionist threshold available to a targeted employee. This would allow for the development of a reasonable surveillance paradigm. Against the paucity of applicable legislative enactments, ultimately, such a paradigm may be better framed via legal guidance obtained from the Fourth Amendment jurisprudence, more specifically, through its *Katz* doctrine.

A. Applying the *Katz* Doctrine in Employer Surveillance of Employees

Despite society’s pervasive digital immersion, an ordinary citizen within society has little or no knowledge of the extent of an employer’s superiority in advanced surveillance techniques. As most employees are hopelessly unaware of the available surveillance they might be under, an individual employee may be at a disadvantage in adequately developing her viewpoint on the scope of employer surveillance. This awareness is important in developing a nuanced roadmap through which to analyze an employee-employer relationship within the workplace – a reality that derives its existence from the nature of employee-employer relationship. Thus, the Supreme Court jurisprudence on employee protection from privacy intrusion is neither settled nor fixed. History of the Court’s jurisprudence has shown the Court adopting a range of approaches. Especially, the Court has given employers a much higher threshold with which to conduct searches of employee communication if such searches are conducted more with the objective of protecting employer’s legitimate business interests, such as, for investigation of employee misconduct at work, or in the context of probing employee misdeeds. See *Ortega*, 480 U.S. at 725.

73. The asymmetry between technological sophistication of an employer’s surveillance and the targeted employee’s awareness of such technology can be compared with the asymmetry that exists between the technological sophistication of United States’ drone operation in Afghanistan and Yemen and the awareness of such drone’s tracking of its target, the suspected terrorists. Thus, most employees have very little idea about the sophisticated tracking ability of their employers’ digital surveillance methodologies and mechanisms. Currently, a variety of employer surveillance software use keystroke-logging mechanisms to follow employees’ digital footprints. The more sophisticated and accurate keystroke logging devices are capable of identifying and keeping records of every keystroke performed by a specific employee. Among the more generic ones, for example, some advanced software can track, monitor and identify occurrences of inappropriate language in employee e-mails. By measuring frequency and pattern of keystrokes, some devices routinely identify and monitor employees in scenarios when employees access employer databases. See Swaya & Eisenstein, supra note 22. In some contemporary employee surveillance, employee monitoring is being done by installing devices that function like global positioning satellite (GPS) tracking devices on company vehicles. See Kendra Rosenberg, *Location Surveillance by GPS: Balancing an Employer’s Business Interest with Employee Privacy*, 6 WASH J. TECH. & ARTS 143, 152 (2010).


75. See supra note 73.
context of a digital footprint search. Residing in this awareness is a balancing paradigm that illuminates the Fourth Amendment to determine how far an individual’s privacy should dictate the limits of a supervisory power – whether coming from the government or from an employer acting in a supervisory capacity.76

The Supreme Court’s adoption of a new standard in Katz, based on Justice Harlan’s concurrence77 opened a new lens through which to evaluate individual privacy against an onslaught of technological advancement. Besides law enforcement intrusion cases, the Katz doctrine has become the reference point for balancing individual privacy against law enforcement supervisory interests according to the Fourth Amendment.78 Justice Harlan articulated a two-fold test for Fourth Amendment protection against unreasonable searches that can be extended to employer surveillance as well. Thus, Katz provides a definitive framework through which to evaluate how far an individual’s privacy should restrict the scope of a supervisory power.79 According to the Katzian construction, privacy violation is to be determined through a two-prong test.80 First, the individual must exhibit an actual and subjective expectation of privacy.81 Second, upon satisfying this threshold, we must evaluate whether, such expectation is one which the broader society is prepared to recognize as ‘reasonable.’82

Continued viability of the above construction comes from the fact that in articulating his two-prong test, Justice Harlan followed the Katz majority’s robust interpretation of the Fourth Amendment that, “[t]he Fourth Amendment protects people, not places.”83 Thus, by staying consistent with the Amendment’s original purpose, the Katz framework has retained validity in defining the contours of Fourth Amendment individual expectation of privacy, even nearly a half-century after Justice Harlan’s “reasonable expectation of

76. In my view, search of an individual’s personal space, regardless of whether it is a physical dwelling or a virtual community, can be brought under a robust constitutional trajectory by following the main doctrinal trajectory of Justice Harlan’s two-part test. The limits to the surveillance power of a supervisory entity can be reasonably identified by evaluating the scope of an individual’s expectation of her own privacy. Therefore, the broader fundamental I seek to develop in the current analysis is that, a threshold for search and seizure within the context of an individual’s private space can be developed by keeping the basic premise of privacy and liberty of the Constitution viable against an onslaught of technological advancement.
77. See Katz, 389 U.S. at 361.
78. See generally Winn, supra note 66.
79. Id.
80. Id.
81. Id.
82. Id. (stating that an individual’s interest in privacy involves determining whether an individual’s subjective expectation of privacy is one that society is willing to recognize as “reasonable”).
83. Id. at 351.
privacy” test. In providing a definitive guidance related to various instances of search and surveillance, *Katz*, provides a threshold for the individual’s subjective expectation of privacy – a threshold that must be evaluated within the evolving context of contemporary individual’s immersion in digital social media. This revitalized look at the fundamental privacy interests opens up to two main threads from *Katz*: (a) the nature of an individual’s expectation of privacy, and (b) the relationship between an individual’s expectation and society’s recognition of what expectation is reasonable.84

Evaluating individual’s subjective expectation of privacy requires both qualitative and quantitative constructs. Here, the qualitative aspect is gleaned from the fact that, although individual expectation is understood to be subjective, such subjective aspects must comport with the actual expectation of the individual.85 The quantitative aspect is derived from the fact that, the means of evaluation is dependent on identifying society’s reasonable expectation, a more measurable and identifiable framework.86 This can be recognized as a predominantly objective framework, which calls for a reliance on identifying society’s reasonable expectation.87 Developing a relationship between an objective framework and a subjective framework may be conceptually difficult. However, such difficulty could be overcome by identifying a set of deterministic benchmarks, such as a set of deciding factors, from which determination can be made.

In trying to identify the scope of an individual’s actual expectation of privacy, it is important to develop all ancillary fact patterns surrounding the individual’s behavioral pattern. Thus, if an individual exhibits a shared sense of space, for example, as manifested in her reluctance to utilize available privacy settings within her digital communication pathway, her actual expectation of privacy may be recognized as having a lower threshold. Contrarily, by utilizing all available privacy settings, one of her Facebook friends could expect a comparatively higher threshold for his expectation of privacy. In this way, although individual expectation of privacy may be both subjective and recognized within a spectrum, they nonetheless, represent the actual expectation of the relevant individual.

85. Here I draw attention to the derived fundamentals of *Katz* two-part test. In this construction of individual privacy, regardless of the subjective nature of such individual privacy, it is ultimately based on a broader society’s evaluation of what is reasonable or not. Thus, privacy is determined based on societal recognition of what is considered legitimate or illegitimate. The fall out of this framework is a gradual decoupling of the element of trespass from the framework, as I have noted elsewhere. See Saby Ghoshray, *Looking through the Prism of Privacy and Trespass: Smartphone’s New Challenge for the Fourth Amendment*, 14 UDC/DCSL L. REV. 73, 74-75 (2012).
86. See Ghoshray, *Privacy Distortion Rationale*, supra note 64, at 56-57.
87. Id.
Thus, staying within the framework of an individual’s subjective expectation, it is possible to identify various subjective thresholds within a wider spectrum. These thresholds can be viewed as triggers left along an individual’s digital footprints. Identifying such footprints would not only reveal contents of an individual’s life, but, more importantly may be used as benchmarks to evaluate an individual’s expectation of privacy. Evaluating these triggers may require an examination of the individual’s digital profile in order to evaluate the pattern of digital exchanges through asking a series of questions. How much sharing of private personal communication the individual conducts? At what frequency does such individual share sensitive personal information with wider society? Does the individual use widely available and appropriate privacy settings in her digital environment?

Identifying the online persona of an individual is important in analyzing the applicable and allowable limits of an employer’s surveillance. In this evaluation, an employee’s behavior can become a predictor of her privacy threshold. For example, if an individual’s digital persona exhibits a disregard for privacy in her online exchanges88 could then such an individual be recognized for having a heightened subjective expectation of privacy? An initial assessment of an individual expectation of privacy would then turn on the second phase of construction to evaluate the nature, scope, and quantitative element in that subjective expectation.

A series of steps may determine what makes that subjective expectation a reasonable expectation. First, as a matter of law, an employee’s subjective expectation of privacy cannot be created in a vacuum. It must have the stamp of approval from society’s reasonable expectation of privacy. Yet, an employer can preempt such community-based expectations of an employee by presenting a more compelling case of legitimate business rationale that may render the individual’s identified reasonable expectation illegitimate. There may be a variety of exigent scenarios that can render an individual expectation illegitimate on account of compliance and violation issues.

Second, evaluation of society’s reasonable expectation has been the subject of debate in various parlances. Implicit in this evaluation is the concept of Third-Party doctrine.89 For the purpose of the current analysis, I shall restrict the

88. See discussion infra note 123 (observing various cases showing employee violation of various employer-employee relationships on account of social media exchanges).
89. See generally Ghoshray, Privacy Distortion Rationale, supra note 64. In my view, what is constitutionally protected under the Fourth Amendment calls for a reinterpretation or complete overhaul of its doctrinal underpinnings; more importantly, the Third-Party doctrine. This has been argued from both sides of the aisle. Within the context of scholarly criticism of the doctrine, there remain two distinct groups. The first group, trailblazers of sorts, began the movement by professing the doctrinal difficulties against technological advancement beginning in the 1980’s. See, e.g., Gerald G. Ashdown, The Fourth Amendment and the ‘‘Legitimate Expectation of Privacy’’, 34
scope of Third-Party doctrine by noting that its implication should be based on
the fact that society’s reasonable expectation for privacy can be attenuated in the
digital communication era if individuals engage in sharing protected information
to a third-party service provider. 90 Given the doctrinal implication of the third-
party that might bring additional complexity in the employee-employer bilateral
relationship, this should remain outside the scope of the current discussion. 91
Moreover, I have already discussed elsewhere the interesting and complicated
dichotomy between human interaction and automated interaction 92 – the bone of
contention in the doctrinal difficulty in Third-Party doctrine. Therefore, let us
focus on other factors that impact the relationship between an individual’s
subjective expectation of privacy and society’s reasonable expectation of such
privacy.

Third, while charting an allowable territory for an employer to track its
employee’s digital footprint, it is important to identify the outliers. By outlier, I
refer to that set of individuals whose subjective expectation of privacy may not

90. See Ghoshray, Privacy Distortion Rationale, supra note 64, at 64.
91. Id. at 64-69 (noting the relationship between a possible attenuation of the Fourth
Amendment protection resulting from individual’s reliance on third-party based on strictly
communication needs is an evolving area of jurisprudence).
92. Id. at 80. The idea of evaluating individual’s subjective expectation of privacy based on
society’s reasonable expectation has an inherent drawback. For example, if majority within the
society is sufficiently acclimatized into digital communication via social media, the majority’s
privacy expectation may not comport with the minority population that are consciously decoupled
from pervasive digital immersion. Thus, society’s reasonable expectation cannot be a proxy to these
individuals’ privacy expectation. Should there be a different test of evaluating individual’s
subjective expectation of privacy, or society should imposed a flawed variant of privacy
expectation upon these individuals. Law must be structured in such a way that all individuals’
privacy concerns are adequately addressed by its imposition.

VAND. L. REV. 1289, 1315 (1981); Arnold H. Loewy, The Fourth Amendment as a Device for
Protecting the Innocent, 81 MICH. L. REV. 1229, 1248-50, 1254-55 (1983); Scott E. Sundby,
“Everyman’s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?” 94
COLUM. L. REV. 1751, 1757-58 (1994). While these articles questioned the doctrine’s continued
viability even before the mass assimilation of cyberspace enabled social media, the second group
has been more persuasive in their argument because of the very same reasons. See, e.g., Jack M.
Balkin, The Constitution in the National Surveillance State, 93 MINN. L. REV. 1, 19 (2008); Susan
W. Brenner and Leo L. Clarke, Fourth Amendment Protection for Shared Privacy Rights in Stored
Transactional Data, 14 J.L. & POL’Y 211, 211-14 (2006); Susan Freiwald, First Principles of
Communications Privacy, 2007 STAN. TECH. L. REV. 3 (2007); Stephen E. Henderson, Beyond the
(Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of
Us Too, 34 PEPP. L. REV. 975, 976-77 (2007); CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW
GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT, 151-54 (2007); Daniel J. Solove,
Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. CAL. L. REV. 1083,
1089-1095 (2002). On the other hand, scholars have argued passionately as to why the doctrine
should retain continued relevance in jurisprudence. See, e.g., Orin S. Kerr, Four Models of Fourth
Amendment Protection, 60 STAN. L. REV. 503, 519-22 (2007); Orin S. Kerr, The Case for the
Third-Party Doctrine, 107 MICH. L. REV. 561, 561 (2009); see also Ghoshray, Privacy Distortion
Rationale, supra note 64.
comport with the society’s reasonable expectation of privacy. The law surrounding use and abuse of a social network must adequately address these issues, failing which the equality doctrine might be in jeopardy. For example, individuals that are not active in social media, or those who do not engage in extensive digital immersion, may expect a much higher privacy protection. Their privacy rights must be evaluated at a more elevated threshold than the other individuals discussed before. The law must ensure that such a lone ranger, is protected from the deleterious impact of society’s mass adoption to social media. Individual conception of a subjective expectation of privacy must not be co-mingled with those of the majority. The employee-employer legal framework must structure reasonable protection for such individuals, failing which the privacy jurisprudence might get further modulated much the similar way the Third-Party doctrine has made inroads into the doctrinal bulwark of the Fourth Amendment. Because, even if one is not immersed in technology, by virtue of living in the society, this individual might become subjected to the broader societal norms.

Fourth, in this discussion of charting a framework for employee-employer relationship and the delineating of an individual’s subjective expectation of privacy, it is important to understand how an individual’s personal behavior may be shaping her own expectations, an area that has not received much attention in contemporary discourse. In the following, I develop a more realistic linkage between individual’s subjective expectation and society’s reasonable expectation through individual behavior in social media.

B. Individual Behavior Shaping Subjective Expectation of Privacy

Today’s individuals live in a digitally connected world in which they form communities - mostly self-selected and closed groups. Yet, paradoxically, these digitally immersed individuals allow their digital DNA to flow across cyberspace. 

93. The idea of evaluating individual’s subjective expectation of privacy based on society’s reasonable expectation has an inherent drawback. For example, if majority within the society is sufficiently acclimatized into digital communication via social media, the majority’s privacy expectation may not comport with the minority population that are consciously decoupled from pervasive digital immersion. Thus, society’s reasonable expectation cannot be a proxy to these individuals’ privacy expectation. Should there be a different test of evaluating individual’s subjective expectation of privacy, or society should imposed a flawed variant of privacy expectation upon these individuals. Law must be structured in such a way that all individuals’ privacy concerns are adequately addressed by its imposition.

94. See generally Ghoshray, Privacy Distortion Rationale, supra note 64, at 64-67 (noting how the Third-Party doctrine may have erroneously attenuated the privacy protection of individuals immersed in digital communication).

95. See Kobrin, supra note 51.
Updating Facebook status, using Twitter, and texting to express emotions are digital activities that are analogous to activities individuals perform within their physical private dwelling. Just as the inside of the private dwelling provides an inner sanctum for an individual to evolve into her desired existence, updating Facebook, Twitter tweeting and texting are components of existential nature. Just as individuals inside their private home have the full complement of Fourth Amendment privacy rights without the deleterious influence and attenuated nuance of the Third-Party doctrine, individuals evolving within Facebook, Instagram, and Twitter should also possess the right to be left alone.

However, while the formation of a community, a self-selected group, may be a necessary prerequisite to exist in this new digital universe, the über-connectivity may have given digitally immersed individuals a flawed sense of empowerment. Individuals immerse themselves in a digital world to present a scripted display of self-advertisement, where the same individual is the writer, producer, and the story teller within a connected environment. Here, the subscribers wait for the next update, the next tweet in this continuously unfolding saga of individual story telling. In the process, these individuals mostly put out “half-baked” and “unbaked” ideas for public consumption. These mostly private musings, which in earlier generations would have remained within the sacrosanct sanctum of secluded moments of private affairs, now get unleashed into the open cyberspace - ready to be viewed, commented on and, often times ridiculed.

Thus, many questions arise. Does an individual’s personal digital exchange lose privacy protection by virtue of having been unleashed upon the public space? Should deliberately disseminated digital communication lose privacy protection on account of its creator’s lowered expectation of privacy?

While arguing for the need to retain the sanctity of individual privacy, we must accept the ground reality. This ground reality provides us with a cautionary tale, a tale of flawed empowerment gone wild. Through these unbridled acts of self display, individuals continue to erode their own expectations of privacy. In

96. See supra note 52.
97. See Ghoshray, Privacy Distortion Rationale, supra note 64, at 82.
98. Id.
99. See supra note 52.
101. See supra notes 65- 66 and accompanying text.
this pursuit, individuals are enabled by corporations that continuously flood the market with newer, lighter, faster accessible gadgets to send messages faster and more frequently. While the digital barriers of privacy continue to become lowered, an individual’s behavior shapes the subjective expectation. This is because at the root, a behavior is an outer expression. Within this expression resides an individual’s stored thought – the thought that manifests in external behavior, while being disseminated through a slew of digital gadgets to connect individuals solely for profit making purposes. Corporations, in essence are a catalyst to lower individuals’ expectation of privacy, as society is predominately formed by such individuals. Therefore, the contemporary society’s digital immersion driven subjective expectation of privacy is not necessarily distinct from Katzian conception of individual privacy that society might consider reasonable.

C. Lowering Subjective Expectation of Individual Privacy Via Seduction to Symmetry

Individuals immersed in social media often are driven by an exigent need to update on almost every instance of their personal lives. Since the majority of these individuals are connected to many other individuals via social media, any one-to-one connection automatically becomes a many-to-many connection. As a result, despite various privacy settings offered in social media, intimate personal details might not stay cloaked within the sacrosanct sanctum of an individual’s personal space. Often times, an individual may be eroding their own expectation of privacy, without even recognizing the long-term deleterious impact of her personal behavior.

Thus, within a discussion of individual privacy erosion, we must not necessarily implicate the employer surveillance alone. Irrespective of the enhanced surveillance capability an employer possesses, irrespective of the digital norm of society, an employee cannot decouple from individual responsibility. Regardless of an ever-enchanting array of digital gadgets corporations place before individuals to digitally immerse society, they also offer various privacy mechanisms that individuals can deploy. Despite the ease of digital communication, in order to establish an individual right to privacy in cyberspace, such individual should adequately protect the gateway to her individual communication. Yet, individuals continue to engage in a promiscuous

104. Id.
exchange of private information in social media. Let us examine the anatomy of such behavior through the concept of seduction to symmetry.105

Seduction to symmetry is the complex phenomenon of social ordering in which majority members’ viewpoints gravitate toward a more socially acceptable side of an argument.106 This sociological trend manifests itself by members of the society exhibiting a predominant bias towards one side of an argument. Here, symmetry acts as the end point towards unification. This unification process proceeds through cohesion amongst members’ behavioral norms and adoption to a predictable set of societal mores, where an emergence of divergence is considered dissent. In a framework where cohesion is the desired target state, any dissent threatens the originator of dissent with expulsion from the community.107 Thus, seduction to symmetry is an enticement to a desired community, where acceptance within the community is predicated upon the member following accepted principles of the community.108 Within the digital context, a set of accepted principles function as society’s imposition of adopting a social media centric mode of communication, where proper conduct would be


106. *Id.* By seduction to symmetry, I refer to the complex phenomenon of social ordering in which majority members’ viewpoints gravitate toward a more socially acceptable side of an argument. This sociological trend manifests itself by members of the society exhibiting a predominant bias toward one side of an argument. Symmetry is unification. This unification process proceeds through cohesion amongst members’ behavioral norms and adoption to a predictable set of societal mores, where an emergence of divergence is considered dissent. In a framework where cohesion is the desired target state, any dissent threatens the originator of dissent with expulsion from the community. Thus, the seduction to symmetry can be seen as an enticement to a desired community, where acceptance within the community is predicated upon the member following accepted principles or proper conduct. Often times, after a community is rocked by violent conduct, both a set of accepted principles and proper conduct are promulgated. Within the context of an all-pervasive digital immersion, often times, late adopters adapt to majority’s social norm, even if they have personal reservations against doing so. These dissenting voices do so, predominantly for fear of facing a de facto expulsion from community should they consider not following the community’s so called accepted principles. Thus, seduction to symmetry is a process that can be either imposed upon an individual, or the targeted individual could be drawn to the symmetry. Individual members of the society fall victim to the seduction to symmetry for various reasons, the most significant of which is the inability to bear the cost of being in asymmetry to their environment. Symmetry is the state of being in unison with external forces or at tandem with the external environment. Asymmetry is the state of being in contradiction with the environment. This may include either being in conflict with accepted principles of the community or being in contradiction with the behavioral modes of conduct, all of which can impose various forms of cost upon the individual attempting to decouple from the symmetry. Therefore, seduction to symmetry can often be an existential response to external stimuli. And an often time, seduction to symmetry is a natural tendency to traverse the path of least resistance, in which the agent does not incur the cost of traveling against the societal trend.

107. *Id.*

108. *Id.*
recognized in the individuals engaging in frequent status updates. Often a non-conforming Facebook friend faces a \textit{de facto} expulsion from the community or by being de-friended. Thus, seduction to symmetry is a process that can be either imposed upon an individual, or the targeted individual could be drawn to the symmetry. Individual members of the society fall victim to the seduction to symmetry for various reasons, the most significant of which is the inability to bear the cost of being in asymmetry to their environment. Symmetry is the state of being in unison with external forces or at tandem with the external environment. Thus, the contrasting status of being in asymmetry is the state of being in contradiction with the environment. This may include either being in conflict with accepted principles of the community or being in contradiction with the behavioral modes of conduct, all of which can impose various forms of cost upon the individual attempting to decouple from the symmetry. In an environment where formation of communities and exchange of information mostly occurs online, being de-friended in social media is tantamount to being lonely in society – a cost most individuals are not willing to incur. As a result, private exchanges continue unabated in cyberspace, allowing individuals to leave an expansive digital footprint for search and surveillance.

IV. SCOPE AND LIMITS OF EMPLOYER RIGHTS IN THE DIGITAL WORLD

Contemporary society offers an individual a plethora of choices. Yet, often times, most of these choices are either one-dimensional or simply coerced. For example, in a social-media driven frenzy, an individual is continuously coaxed and cajoled into setting up profiles in additional social media channels – be it Facebook, Instagram or Pinterest. Similarly, a potential employee is reprimanded by friends and professionals about the dangers of not setting up a profile in the popular employment based online community like LinkedIn.\textsuperscript{109} Predictably, the individual finds herself fully immersed in social media. Soon, her digital footprints begin to be stored in cyberspace. Therefore, an individual’s exuberance to be seen, to be known and to be über-visible in social media, propels such individual to leave behind her digital footprints.

Leaving digital DNA in cyberspace, however, does not decouple an individual from her fundamental rights - the rights of privacy and a right to be left alone, an area I have interpreted elsewhere.\textsuperscript{110} Both the employee and the employer exist in a bilateral relationship within a bilateral and complimentary framework. Both have certain rights within the shared space. These rights do not evolve in a vacuum. Neither, do they evaporate readily. And, we must

\textsuperscript{109}. See Ghoshray, \textit{Privacy Distortion Rationale}, supra note 64, at 82-83 (observing the existential need for post-modern individuals in belonging to digital social networks).
\textsuperscript{110}. \textit{Id.} at 82.
understand the dynamic nature of these rights. When two apparently complimentary entities evolve within a shared space, friction develops.\textsuperscript{111} Germinated via the evolution of a competing set of rights, competing interests of these complimentary entities interact.\textsuperscript{112} They interact to find the answer to whose rights might prevail. Against this general backdrop, the following discussion identifies a new reality of why individual behavior online may have given post-modern employer an enhanced right for surveillance of its employees.

\textbf{A. Recognizing Employer Right as a Function of Employee Behavior}

Driven by the urgency to assimilate into an all pervasive digital world, a prototypical employee enjoys an active online presence and exhibits predictable social media behavior. In the process, the individual generates and leaves behind a sizable digital footprint in the cyberspace.\textsuperscript{113} These digital footprints act as catalyst for an employer to embark on surveillance to regulate and modulate employees’ social media activities.\textsuperscript{114} One of the real tangible impact of über-digitization of contemporary society is granting an employer a much broader right of surveillance of its employees on account of such employees' excessive online activities.

The context of an individual’s loss of privacy is important. As identified above, individual privacy attenuation results from such individual’s over indulgence in the digital media. Often times, such abrogation of privacy may be an outgrowth of unscrupulous or irrational use of individual choice by the employee. There is an apparent paradox in this argument. The right to privacy is a fundamental liberty component. By its very invocation, liberty connotes individual pursuit of freedom - a freedom animated in the search for choice. Choice has multiple prongs of decision outcomes. Through her unbridled digital

\textsuperscript{111}. In this narrative of rights, invocation of rights continues along fluid lines. Sometimes legal rights of two entities occupying a shared space may undergo some friction, whereby one entity’s right may be suppressed against the right of another. For example, workplace environment is a shared space, where through a bilateral relationship structured in settled laws and evolving regulations, employer and employee continuously interact with a view to assert each other’s right. While an employer is fundamentally concerned with upholding legitimate business interest of the corporate entity, the employee is interested in ensuring its privacy interest. In this continuous tug-of-war between rights of two competing entities connected by a bilateral interest, one entity’s right may be subsumed into the other entity’s right until the next judicial determination or legislative enactment. These result in the emergence of diverging strands of rights within a broader right continuum. Therefore, in order to develop an adequate supervisory framework to delineate employee-employer relationship within the evolving confines of social media, it is important to granulating these commingled rights under distinct threads of labor law, corporate law and fundamental privacy doctrines will help in understanding this complex legal narrative.

\textsuperscript{112}. \textit{Id.}

\textsuperscript{113}. See Kobrin, supra note 24.

\textsuperscript{114}. See supra note 53.
pursuit, an individual sacrifices her privacy in social media. On the contrary, by limiting her choice of how much and how promiscuous\textsuperscript{115} her digital engagement is, the same individual may expect a higher threshold of privacy. Thus, liberty endows an individual with a right of exercising rational choice. Within the context of privacy shrinkage at workplace, the emerging reality of social media communication must be seen through this prism of an individual’s rational choice.\textsuperscript{116} In this tension between choice and privacy, how does exercising one’s individual choice jeopardize such individual privacy?

Technology’s sophistication and pervasive access to digital gadgets have provided an individual with an over abundance of choices. What an individual does with that access is what would shape the contours of some individual rights. How much self-aggrandizement an individual might engage in is predominantly an individual choice. Technology is available to use in the most prudent way - in a way that neither implicates privacy nor unnecessarily extends one’s choice. Unfortunately, this abundance of choices may have begun to complicate the basic fundamentals of privacy in the post-modern era. As Judge Kozinski has alluded to, a majority of individuals are pursuing temporary glorification in the social media. Often times, they announce their importance by unleashing in cyberspace incomplete ideas and immature thoughts,\textsuperscript{117} leaving open the floodgates of private communications for other individuals to peek in. The abundance of digital footprints left by an individual now becomes readily available for employer surveillance. By virtue of her conduct, the individual has already lowered her expectation of privacy against such a search.

By searching these digital footprints, an employer can cultivate and compose an individual’s comprehensive profile for further review. Such review can then be used to make decisions about the employee’s future. Leaving these digital footprints in the cyberspace is borne out of a choice – a choice that was available to the individual. Yet, in the flawed pursuit of self-importance, the individual continued to share personal information with her digital community, while lowering her privacy threshold along the way.\textsuperscript{118} Thus, faulty exercise of choice by employees may have given today’s’ employer an opening for surveillance. Privacy shrinkage after all, may have been a natural outgrowth of such choice.

\textsuperscript{115} By promiscuous, I do not assert any aspersion on an individual’s character, rather the word “promiscuous” is being used to reflect the unbridled and non-discriminatory nature of digital exchange an individual partakes in.

\textsuperscript{116} By rational choice, I draw attention to the relationship between individual’s choice and her expectation of privacy. In this paradoxical dynamics, by lowering her choice set, an individual may be able to extract a higher threshold of privacy. On the other hand, by expanding her choice set in her pursuit of social media driven exchanges, the same individual may be lowering her expectation of privacy. Therefore, an individual may be able to balance her social media exuberance and have a heightened expectation of privacy by selecting a rational set of choices.

\textsuperscript{117} See Kozinski, supra note 100.

\textsuperscript{118} See supra Part III.
B. Seduction to Symmetry – Connected, Yet Invisible

Technology and social media have bestowed upon today’s individual a unique modicum of communication. In this new mode, an individual no longer has to communicate with other individuals on a level of palpable immediacy. For her communicating needs, an individual is no longer needed to hear voices on the other end, nor is she compelled into looking at another individual’s eyes. Membership in the social media, the ability to be connected at all times has lifted the traditional veils of behavioral drawbacks - nervousness, anxiety and awkwardness. Thus, the individual can stay protected from the peering eyes of a fellow individual and still can communicate. Like a contagious impulse, this digital immersion has engulfed society, where an individual is constantly eye-locked into a fixed digital screen. As she communicates, she instantly exchanges information, frequently and simultaneously with multiple individuals. This communication mode is part of a pervasive seduction to symmetry. Reluctant to exercise individual uniqueness, the individual is unable to break from such symmetry. This inability compels the individual to respond to innumerable tweets and status updates, and the invisible nature of such communications provides the additional impetus. Yet, this seduction to symmetry is a function of the choice – the choice of the individual to stay locked in the symmetry or to break out of the symmetry.

Seduction to symmetry is not the focal point of this discussion, as I have explained this phenomenon in pertinent details elsewhere. But the idea of seduction to symmetry is a lens through which to understand the society’s digital immersion. This seduction is a viable force. It should be recognized as a phenomenon, through which to understand why these individuals continue to make choices - choices that continue to abrogate their expectations of privacy. How the expectations of privacy may have shrunk over the years can be seen through a comparison of two periods – the pre-Katz era and the post-Katz era.

For example, when the Katz case was decided, this seduction of symmetry was not such a potent force, as there may have been more divergences and disconnects between individual’s subjective expectation of privacy and society’s reasonable expectation of such privacy. In other words, in the pre-social media era, the natural divergence between individual’s subjective expectation of privacy and society’s reasonable expectation of privacy provided some cushion of uncertainty in the eyes of the courts and the judges. In the post-modern era, digital immersion is so wide-spread that the cushion is no longer there. By forcing mass adoption of ideas and ideologies, the seduction to symmetry may have reduced the divergence between an individual’s subjective expectation of

119. See Ghoshray, Seduction to Symmetry, supra note 105.
120. I have used seduction to symmetry and seduction of symmetry interchangeably.
privacy and the society’s reasonable expectation of privacy. This may ultimately provide an employer with a stronger rationale to conduct surveillance as the individual may have shaped her own destiny toward a much lower threshold of privacy than before.

C. Employer’s Surveillance Rights against a New Reality

Although individual’s privacy right may be shaped by individual behavior, there must be limits to how far an employer can conduct surveillance on employee’s digital footprints. The scope of employer surveillance must therefore, be based on a robust framework defined through a set of established paradigms.

In this surveillance framework, employer surveillance should be triggered by an employee conducting herself outside the predicated norm. Articulated in the employee handbook, such rules should clearly limit the employee’s allowable behaviors and connect such limitation with the scope of surveillance. How far the surveillance is able to intrude upon employee’s privacy is to be determined by the set of signature pattern of behaviors that the employee engages in at the workplace.

An employee’s engagement in a particular signature pattern of behavior, must not give the employer carte blanche continuous surveillance. Such surveillance should be based on two main paradigms: (i) an employer’s legitimate business interests, connecting an employee’s social media activities with possible loss of productivity and, (ii) an employer’s exposure to liability from an employee’s social media activities triggering either a regulatory review, or potential defamation of fellow employees.

121. See supra Part IV A

122. One of the drivers for employer surveillance is enhancing or sustaining workplace productivity. The general concern an employer may have relates to work stoppage via employee social media activities, causing drain on productivity. Yet, complete prohibition of employee social media activities may adversely affect employee morale. This, indeed, may negatively impact employee morale as well. See Renee M. Jackson, Social Media: Counsel for Clients and Firm Managers, LAW OFF. MGMT. & ADMIN. REP. (Apr. 2010), at 1, 14 (“The most obvious hazard regarding the use of social media during employment is internal to the organization: Employees may spend so much time using social media during working hours that productivity decreases.”). This is, however, not a new phenomenon. Employee’s digital presence has been causing employer concern ever since use of internet and email has become widespread at workplace. Social media usage has added another new layer upon employee digital presence at workplace. See Teresa Thompson, Time Suck Or Moral Booster: How Does Social Media Impact Employee Productivity?, NETWORKED (Mar. 19, 2011), http://www.networkedlawyers.com/time-suck-or-morale-booster-how-does-social-media-impact-employee-productivity/.

123. Due to its speed of information transmission and pervasive use, social media use by a company’s employees can have significant reputational risk for an employer. Like in most cases, an employee may not be aware of the highly sophisticated surveillance capability of its employer, an employer may not be aware of how its employee’s use of social media could be generating a
In identifying an employer’s legitimate business interests in the scope of employee surveillance, two major points must be noted. First, employers have a legitimate business interest in ensuring their employees are productive. Based on the identification of a signature pattern, if an employer observes an employee devoting a disproportionate amount of work hours engaged in social media, the employer may have a legitimate right to conduct surveillance and collect her digital footprint. The products of such searches can be used to discipline, penalize, or even terminate such employees. Second, if an employee’s social media exchanges reveal wrongdoings like giving out trade secrets, signaling competitive positions, or proprietary information, the employer may be within its legitimate right to employ constant monitoring of every digital footprint of such an employee. We must recognize that the Fourth Amendment does not preclude an employer’s right to a meaningful existence. Privacy of an individual in this context is not a blank check to engage in unbridled exchanges of digital information cloaked under the sanctum of individuality.

Similarly, an employer has the legitimate right to protect itself from liability. Liability can arise in two forms: (i) liability from an employee that may have been the subject of an improper communication exchange of the employer’s employee and, (ii) liability from breach of corporate regulations by the employee. In both cases, the employer is within its legitimate right of sustained surveillance of the employee.124

negative image of the company, thereby causing reputation loss in the market place. Often times, when a company is being perceived in a derogatory light in its relevant marketplace, it may invite regulatory look into the affairs of such organization. For example, Facebook has what is known as “community pages” which are general sites dedicated to certain topics (or businesses) developed based on information provided in personal profiles. See Kashmir Hill, Law Firm Facebook Pages Reveal How Associates Really Feel (June 1, 2010, 3:05 PM), http://abovethelaw.com/2010/06/law-firm-facebook-pages-reveal-how-associates-really-feel (observing how an employee’s uploading of a profile on a dedicated web page may adversely impact the relevant employer).

124. A slew of litigation against employers in the last decade reveals a potential Achilles’ heel of an employer that comes from employee communication in digital media. When an employee uses an employer issued computer, smartphone, or email account and communicates with the outside world, such act of communication exposes the issuing employer to lawsuits for defamation, harassment, or any such illegitimate act of its employee. See Blakey v. Cont'l Airlines, Inc., 751 A.2d 538, 543 (N.J. 2000) (reversing a motion to dismiss in favor of the defendant Continental Airlines for failure to properly respond to its employee’s harassment of a fellow employee by using a company electronic bulletin board) (observing, “[a]lthough the electronic bulletin board may not have a physical location within a terminal, hangar or aircraft, it may nonetheless have been so closely related to the workplace environment and beneficial to Continental that a continuation of harassment on the forum should be regarded as part of the workplace”). See Krinsky v. Doe, 72 Cal. Rptr. 3d. 231, 234 (Cal. App. 2008) (arguing whether the identity of the creator of a pseudonymous poster on a financial message board should be disclosed for possible punishment on account of conversation that has “devolved into scathing verbal attacks on the corporate officers of a Florida company, prompting a lawsuit by one of those officers”). Scholars have noted the increasing vulnerability employers face with the rise of social media use by employees, either during work hours or by virtue of using company’s computers. See Laura Thalacker and Jelly
Despite wide latitude granted to the social-media behavior of its employees, an employer may not engage in an unbridled or discriminatory surveillance of its employees. There are limits to such acts. Curiosity, vendetta and personal issues can never be legitimate grounds for employer surveillance of an employee. Personal issues related to curiosity and vendettas do not fall in the category of legitimate business interests. Their non-fulfillment does not trigger employer liability either. Therefore, under no circumstances should an employer be allowed to impinge upon individuals’ Fourth Amendment right to privacy.

The reality of pervasive social media usage by employees invites us to explore when an employer is within its legitimate rights to engage in surveillance. Surveillance may be justifiable on grounds of probable cause of employee violation as revealed in examination of the signature behavior patterns of an employee. If a review of employee’s signature behavioral patterns reveals a threat to employer’s legitimate business interests, or signals a potential for employer liability, the threshold of probable cause for surveillance may be achieved. Only then can an employer be legally permitted to engage in surveillance. The results of such surveillance could then be utilized to make decisions on the outcome of the employment relationship in question.

V. CONCLUSION

In the limitless possibilities of a hyper-technological era, contemporary society is increasingly confronted with newer challenges. Pervasive digital immersion of individuals awakens us to emerging tensions between social norms and fundamental rights. On one side of this equation are the ease, access, and sophistication of technology manifested in newer modicums of social media driven communication. On the other side is the debilitating specter of privacy loss individuals are facing in almost every aspect of their lives. Employee privacy in the workplace is of no exception. Retaining individual privacy has become increasingly difficult in recent years as employers have an unprecedented arsenal of surveillance mechanisms with which to search digital footprints employees leave behind in cyberspace. To evaluate the allowable contour of employer surveillance, this article engaged in a fundamental analysis of the linkage between individual behavior in social media and expectation of privacy at workplace and made a set of observations.

First, digital immersion with social media exuberance has given rise to pervasive online communication between strangers now labeled as friends in

Kichline, Pitfall Potential: The Risk of Social Media, 18- SEP NEV. LAW. 16, 17 (2010) (observing that employer may find itself liable for failure to take remedial action when one of its employee engages in harassing behavior towards a fellow employee by using social media during work hours or using company issued machines) (emphasis omitted).
cyberspace. Often times, this will result in sharing intimate details to virtual stranger friends in a shared many-to-many exchange. In the process, this erodes an individual’s privacy interest. As this privacy interest is transferred into an employer-employee relationship, such individual brings in the emerging behavioral norm of social media. In the process, such individual inherits an attenuated expectation of privacy.

Second, the scope of an employer’s surveillance must be balanced with the targeted employee’s subjective expectation of privacy, for which constitutional jurisprudence should provide the guiding principle. Revisiting Justice Harlan’s two-prong test of privacy, this article contextualized individual privacy as a function of society’s technology mediated behavior. Thus, the legality of an employer’s surveillance should be analyzed as a function of both the employer’s legitimate business interest and the affected employee’s expectation of privacy as measured through the lens of the broader society’s expectation.

Third, seamless communication across multiple platforms with multiple individuals with superior access and speed has lowered the threshold of individual privacy. However, residing within each individual is an ability to self-determine the individual contour of sharing. This in turn must shape an individual’s expectation of privacy in society, which can be used as objective indicia of an individual’s expectation of workplace privacy. Employer surveillance must not be able to jeopardize such expectation. Yet, such expectation must be objectively indexed based on the new reality of an über-connected social landscape.

Finally, driven by social media exuberance, an emerging behavioral norm is taking root within contemporary society. This norm must be recognized as a driver for shrinking contours of individual privacy. Within this new reality, employer surveillance is a predicated response to an all-pervasive digital immersion into social media.
CHANGING DYNAMICS OF EMPLOYER-EMPLOYEE RELATIONSHIP AND THE TECHNOLOGY INTERFACE: A CRITICAL ANALYSIS

Tania Sebastian*

Abstract: There has been a significant deal of attention given to the general role of technology, its impact on society, and laws relating to technology. However, the role of employment law and contracts in the context of technology has created many changes in human capital mobility. Although technology is intertwined and of great importance in the lives of almost every employee and employer, organization, institution, etc., the interplay between technology and labor and employment law is a relatively new and understudied field. This paper addresses the ability of current law to address some of the challenges raised by the shift towards the “knowledge economy” and the argument that employment law doctrines should incorporate some protections regarding the ability of employees to exchange information regarding their terms and conditions of employment, both inside and outside their organizations.

I. INTRODUCTION

In today’s technologically permeated society, intellectual property and its associated rights undoubtedly play a pivotal role. As just one example, as a result of the burgeoning intellectual property era, there has been a paradigm shift in the employer-employee relationship concerning information sharing, particularly with respect to employability in rival organizations. Thus, it is of great importance to understand the drastic changes in the relationships between employers and employees over the past couple of decades.

In the 1980’s, the employee would look for a long-term commitment with the employer; in fact, some employees would remain at one job for a lifetime. However, this practice has seen a drastic shift in the last ten years, with employees staying with an employer for a short period of time before moving to another employer offering a promotion. This changing dynamic coupled with the “information” revolution is the tip of the iceberg for a vast transformation. As the shift from the manufacturing economy to the knowledge economy gains momentum, with the tentacles of change being seen in not just the developed

* Assistant Professor of Law, Gujarat National Law University, Gandhinagar, India.
1. Other interchangeable terms include: technological revolution, electronic revolution, digital revolution, etc.
nations but the developing nations as well, we are heading towards what one commentator has correctly described as a “boundaryless” workplace. Perhaps the single most important factor in the changes occurring during this new era in the workplace is the increasing use of technology and the changes technology use creates.

II. CARDINAL ROLE OF TECHNOLOGY

It is now beyond doubt that information and its ancillaries hold center stage. As a natural consequence to the changes in modern economies, the importance of intellectual capital has increased. The dependence has steadily increased on information and knowledge to perform work, and more people than ever before make a living buying and selling information, rather than material commodities. The application of technology to the employer-employee relationship has culminated in improved communication and information processing technology, having a striking effect on the contours of that relationship. As one observer has noted, “the twenty-first century economy is one of ever-increasing information intensity . . . knowledge has become what we buy, sell and do . . . . It is the most important part of production . . . . Knowledge assets have become more important to companies than financial and physical assets.” Consequently, employers go to great lengths (litigation and otherwise) to restrict employees from divulging what they learn at work to business rivals.

The convergence of these dramatic changes spaced over the last couple of decades has created a need to address the resulting dilemmas of employees. Even more, it has created a need for re-examining labor and employment law and policy as employers vigorously protect IP developed by employees. For example, seeking to protect proprietary information, it is not uncommon for employers to conduct exhaustive exit interviews and force employees to sign non-disclosure agreements. This is because the transition into a Knowledge Economy has created a premium on the value of information, and a corresponding emphasis on the ability of employers and employees to communicate outside as well as within the work environment. This premium value placed on information is just as likely to affect the rights of employees and employers during the employment relationship as their rights after the employment relationship ends. Because knowledge plays such a decisive role, there is a paradoxical result in this knowledge economy: Employees are subject

to a myriad of restrictions regarding their ability to communicate, and, to restrictions regarding information exchange via technology.4

III. CRYSTALLIZING THE DEBATES

The viewpoint of conceptualizing information and knowledge in terms of real estate (property in the strict sense), and thereby to guarantee and grant the rights associated with it, inclusive of putting up fences, evicting trespassers, etc., comes at a conflict with the true spirit of the very concept and purpose of intellectual property. Specifically, when applied to the employees’ knowledge, it takes the form of exploiting the employees’ creations and preventing former employees from working for competitors, because the former employers think these employees could damage the value of the employers’ intellectual property. The question then becomes whether employers’ rights in certain “proprietary information” entitles them to restrict the freedom of former employees to work elsewhere; the result being the disentitlement of the employees from taking any job that will require them to use or disclose knowledge that the employer unilaterally deems proprietary.5

Undoubtedly, the importance of intellectual capital has increased with the acceleration in changes to the industrial and post-industrial economies. Even more of an increase is displayed in the over-dependence on information and knowledge in arenas of work. Consequently, more and more people than ever before make a living buying and selling information as opposed to material goods.6 Put another way, knowledge as power has become a component of economic activity. In the first instance, knowledge has certainly become an important component of modern production processes. However, perhaps more importantly, knowledge has also become the product itself, rather than simply the means of production. The shift from knowledge as a component of production to the product itself has changed the relationship between capital and labor. Knowledge and technology were considered to be external or secondary aspects of the production process, and thus, not directly related to the processes; criterions which have now undergone an enormous shift. Knowledge and technology are now seen as important and inseparable components in the

5. Catherine Fisk, Knowledge Work: New Metaphors For The New Economy, 80 CHI-KENT L. REV. 839, 846 (2005). See also PepsiCo Inc. v. Redmond, 54 F.3d 1262, 1272 (7th Cir. 1995) (affirming an injunction against a marketing employee working for a competing soft drink company because he knew too much about his former employer’s marketing strategy and inevitably would bring that knowledge to bear in his next employment).
production process. These two factors, today more than ever before, have the capability of increasing the productive capacity of the other production factors. And more importantly, knowledge (as against labor and capital) can “grow rather than diminish with use,” which in turn allows for the possibility of sustained competitive advantages to an extent never before seen. Additionally, not only has knowledge become a key factor of production, it has also become more important as a product.7

IV. THE INTELLECTUAL PROPERTY LOCKSMITHS: STEALING FROM THE MIND

Given the shift from knowledge as a means of production to product in its own right, it is important to consider the role of technology. As employees move between employers, the issue of “knowledge acquired through employment” arises. For example, consider the data stored and worked upon by former employees – to whom does it now belong? The employees who developed it or the employers under whom the employees developed it, given suitable working conditions and accommodative infrastructure? These questions exist in all establishments and in different forms of employee-employer relationships. With the spread of technology, these questions have only increased manifold as technology has essentially allowed the transfer of data instantly. As a result, technology plays a central role in the new employer-employee relationship.

The winds of change have already affected the workplace and as a result the previously established relationships have undergone drastic changes. While the changes are no longer in debate, what necessarily constitutes the debate is how these changes have affected employees’ employment mobility and the far-reaching concerns that employers face with respect to “their” intellectual property.

V. ARENAS OF CONCERN

Traditionally, intellectual property rights in the employment arena were governed by common law doctrines, statutory law, and contractual arrangements. However, over the past few decades, employers have increasingly demanded control over intellectual property rights during post-employment activity. This control has impacted the flow of information in the marketplace due to employers frequently demanding that employees sign covenants not-to-compete and agreements to assign inventions to the company. Thus arises an obvious

conflict between innovation and dissemination of knowledge, with the resulting dilution of the dual aim of law to encourage both.8

In such an era, the implications of the transition towards a knowledge economy on the rights of employees to exchange information about their jobs is the pertinent area for consideration. The dynamics of the knowledge economy demand a better appreciation of the importance of information exchanges in the workplace. This greater appreciation requires that legal rules be made clear and strengthened regarding the dissemination of information without strings at the workplace.

Employment law doctrines should incorporate some minimum protections regarding the ability of employees to exchange information regarding their terms and conditions of employment, both within and outside their organizations. The foundation of the new contract should be on lifetime learning. For example, employers should be expected to provide employees with the opportunity to learn multiple aspects of any job. Employees, on the other hand, cannot expect lifetime employment, but instead should expect to change jobs many times during their working lives. In this new contract, employees are more strongly attached to their “careers” or “professions” than to any one employer.

The focus of the new contract therefore should be employee mobility, where employees move quickly from one place of employment to the other, termed, appropriately as the “new psychological contract,”9 as opposed to the “old psychological contract.” The old psychological contract had the loyalty element, where employees stayed for nearly an entire lifetime with one employer, before retiring with a gold watch, which was a symbolic gesture by firms to the employees for lifetime spent with them. The new psychological contract, however, reflects a new set of expectations by employees by not anticipating long term jobs, or job security, or even continuous promotion.

Another interlinked aspect of the new psychological contract is that of the boundaryless career. In essence, a boundaryless career is created when employees frequently move laterally among employers so as to join in a higher capacity, thereby increasing mobility and not following the traditional notions of advancement within a single hierarchical organization. Factors increasing the gradual spread of such boundaryless careers include outsourcing and joint ventures.

Three important works analyzing this seismic shift are by Professors Heckscher, Stone, and Drucker. Prof. Heckscher has documented the advent of the boundaryless career over the century, explaining the growth of post-bureaucratic organizational forms, by stating, and correctly so, that in today’s

8. See Stone, supra note 2, at 748.
organizations, there is no expectation that employees will spend their entire careers in one organization. 10 Drucker has pointed to a historical shift throughout the twentieth century in career patterns, where most adults, though still engaged in large organizations as before, are nevertheless increasingly not employees of that organization, but rather contractors, part-timers, or temporary workers. He has predicted that there may soon come a time when even a sizeable minority of managers and professionals will not be employees of the firms with whom they do business. The concept of a boundaryless career, like that of the new psychological contract, reflects the shift in job structures away from internal labor markets. Instead of job ladders along which employees advance within stable, long-term employment settings, there are possibilities for lateral mobility between and within firms, with no set path, no established expectations, and no tacit promises of job security. As Drucker has stated, “there is no such thing as lifetime employment anymore . . . ” 11 Professor Stone has further explained and crystallized these arguments. 12 Also, it has to be remembered that the old psychological contract is no longer dominant, but the new psychological contract is yet to be defined and that it has not emerged in all the workplaces and on all the continents.

However, what has to be considered is the juxtaposition between sharing confidential information when one moves from one company to another, and the mechanisms through which the law can affect people’s behavior by curbing the natural desire to use information gained to improve his or her own position. 13 Interwoven developments in production, technology, and globalization have changed the nature of labor and employment relations, particularly in the context of employment-based intellectual property. 14 In particular, the laws regulating the ability of employees to own and share information about their jobs are based on the assumptions underlying last century’s industrial economy. A disconnect thus has developed between the legal regime and the actual operation of labor markets, making our employment laws ineffective in handling the demands created by the shift towards the knowledge economy.

In this era of globalization and information technology, the aspects of how we work and its related ancillaries are undergoing a drastic change. Scholars have correctly noted that the issue of this transition towards a knowledge

---

12. See Stone, supra note 9, at 541. See also Gely & Bierman, supra note 4, at 653.
economy and the implications that it has in resolving the inherent conflict between employers and employees, has gone almost totally unnoticed by courts, legislatures, and legal scholars alike. Scholars have noted the disconnect between the legal regime and the actual conduct of labor in its workplace, creating loops and holes in the prevailing employment laws in relation to the “knowledge economy.”

The most immediate effect concerns trade secrets, which can be easily disseminated, shared, and distributed through the use of technology. When this ease of dissemination is paired with the rise in employee mobility, concerns arise about the knowledge that former employees take with them to new workplaces, and the hypocritical attitude of former employers in asserting ownership over this retained knowledge.15

Although lifetime employment is no longer part of the employment “contract,” it has been replaced by the implicit promise of training and the acquisition of technical skills. However, a natural consequence of this trade-off is a dispute concerning who owns the technical knowledge that an employee acquires on the job: the employees or the employers. Employers attract employees with the promise of facilitating opportunities for acquiring skills and knowledge with the understanding that even though employment is temporary, employees will be able to market themselves to other employers by using the technical knowledge gained on the job. This balance ensures that employees accept the fact that their employment may not last forever (or even for a long time), and in exchange they obtain valuable knowledge and skills, which they assume will be portable when the current employment relationship ends. However, when employers later seek enforcement of a covenant or the invocation of trade secret protection, they violate the terms of this tacit agreement by denying former employees the promised benefit – the portable use of the specialized training and knowledge. Based on this model, Prof. Stone suggests that courts should refuse to enforce covenants or to invoke the trade secrets doctrine because such restraints violate the terms of what she views as an implied employment contract. Professor Eileen Silverstein advances an alternative theory for why courts should not enforce covenants in the employment context: the workers themselves should be the owners of their own

15. David Greene, Trade Secrets, the First Amendment and the Challenges of the Internet Age, 23 HASTINGS COMM. & ENT. L.J. 537, 556 (2001). See also Ford Motor Co. v. Lane, 67 F. Supp. 2d 745, 750 (E.D. Mich. 1999), in which the argument was that the defendant obtained the trade secrets from Ford employees and that there was a violation of the confidentiality agreements that was part of the employment contracts. Ford sought a preliminary injunction prohibiting the defendant from disclosing any of its internal documents. The district court held that, under these facts, the Michigan Act’s “authorization of an injunction violates the prior restraint doctrine and the First Amendment.” The court rejected the argument that trade secrets should be judged against different standards than the information that was the subject of the seminal prior restraint cases.
human capital for the simple reason that laborers have a moral claim to the fruits of their own labor.

VI. CONCLUSION

Employers no longer implicitly promise employees long-term employment, but rather promise to provide training and networking opportunities that will enable employees to develop skills they can use elsewhere in the labor market and also, in return, seek to control how that knowledge is used. Employers increasingly seek to impose restraints on employees’ mobility either by enforcing covenants not to compete or by bringing trade secret actions. However, when employers gain by the development of employees’ human capital and social networks, employers should not restrain employees from using these skills and assets for the employees’ future benefit.16

Additionally, the exchange of information and sharing on-the-job skills is an essential component of the “new psychological contract” between employers and employees, which in turn enhances employees’ career-building and job mobility. Attempts to limit the ability of employees to exchange information after employment ends will no doubt frustrate the expectations employees have under the new psychological contract. Thus, employment law doctrines should reflect this understanding by prohibiting restrictions on the ability of employees to exchange information both inside and outside the organization regarding their terms and conditions of employment.

PROTECTING PRIVACY OF MEDICAL RECORDS OF EMPLOYEES AND JOB APPLICANTS IN THE DIGITAL ERA UNDER THE AMERICANS WITH DISABILITIES ACT

Michael L. Tudor

I. INTRODUCTION

The familiar sight of folders filling rows of shelves or file cabinets in medical offices and hospitals is quickly disappearing.\(^1\) It will not be quite so funny to see Chevy Chase in Fletch standing in front of a computer terminal in the records room of a hospital asking, “Do you have the Beatles’ White Album?”\(^2\) The federal government and health care advocates promote health information technology (HIT) and electronic health record (EHR) systems to improve efficiency, reduce medical errors, and save costs.\(^3\) The Health Information Technology for Economic and Clinical Health (HITECH) Act, as part of the American Recovery and Reinvestment Act of 2009 (ARRA), provided 25.9 billion dollars in incentive payments to medical professionals and hospitals to promote and expand the use of certified EHR technology.\(^4\) Congress set the goal of computerizing all U.S. patient health records by 2014.\(^5\) According to a 2011 survey, 55% of physicians use an electronic record system with another 25% planning to use one within the next year.\(^6\)

Electronic medical records (EMRs) are patient files stored in computer format rather than hard files by individual healthcare providers.\(^7\) Electronic health record (EHR) systems aggregate a patient’s electronic medical records across multiple providers\(^8\) and are more comprehensive than the typical paper

\(^{*}\) J.D. candidate 2014 at the Salmon P. Chase College of Law at Northern Kentucky University.
2. FLETCH (Universal Pictures 1985).
3. Hoffman & Podgurski, supra note 1, at 104-06.
8. Id.
file\(^9\) because they collate a patient’s entire health history and often include information management tools.\(^{10}\) These systems collect and manage everything from patient demographics to laboratory test results to lists of patient allergies and medications to medical diagnoses and providers’ notes all in one place.\(^{11}\) EHR systems can also collect information from personal health records (PHRs), which patients manage and enter data into themselves.\(^{12}\) A PHR is a particular form of EHR “that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.”\(^{13}\)

With the move to electronic record keeping, employers now obtain and process electronic medical records for many reasons, including fitness for duty exams, workers’ compensation claims, reasonable accommodation requests by individuals with disabilities, Family Medical Leave Act (FMLA) requests, and processing insurance claims.\(^{14}\) Computerization of records creates new types of security vulnerabilities that come with additional possibilities of privacy breaches of employee records and litigation for employers.\(^{15}\) The increased use of electronic records has made it easier for employers to access a wider range of an employee’s medical records.\(^{16}\) Employers might ask or require workers to sign release authorizations that allow them access to their entire EHR or PHR.\(^{17}\) The often-voluminous nature of electronic records “may make the handling of medical data far more cumbersome and complicated for employers” and has raised workers’ concerns that employers can more easily access their personal health details.\(^{18}\)

Additional concerns arise because some employers maintain their own electronic health record systems. A number of large employers including Applied Materials, AT&T, BP America, Inc., Cardinal Health, Intel, Pitney Bowes, sanofi aventis, and Wal-Mart have formed a PHR system named Dossia.\(^{19}\) Dossia’s database is available to individuals for life, even if they

---

10. Hoffman & Podgurski, supra note 1, at 104 n.1 (citing EDWARD H. SHORTLIFFE & JAMES J. CIMINO, BIOMEDICAL INFORMATICS: COMPUTER APPLICATIONS IN HEALTH CARE AND BIOMEDICINE 937 (3d ed. 2006)).
11. Id. at 108.
12. Id. at 110-11.
15. Id. at 410.
16. Id. at 421-22.
17. Id. at 413.
18. Id. at 410.
change employers. Although Dossia represents that no one will have access to the information without explicit consent from the user, employees remain concerned that health information stored on employer-provided PHRs may not be fully protected.

Despite these growing concerns regarding the privacy of medical records, Congress has not implemented a comprehensive scheme concerning the use of medical records in the employment context. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) contains strong protections of medical records, but applies only to “covered entities” such as medical providers and insurers. Although Congress extended HIPAA to covered entities’ business associates, these rules apply to employers only to the extent that they operate as health insurers. The Genetic Information Non-Discrimination Act of 2008 (GINA) covers employers but is limited to genetic information. The Americans with Disabilities Act (ADA) has broad privacy provisions that aim to protect the medical records of job applicants and employees. However, the courts remain split about whether these provisions apply to all employees and applicants and have erected substantial barriers to broad enforcement of these provisions.

The commentaries are divided like the courts concerning whether the ADA protects the medical privacy of all employees and job applicants or only qualified individuals with disabilities, leaving millions of American workers vulnerable to violation of their private medical information by their potential and present employers without redress. This article updates the existing literature

20. Id.
22. See infra Section II.A.
24. See infra Section II.B.
25. See infra Section II.C.
26. See id.
27. Compare Natalie R. Azinger, Comment, Too Healthy to Sue Under the ADA? The Controversy over Pre-Offer Medical Inquiries and Tests, 25 J. CORP. L. 193, 208 (1999) (arguing that the broader viewpoint, “in which nondisabled plaintiffs are allowed to sue, will effectuate a greater deterrent for employers to not violate section 12112(d), thereby reducing discriminatory hiring practices”), with Allyson R. Behm, Note and Comment, The Americans with (or Without) Disabilities Act: Pre-Employment Medical Inquiries and the Non-Disabled, 26 AM. J.L. & MED. 439, 452 (2000) (arguing that non-disabled individuals should not be permitted to pursue a discrimination claim under section 12112(d)(2)(A) of the Americans with Disabilities Act), and William D. Wickard, Comment, The New Americans Without A Disability Act: The Surprisingly Successful Plight of the Non-Disabled Plaintiff Under the ADA, 61 U. PIT. L. REV. 1023, 1052 (2000) (arguing that the text of the ADA does not authorize enforcement by individuals who do not have disabilities but the purpose of the ADA is only enforcement “on behalf of individuals with disabilities”). See also Michelle A. Travis, Lashing Back at the ADA Backlash: How the Americans
to address the current circuit split regarding the applicability of the ADA privacy provisions to non-disabled individuals with consideration to the growing use of electronic records and the impact of the ADA Amendments Act of 2008 (ADAA). Part II of this article describes the current laws concerning privacy of medical and employment records and discusses how they fall short of providing comprehensive coverage for American workers. Part III explains the current circuit split concerning whether non-disabled individuals have standing to make claims under the ADA privacy provisions. Part IV argues that non-disabled individuals should be allowed to make claims under the privacy provision of the ADA because (1) the majority of courts considering the issue have adopted this position, (2) it is consistent with the intention for broad applicability of the ADA, (3) it follows the guidance of the EEOC, and (4) it better protects confidential medical records of employers in the digital era.

II. CURRENT LAW DOES NOT PROVIDE COMPREHENSIVE PROTECTION OF MEDICAL RECORDS FOR AMERICAN WORKERS

No one set of laws or regulations govern the privacy of medical information in the employment context. The laws and regulations that do govern personal health information were developed for various and sometimes conflicting purposes. This section will discuss the various medical privacy laws and regulations and their shortcomings as applied to privacy of medical information in the employment context with emphasis on digital record keeping.

A. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA regulations govern disclosure of medical information by healthcare providers to third parties, including employers.28 Although HIPAA with its Privacy and Security Rules contains “the most comprehensive medical privacy regime” for confidential medical information that Congress has ever passed, it does not regulate employers “except with respect to their group health insurance plans and any on-site health clinics they may maintain.”29 In fact, the U.S. Department of Health and Human Services (HHS), which enforces HIPAA, “has no authority over employers.”30

30. Id.
HHS issued the HIPAA Privacy Rule and the HIPAA Security Rule in 2002 to require covered entities to have safeguards for protected health information (PHI). The HITECH Act of 2009 amended HIPAA to ensure it would cover EHRs and afforded HHS the opportunity to issue updated guidance regarding the security of electronic PHI.\(^3^1\) HHS published the final rule on January 25, 2013 with an effective date of March 26, 2013 and requiring compliance by September 23, 2013.\(^3^2\) HIPAA defines PHI as “individually identifiable health information” that is electronically or otherwise transmitted or maintained by a covered entity.\(^3^3\) Covered entities include health plans, health care clearinghouses, and health care providers who transmit health information electronically for particular purposes, generally claim or benefits activities.\(^3^4\) Although the HITECH Act amended HIPAA to extend its enforcement mechanisms to covered entities’ business associates and their subcontractors,\(^3^5\) the rules apply to employers only to the extent that they operate as business associates of covered entities or health insurers on behalf of their own employees.\(^3^6\) The rule specifically excludes “employment records held by a covered entity in its role as employer” from the definition of PHI.\(^3^7\)

The HIPAA Privacy Rule prohibits covered entities from utilizing and disseminating PHI without the patient’s consent.\(^3^8\) The rule requires covered entities to “make reasonable efforts to limit” the release of PHI “to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.”\(^3^9\) However, the comprehensive nature of EHRs makes it difficult for health record providers to identify the minimum records necessary to satisfy an employer’s request, increasing the risk that the information sent will be overly


\(^3^3\). 45 C.F.R. § 160.103 (2013).

\(^3^4\). Id.


\(^3^7\). 45 C.F.R. § 160.103 (2013).

\(^3^8\). See generally id. at §§ 164.502, .512.

\(^3^9\). Id. at § 164.502(b)(1).
broad and will disclose information the employee would prefer to remain private.40

The HIPAA Security Rule contains provisions to ensure the security of electronically stored health information.41 Covered entities must (1) ensure the “confidentiality, integrity, and availability” of PHI, (2) safeguard against reasonably anticipated security threats to the data, (3) protect against reasonably anticipated prohibited uses and disclosures of the data, and (4) ensure compliance by their workforces.42 The HIPAA Security Rule establishes administrative, physical, and technical safeguards for electronic records, including provisions for measures such as security awareness and training, security incident procedures, sanctions policy for non-compliant employees, log-in monitoring, password management, workstation use, workstation security, device and media controls, facility security, access control and validation, data backup and storage, encryption, decryption, and authentication mechanisms.43 Employers are not required to implement these security measures because they are not covered entities and therefore “may not adequately protect health information that they possess.”44

This is not to say that HIPAA does not affect employers. “The fact that most employers do not qualify as covered entities is irrelevant.”45 Employers enter into “business-associate agreements” with covered entities that require “satisfactory assurances that they will safeguard the confidentiality of the PHI they receive or maintain as if they were covered entities themselves.”46 Although employers that sponsor their own health plans must be HIPAA compliant “as a practical matter,”47 this does not necessarily protect all health information that employers receive or maintain because “the Rule creates a fiction that an employer’s group health plan is an actual living, breathing entity rather than a legal document that governs how the employer provides health benefits.”48 Consequently, The HIPAA Privacy and Security Rules apply to information obtained for use by the group health plan but do not cover the employer obtains for other reasons; the ADA covers medical records obtained or

40. Hoffman, supra note 14, at 419.
41. 45 C.F.R. § 164.306(a) (2013).
42. Id.
43. Id. at §§ 164.308(a), .310, 312. For a critique of the HIPAA Security Rule, see Hoffman & Podgurski, supra note 1, at 338-44.
44. Hoffman, supra note 14, at 420.
47. Powell & Bales, supra note 45, at 150.
maintained for other reasons. For example, if an employer’s human resources manager obtains a psychiatric evaluation a part of a fitness for duty exam, HIPAA does not cover the confidentiality of that document once it leaves the office of the psychiatrist. However, if the employee or the psychiatrist seeks reimbursement from the health plan, HIPAA would govern any information obtained during that process. Thus, the manager of the health plan could not share any information additional information obtained with the human resources manager. Therefore, HIPAA requires “adequate separation between the group health plan and the plan sponsor.”

Because the rules distinguish between the employer as an entity that sponsors a health plan (which is not subject to HIPAA) and the entity of health plan itself (which is), the HIPAA privacy regulations instruct that the health plan may disclose PHI to the employer only if the employer certifies the amendment of the plan documents as required. The rules prohibit the health plan from the using or disclosing PHI “for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor.” The employer must report any prohibited use of PHI to the plan and must “return or destroy” PHI after a permitted use is completed. The rules require the plan documents to define which employees will have access to PHI, restrict their access to permitted use, and require an “effective mechanism for resolving any issues of noncompliance” by such persons. Finally, the rules restrict access of PHI to “plan administrative functions.”

The HITECH Act added breach notification provisions to HIPAA to require covered entities and their business associates “to provide notification to affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured protected health information.”

49. Id.
50. Id.
51. Id. at 461-62.
52. Id.
54. 45 C.F.R. § 164.504(f) (2013).
55. Id.
56. Id.
57. Id.
58. Id.
59. Id.
information.”61 Unauthorized disclosure of PHI from the health plan to the employer would constitute a breach requiring notification to affected individuals.62 This could consist of something as simple as leaving the keys to the filing cabinet containing employee health records to storing protected health information in a computer system with inadequate password protection to accidentally blast emailing a list of all employees who take Prozac to the entire company. However, HIPAA would not apply to this same information if the employer obtained and maintained it as part of the employee’s occupational health file.63 These rules can be confusing to employers because they may not know whether they obtained medical information as the plan sponsor or the health plan.64

Even if HIPAA was to cover all health information obtained and maintained by employers, however, its enforcement mechanisms are inadequate for many individual cases because they only allow the Secretary of the HHS to impose civil penalties65 or criminal penalties for those who “knowingly” obtain or disclose protected information.66 HIPAA does not create a private right of action.67 Private actions are available only under GINA, the ADA, or state law.

B. The Genetic Information Non-Discrimination Act of 2008 (GINA)

Title II of the Genetic Information Non-Discrimination Act of 2008 (GINA) includes a confidentiality provision that requires employers to maintain any lawfully obtained genetic information on separate forms and in a confidential medical file in accordance with similar provisions in the ADA.68 Congress enacted GINA as an amendment to Title VII of the Civil Rights Act of 1964 to establish that it is unlawful for employers to discharge, refuse to hire, or make employment decisions relating to compensation or the terms and privileges of employment based on an employee’s genetic information.69 Although GINA

61. Id.
62. See id.
63. SUMMARY OF THE HIPAA PRIVACY RULE, supra note 36, at 4 (“The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer.”).
64. Ardelean, supra note 29, at 461.
67. See, e.g., Acara v. Banks, 470 F.3d 569, 571 (5th Cir. 2006).
68. 42 U.S.C. § 2000ff-5 (2012). GINA was most recently amended “to clarify that genetic information is health information and to prohibit group health plans, health insurance issuers (including HMOs), and issuers of Medicare supplemental policies from using or disclosing genetic information for underwriting purposes.” Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5566-01, 5659 (proposed Jan. 25, 2013) (to be codified at 45 C.F.R pts. 160 & 164).
69. Id. at § 2000ff-1.
prohibits employers from requesting, requiring, or purchasing genetic information about employees or their family members, the increased use of EHRs make it likely that employers will gain access to genetic information. GINA does not provide a comprehensive solution to protection of medical information because it is limited to genetic information and the case law is too sparse to know how the courts will enforce it.

C. The Americans with Disabilities Act (ADA)

The ADA was enacted by Congress and signed into law by President George H. Bush in 1990, in part, “to provide a clear and comprehensive national mandate for the elimination of discrimination against individuals with disabilities.” Prior to the enactment of the ADA, individuals with disabilities were only able to obtain legal redress from discrimination they experienced in the federal arena. Congress, in enacting the ADA, recognized the realm of employment as one significant area of discrimination. The employment provisions are set forth in the first section of the ADA and are a major source of ADA litigation.

1. Overview of The ADA

The intent of the ADA is to “assure equality of opportunity, full participation, independent living, and economic self-sufficiency” for individuals with disabilities. The Act has four titles. The first three titles focus on the major areas in which individuals with disabilities have historically experienced discrimination: employment, public services and public accommodations. The final title incorporates miscellaneous provisions.
The ADA defines “disability” with respect to an individual in three ways: (1) “a physical or mental impairment that substantially limits one or more major life activities of such individual;” (2) “a record of such an impairment; or” (3) “being regarded as having such an impairment.”84 A person must meet only one of these definitions to be considered “disabled.”85 On September 25, 2008, President George W. Bush signed into law the ADA Amendments Act of 2008 (ADAAA),86 which broadened the definition of “disability” by expanding the list of “major life activities.”87

Title I of the ADA covers discrimination against disabled persons in employment.88 Title I prohibits employers from discriminating against a person because of disability in all aspects of employment, including the application and hiring process, provision of reasonable accommodations, and wages and benefits.89 Title I of the ADA applies to private employers with 15 or more employees.90 The ADA does not apply to the federal sector.91

Title II of the ADA concerns discrimination in the administration of public services.92 Title II prohibits the denial of public services to individuals with disabilities and assures that individuals with disabilities can participate in all public programs in the same way as non-disabled individuals.93 Title II also requires that individuals with disabilities must have full access to public transportation systems,94 including those operated by local government instrumentalities and commuter authorities.95

Title III of the ADA describes public accommodation regulations.96 Title III requires that public facilities must remove existing obstacles to the servicing of the individuals with disabilities97 and all new building construction and modifications to be accessible.98 For purposes of Title III, public facilities include restaurants, hotels, retail stores, and privately owned transportation systems.99

84. Id. at § 12102.
85. Behm, supra note 27, at 441.
89. See id. at § 12112.
90. See id. at § 12111(5)(A).
91. See id. at § 12111(5)(B).
92. See id. §§ 12131-12165.
93. See id. at § 12132.
95. See id. at § 12131.
96. See id. §§ 12181-12189.
97. Id. at § 12182(b)(1)(A).
98. Id. at § 12183.
Finally, Title IV of the ADA sets forth miscellaneous provisions. Title IV’s provisions include that states shall not be immune from the ADA under the eleventh amendment to the Constitution, a prohibition against retaliation and coercion against persons bringing a claim under the ADA, the recovery of attorney’s fees to the prevailing party in an ADA claim, and a prohibition on categorizing illegal drug use as a disability.

2. The ADA’s Privacy Provisions

The ADA seeks to prevent discrimination against individuals with disabilities in employment by protecting an applicant’s or an employee’s medical privacy. The ADA does this by limiting employer access to medical information and limiting the disclosure of medical records by employers. The ADA limits employer access to medical records in three ways. First, the ADA limits the examination or inquiry of a job applicant as to whether such applicant is an individual with a disability or as to the nature or severity of such disability until after an employment offer. Second, employers cannot make any medical inquiries or require any medical examinations of employees unless they are “job-related and consistent with business necessity.” Finally, the ADA contains a medical confidentiality provision, which limits the disclosure of medical information by employers and requires employers to keep employee medical records separate from the employee’s personnel file.

By limiting disability inquiries and medical exams until after and employer has extended an employment offer, Congress aimed to curtail all questioning that would serve to identify and exclude persons with disabilities from consideration for employment. However, the ADA “imposes no restriction on scope of entrance exams; it only guarantees the confidentiality of information gathered… and restricts the use to which an employer may put the

100. Id. §§ 12201-12213.
102. Id. at § 12203.
103. Id. at § 12205.
104. Id. at § 12210.
105. Ardelean, supra note 29, at 459.
107. See id. at § 12112(d).
108. Id.
109. Id.
110. Id.
111. Id.
Cases involving violations of this provision of the ADA tend to fall under one of two categories: overbroad pre-offer inquiries that go beyond business necessity or use of information obtained in post-offer inquiries to discriminate against the applicant.

The ADA prohibits an employer from making medical inquiries or requiring any medical examinations of employees unless they are “job-related and consistent with business necessity.” Unlike the unlimited scope of information that employers may request during inquiries of applicants who have been extended an employment offer, inquiries of current employees are strictly limited to business purpose. Therefore, an employer is precluded under the ADA from requiring medical examination of an employee where the employer has knowledge of employee’s health condition but has no other indicators that employee cannot perform job. Cases illustrating violations of this provision tend to involve inquiries that go beyond the employee’s ability to perform the

---

114. See, e.g., Barnes v. Cochran, 944 F. Supp. 897, 904-05 (S.D. Fla. 1996), aff’d sub nom. Barnes v. Broward Cnty Sheriff's, 130 F.3d 443 (11th Cir. 1997) (holding that pre-employment medical exam violated ADA because it covered a wide range of incidents and probed areas tending to disclose specific psychological disabilities); but see Murray v. John D. Archbold Mem'l Hosp. Inc., 50 F. Supp. 2d 1368, 1375-78 (M.D. Ga. 1999) (inquiring about a job applicant’s characteristics such as height and weight is not prohibited by the ADA); Cannizzaro v. Neiman Marcus, Inc., 979 F. Supp. 465, 477 (N.D. Tex. 1997) (interviewer’s discussion of employee’s subdural hematoma and comment that he would not hire her for sales coordinator position “for her sake” because he felt “the job would kill her” was not held to be a violation because the comment concerned “the job” rather than her medical condition); Hoffman v. Fid. Brokerage Servs., Inc., 959 F. Supp. 452, 459 (S.D. Ohio 1997) (employer did not violate ADA by making pre-offer inquiries into whether applicant’s known vision impairment would prevent her from performing customer service representative job that required use of computer system).
115. See, e.g., Connolly v. First Pers. Bank, 623 F. Supp. 2d 928, 931 (N.D. Ill. 2008) (holding that although drug test to determine illicit drug use of a post-offer employee is not a prohibited medical exam by ADA, the exemption for drug testing is “not meant to provide a free peek into a prospective employee’s medical history and could violate ADA if used in this manner); Gillen v. Fallon Ambulance Serv., Inc., 283 F.3d 11, 43 (1st Cir. 2002) (reversing an entry of summary judgment for defendant when preemployment inquiry was possibly pretextual for discrimination); but see Grenier v. Cyanamid Plastics, Inc., 70 F.3d 667, 678 (1st Cir. 1995) (employer did not violate ADA by requiring former employee with a recent known disability applying for reemployment to provide medical certification as to ability to return to work because it is relevant to assessment of ability to perform essential job functions).
117. See id.
job, 119 while cases illustrating non-violations tend to involve necessary inquires of fitness for duty. 120

The ADA’s confidentiality provision permits disclosure of medical information only for three specific reasons. 121 First, it allows disclosure to supervisors and managers regarding necessary restrictions on work duties and any necessary reasonable accommodations. 122 Second, it allows disclosure to first-aid and safety personnel to provide any necessary emergency treatment. 123 And third, it allows disclosure to government officials investigating compliance with the ADA. 124 These protections were designed to provide equal opportunity by aiming to ensure that employment decisions are based on appropriate performance criteria rather than stereotypes regarding the employee’s medical condition 125 and they are grounded in concepts of privacy. 126 Finally, the ADA

119. See, e.g., Kronenberg v. Baker & McKenzie LLP, 747 F. Supp. 2d 983, 990 (N.D. Ill. 2010) (court suggested that the psychotherapist-patient privilege would disappear in ADA cases if the court permitted defendant access to plaintiff’s mental health records so it could explore whether he was able to perform the essential functions of a position as an attorney without reasonable accommodation); Farmilo v. Ford Motor Co., 277 F. Supp. 2d 778, 793-94 (N.D. Ohio 2002) (holding genuine issue of fact whether employer’s requests of wide-ranging mental or physical assessments for retiree desiring to return to work, including disclosure of his entire medical record, violated the ADA); Doe v. Kohn Nast & Graf, P.C., 866 F. Supp. 190, 197 (E.D. Pa. 1994) (holding that search of plaintiff attorney’s office would be an improper medical inquiry where employer discovered letter affirming plaintiff’s Acquired Immune Deficiency Syndrome (AIDS) services and placed it in his personal file).

120. See, e.g., Hennenfent v. Mid Dakota Clinic, P.C., 164 F.3d 419, 422 (8th Cir. 1998) (clinic’s request that physician undergo independent medical examination to determine his level of disability following amputation of his remaining leg did not violate ADA); Conrad v. Bd. of Johnson Cnty. Comm’rs, 237 F. Supp. 2d 1204, 1231 (D. Kan. 2002) (county had legitimate concern about employee’s ability to perform her job as prenatal program manager in health department, as required before county could require employee to undergo psychiatric evaluation under ADA); Johnson v. Eastchester Union Free Sch. Dist., 211 F. Supp. 2d 514, 519 (S.D.N.Y. 2002) (school district’s decision requiring a cleaner to undergo a physical examination was reasonably based because the district was concerned that the cleaner had been experiencing problems with his eyes which impaired his ability to read directions for the use of cleaning supplies, and examination revealed that the cleaner did in fact have a visual impairment); Ketcher v. Wal-Mart Stores, Inc., 122 F. Supp. 2d 747, 754 (S.D. Tex. 2000) (employer was entitled under ADA to require employee working as heavy machinery operator who complained of dizziness to obtain medical examination releasing him to continue in job or listing restrictions as condition of remaining on job); Porter v. U.S. Alumoweld Co., Inc., 125 F.3d 243, 246 (4th Cir. 1997) (employer’s requirement that machine operator, whose job required lifting and pulling and who had encountered problems carrying out his job due to back problems, submit to medical fitness examination as precondition of returning to work after back surgery, was job related and consistent with business necessity and thus did not violate ADA).

122. Id.
123. Id.
124. Id.
125. Id. at § 12101(b).
126. Ardelean, supra note 29, at 459-60.
medical confidentiality provision requires employers to keep employee medical records separate from the employee’s personnel file127 and limits disclosure of medical information to supervisors and managers regarding necessary restrictions on work duties and any necessary reasonable accommodations.128

Cases illustrating violations of the confidentiality provision include unwarranted disclosures to co-workers129 and other third parties such as prospective employers130 or the media.131 Disclosure by a company physician to employer of omissions in employee’s confidential medical record may violate ADA confidentiality provisions if not sufficiently related to a business purpose.132 However, there have been relatively few successful cases under the ADA based on alleged wrongful disclosure of health information.133

Despite the seemingly broad applicability of these provisions, the courts have created several obstacles to claims under this section of the ADA. First, the plaintiff in an ADA medical examination/inquiry case must show more than a mere technical violation of the ADA, but a resulting injury in fact.134 Second, a plaintiff in an ADA disclosure case must demonstrate that the information was

128. Id.
129. Garrison v. Baker Hughes Oilfield Operations, Inc., 287 F.3d 955, 960 (10th Cir. 2002) (affirming jury verdict finding abuse of entrance examination results by giving them to hiring managers rather than qualified medical personnel); and Cossette v. Minnesota Power & Light, 188 F.3d 964, 972 (8th Cir. 1999) (reversing summary judgment of employer’s disclosure of confidential medical information to co-workers); E.E.O.C. v. Ford Motor Credit Co., 531 F. Supp. 2d 930, 943 (M.D. Tenn. 2008) (holding that employer’s disclosure of plaintiff’s HIV status to co-workers causing shame, embarrassment, and depression, satisfied summary judgment burden of “tangible injury” for violation of ADA); Desano v. Blossom S., LLC, 553 F. Supp. 2d 247, 251 (W.D.N.Y. 2008) (holding that employee’s diagnosis of cancer was required to be kept confidential from non-managerial co-workers).
130. Cossette, 188 F.3d at 969 (holding disclosure of back injury and lifting restriction to prospective employer was a case of illegal disclosure of confidential medical information under the ADA).
131. See, e.g., Pouliot v. Town of Fairfield, 184 F.Supp.2d 38, 54 (D. Me. 2002) (finding disclosure to the press that his “condition contributed to the mismanagement of department funds” to be actionable under ADA); Pollard v. City of Northwood, 161 F.Supp.2d 782, 793 (N.D.Ohio 2001) (finding that disclosure to the press that “I didn’t want an officer on Prozac on the police force” constituted a genuine issue of material fact concerning an illegal disclosure of confidential medical information).
134. See, e.g., Tice v. Centre Area Transp. Auth., 247 F.3d 506, 519 (3rd Cir.2001) (finding required injury may be “emotional, pecuniary, or otherwise”); Cossette, 188 F.3d at 970 (finding “some sort of tangible injury” from the testing is required); Armstrong v. Turner Indus. Inc., 141 F.3d 554, 562 (5th Cir.1998) (injury must be “cognizable”). For argument against this approach, see James C. Harrington, Survey Article: Civil Rights, 30 TEX. TECH L. REV. 507, 532-33 (1999).
not voluntarily disclosed. Finally, the circuits are split as to whether any of these privacy provisions apply to non-disabled persons. In response, Congress amended the ADA in attempt to overcome judicial hostility to it.

3. The ADA Amendments Act of 2008 (ADAAA)

The primary purpose of the ADA Amendments Act of 2008 (ADAAA) is to assure a broad scope of protection for people with disabilities and to ensure that the definition of “disability” is “construed broadly in favor of expansive coverage to the maximum extent permitted by the terms of the ADA.” Therefore, the focus of cases brought under the ADA should be “whether covered entities have complied with their obligations and whether discrimination has occurred, not whether the individual meets the definition of disability.”

Following the passage of the ADAAA, lawsuits filed under the ADA have increased significantly. As with other civil rights laws, individuals seeking protection under these anti-discrimination provisions of the ADA generally must allege and prove that they are members of the “protected class.” Under the ADA, this typically means that they must meet the statutory definition of ‘disability.’ However, “Congress did not intend for the threshold question of

135. See, e.g., E.E.O.C. v. C.R. England, Inc., 644 F.3d 1028, 1048 (10th Cir. 2011) (holding that voluntary disclosure of HIV status not protected by ADA); Rohan v. Networks Presentation, LLC., 175 F. Supp. 2d 806, 813-14 (D. Md. 2001) (holding that plaintiff’s voluntary disclosure of her mental impairment to fellow cast members during the “Jekyll & Hyde” tour was not made as part of an employee health program and not protected by the ADA).


138. Id. at § 1630.1(c)(4).

139. Id. at § 1630.1.


141. 29 C.F.R. app. § 1630 (2012).

142. Id. (citing a 2008 House Judiciary Committee Report).
disability to be used as a means of excluding individuals from coverage.\footnote{Id.}

Therefore, “claims of improper disability-related inquiries or medical examinations, improper disclosure of confidential medical information, or retaliation may be brought by \textit{any} applicant or employee, not just individuals with disabilities.”\footnote{Id.} However, courts continue to examine whether these privacy provisions apply to non-disabled persons\footnote{See, e.g., Tamburino v. Old Dominion Freight Lines, Inc., 2012 WL 526426, *6 (D. Or. Feb. 16, 2012); Martino v. Forward Air, Inc., 609 F.3d 1, 4 (1st Cir. 2010) (discussing the circuit split concerning the applicability of the ADA to non-disabled individuals while ruling on similar state provisions).} and continue to reserve the question of whether a person who does not meet the definition of disabled under the ADA has standing to bring a claim under it.\footnote{See, e.g., Bachman v. Donahoe, 460 F. App’x 383, 384 (5th Cir. 2012); Mickens v. Polk Cnty Sch. Bd., 430 F. Supp. 2d 1265, 1277-78 (M.D. Fla. 2006), aff’d, 195 F. App’x 928 (11th Cir. 2006).}  

\subsection*{D. State Laws Concerning Medical Privacy}

One argument against a comprehensive federal scheme of regulation for the protection of medical privacy is that existing state law renders such regulation unnecessary.\footnote{Sharona Hoffman & Andy Podgurski, \textit{In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information}, 48 B.C. L. REV. 331, 359 (2007).} However, as Congress recognized in adopting the HIPAA Privacy Rule, state law is currently inadequate.\footnote{Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462-01 (Dec. 28, 2000) (to be codified at 45 C.F.R pts. 160 & 164).} “Neither private action nor state laws provide a sufficiently comprehensive and rigorous legal structure to allay public concerns, protect the right to privacy, and correct the market failures caused by the absence of privacy protections.”\footnote{Id.} The traditional common law privacy torts are inadequate for protecting personal health information.\footnote{Peter A. Winn, \textit{Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law}, 33 Rutgers L.J. 617, 652-53 (2002).} For example, the tort of public disclosure of private facts is inadequate because it requires “intent” while most medical privacy cases involve “negligence.”\footnote{Id.}

Due to the lack of applicability of the traditional privacy torts, many states recognize a breach of confidentiality tort “designed to address precisely the problem of improper disclosure of sensitive medical information.”\footnote{Id. at 619.} Despite

\begin{thebibliography}{99}
\bibitem{Id} Id.
\bibitem{Id} at n.1 (citing Cossette v. Minn. Power & Light, 188 F.3d 964, 969-70 (8th Cir. 1999); Fredenburg v. Contra Costa Ctty. Dept’ of Health Servs., 172 F.3d 1176, 1182 (9th Cir. 1999); Griffin v. Steeltek, Inc., 160 F.3d 591, 594 (10th Cir.1998), \textit{cert. denied}, 526 U.S. 1065 (1999)) (emphasis added).
\bibitem{Id} at n.1 (citing Cossette v. Minn. Power & Light, 188 F.3d 964, 969-70 (8th Cir. 1999); Fredenburg v. Contra Costa Ctty. Dept’ of Health Servs., 172 F.3d 1176, 1182 (9th Cir. 1999); Griffin v. Steeltek, Inc., 160 F.3d 591, 594 (10th Cir.1998), \textit{cert. denied}, 526 U.S. 1065 (1999)) (emphasis added).
\bibitem{Id} at n.1 (citing Cossette v. Minn. Power & Light, 188 F.3d 964, 969-70 (8th Cir. 1999); Fredenburg v. Contra Costa Ctty. Dept’ of Health Servs., 172 F.3d 1176, 1182 (9th Cir. 1999); Griffin v. Steeltek, Inc., 160 F.3d 591, 594 (10th Cir.1998), \textit{cert. denied}, 526 U.S. 1065 (1999)) (emphasis added).
\bibitem{Id} at n.1 (citing Cossette v. Minn. Power & Light, 188 F.3d 964, 969-70 (8th Cir. 1999); Fredenburg v. Contra Costa Ctty. Dept’ of Health Servs., 172 F.3d 1176, 1182 (9th Cir. 1999); Griffin v. Steeltek, Inc., 160 F.3d 591, 594 (10th Cir.1998), \textit{cert. denied}, 526 U.S. 1065 (1999)) (emphasis added).
\bibitem{Id} at n.1 (citing Cossette v. Minn. Power & Light, 188 F.3d 964, 969-70 (8th Cir. 1999); Fredenburg v. Contra Costa Ctty. Dept’ of Health Servs., 172 F.3d 1176, 1182 (9th Cir. 1999); Griffin v. Steeltek, Inc., 160 F.3d 591, 594 (10th Cir.1998), \textit{cert. denied}, 526 U.S. 1065 (1999)) (emphasis added).
\bibitem{Id} at n.1 (citing Cossette v. Minn. Power & Light, 188 F.3d 964, 969-70 (8th Cir. 1999); Fredenburg v. Contra Costa Ctty. Dept’ of Health Servs., 172 F.3d 1176, 1182 (9th Cir. 1999); Griffin v. Steeltek, Inc., 160 F.3d 591, 594 (10th Cir.1998), \textit{cert. denied}, 526 U.S. 1065 (1999)) (emphasis added).
\end{thebibliography}
“clear modern consensus of the case law” to recognize the breach of confidentiality tort.153 Courts require that the disclosure violate a relationship (such as doctor-patient) established by statutes or ethical rules and therefore do not apply to third parties such as employers that do not inherently owe a duty of confidentiality.154 Even states, such as Ohio, that extend this breach of confidentiality tort to third parties, require that the third party acted intentionally to circumvent patient-doctor confidentiality.155 Therefore, “the breach of confidentiality tort will not apply to disclosures made by employers, data miners, and others who obtained PHI by means other than physician disclosure.”156

Two additional barriers limit the ability of employees to seek private rights of actions against employers for violations of medical privacy. First, the Employee Retirement Income Security Act of 1976 (ERISA) applies to employers that sponsor health or wellness plans preempts state confidentiality standards applicable to invasions of medical privacy but “lacks any equivalent provisions for the protection of patient confidentiality and privacy.”157 Although HIPAA sets such provisions for these employer-sponsored plans,158 HIPAA does not establish a private right of action.159 In addition, many states limit the ability of employees to sue their employers for any injury—mental or physical—that occurs on the job absent an intent to cause such injury through their worker compensation laws.160 Thus, an employee who suffers mental distress due to the unwarranted intrusion into or release of his medical information on the job may

154. Winn, supra note 150, at 661-665.
155. Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 528 (Ohio 1999) (quoting Alberts v. Devine, 479 N.E.2d 113, 120 (1985)). “[A] third party can be held liable for inducing the unauthorized, unprivileged disclosure of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship. ‘To establish liability the plaintiff must prove that: (1) the defendant knew or reasonably should have known of the existence of the physician-patient relationship; (2) the defendant intended to induce the physician to disclose information about the patient or the defendant reasonably should have anticipated that his actions would induce the physician to disclose such information; and (3) the defendant did not reasonably believe that the physician could disclose that information to the defendant without violating the duty of confidentiality that the physician owed the patient.’” Id.
156. Hoffman & Podgurski, supra note 147, at 359.
158. SUMMARY OF THE HIPAA PRIVACY RULE, supra note 36.
159. See, e.g., Acara v. Banks, 470 F.3d 569, 572 (5th Cir. 2006).
160. Erwin S. Barbre, Workmen’s compensation provision as precluding employee's action against employer for fraud, false imprisonment, defamation, or the like, 46 A.L.R.3d 1279 (1972) (stating that “many workmen's compensation statutes contain a provision to the effect that the injured employee's remedy under the workmen's compensation statute shall constitute his exclusive remedy against the employer”). See also STEVEN L. WILLBORN ET AL., EMPLOYMENT LAW: CASES AND MATERIALS 882-907 (5th ed. 2012).
not be able to sue his employer absent a state statute to the contrary or a preemptive federal regulation, such as the ADA. Therefore, the privacy provisions of the ADA and GINA remain the best option at present for assuring that all employers protect the medical privacy of all job applicants and employees. However, the ADA and GINA do not contain any specific provisions regarding the use or storage of electronic records.

E. EEOC Guidance Concerning Electronic Medical Records

The Equal Employment Opportunity Commission (EEOC) issued an informal discussion letter on May 31, 2011, concerning the electronic storage of employee’s medical records by employers.161 The EEOC is the federal enforcement agency for Title I of the ADA and Title II of GINA.162 The letter noted that neither the ADA nor GINA specifically addresses the need for encryption, password authorization, and other security safeguards for electronic records maintained by employers.163 However, the EEOC does not interpret either statute’s confidentiality provisions as applying only to paper records.164 Rather, just like for paper records, the letter advised that the ADA and GINA require that employers who store medical and genetic information electronically must also keep this information separate from personnel files and treat it as a “confidential medical record.”165 The letter concludes: “maintaining personal health information and occupational health information in a single [Electronic Medical Record [EMR]], particularly one that allows someone with access to the EMR to view any information contained therein, presents a real possibility that the ADA, GINA, or both will be violated.”166

Despite this guidance, many employees’ medical information potentially remains vulnerable because some jurisdictions only allow enforcement of the ADA by qualified individuals with disabilities.167 The laws governing the protection of medical records and information are an uncoordinated patchwork of rules and regulations designed for various purposes. Without a comprehensive federal solution, employers will continue to be able to gather unlimited amounts of medical information at the stage of conditional hire and

163. ADA & GINA: CONFIDENTIALITY REQUIREMENTS, supra note 161.
164. Id.
165. Id.
166. Id.
167. See infra Section III.
may not be liable for unwarranted intrusion into or release of that information unless the employee is a qualified individual with a disability.

III. THE CIRCUIT SPLIT REGARDING THE ADA PRIVACY PROVISIONS

Although the ADA limits employer access to medical information and the disclosure of medical records by employers, the statute does not specify the remedies available for violation of its provisions.\(^{168}\) The circuits are split as to whether a job applicant or employee is precluded from stating a prima facie claim under Title I of the ADA by fact that applicant or employee is not disabled or perceived to be disabled.\(^{169}\) There is no generally accepted rule of law with regard to whether a non-disabled individual may bring a claim for a violation of the ADA.\(^{170}\) Two different interpretations have prevailed in the courts that have considered the question of who may bring a claim for a 42 U.S.C. § 12112(d) privacy provision violation. The “All Applicants and Employees Approach” allows any individual who has been subjected to a violation of the provisions of the ADA to bring an action under the statute.\(^{171}\) The “Qualified Individuals with a Disability Approach” requires that only individuals with disabilities may bring claims under 42 U.S.C. § 12112(d).\(^ {172}\)

A. The All Applicants and Employees Approach

Consistent with the approach that the EEOC advocates, the majority of courts have concluded that 42 U.S.C. § 12112(d) allows claims by non-disabled

---

171. Griffin, 160 F.3d at 595; Roe, 124 F.3d at 1229; Cossette, 188 F.3d at 964; Fredenburg, 172 F.3d at 1182; Harrison, 593 F.3d at 1214; Lee, 636 F.3d at 252; Karraker, 239 F. Supp. 2d at 834 (holding that non-disabled individual has standing to assert claim).
172. Turner Inc., 141 F.3d at 561 (deferring question of applicability of ADA to non-disabled individuals and holding that non-disabled plaintiff did not have “cognizable injury” and did not have claim under ADA); Hunter, 139 F.3d 901 at *13-14 (7th Cir. 1998) (holding that ADA does not apply to non-disabled individuals); Turner Ltd., 950 F. Supp. at 167.
individuals. These courts offer several reasons in support of this holding. First, the statutory language refers to “applicants” and “employees” in this section of the ADA rather than “qualified individual with a disability.” Second, public policy favors a broad application of the ADA to further its purpose of eliminating discrimination of persons with disabilities because “allowing non-disabled who are injured thereby to sue will enhance and enforce the blanket prohibition drafted by Congress.” Third, the courts assert that holding otherwise would “obliterate” much of the statute’s usefulness because it “makes little sense to require an employee to demonstrate that he has a disability to prevent his employer from inquiring as to whether or not he has a disability.” The seminal case for the “All Applicants and Employees Approach” is Griffin v. Steeltek, Inc. Griffin involved an appeal from a district court holding that the plaintiff, as a matter of law, had failed to establish a prima facie case under § 12112(d)(2) because he was “neither disabled nor perceived to be disabled.” The plaintiff in the underlying action, Randy Griffin (Griffin), had applied for a position as a grinder with the defendant, Steeltek, Inc. (Steeltek). Steeltek declined to hire Griffin, allegedly because he did not have the two years of required grinding experience. Griffin claimed that he was never told about the required two years of grinding experience but was told at the time he applied that he was the “best qualified applicant for the position” and “would probably be hired.”

Griffin alleged in the suit that Steeltek’s application process violated the ADA because Steeltek asked questions concerning whether he had a disability and the nature or severity of such disability. He identified two questions in particular on Steeltek’s employment application, which he alleged to violate § 12112(d). The first question asked, “Have you received Worker’s Compensation or Disability Income payments? If yes, describe.” The second asked, “Have you physical defects which preclude you from performing certain

173. Travis, supra note 27, at 336-37.
174. See Griffin, 160 F.3d at 594; Fredenburg, 172 F.3d at 1182; Cossette, 188 F.3d at 969.
176. See Cossette, 188 F.3d at 969 (quoting Griffin, 160 F.3d at 594 and Roe, 124 F.3d at 1229).
177. Behm, supra note 27, at 444.
178. Griffin, 160 F.3d at 592.
179. Id.
180. Id.
181. Id.
182. Id.
183. Id.
jobs? If yes, describe."185 Griffin listed a number of past injuries in response to the first question and left the second question blank.186 Griffin did not contend that he was disabled or that Steeltek perceived him to be disabled. Rather, the sole basis of his claim was that these questions were improper under the ADA.187 Steeltek won a motion for summary judgment because the district court held that Griffin had not stated a prima facie case of disability discrimination.188 However, on appeal, the Tenth Circuit Court of Appeals reached the opposite conclusion, holding that “[a] job applicant need not make a showing that he or she is disabled or perceived as having a disability to state a prima facie case under 42 U.S.C. § 12112(d)(2).”189

The court began its analysis by stating, “It makes little sense to require an employee to demonstrate that he has a disability to prevent his employer from inquiring as to whether or not he has a disability.”190 Next, the court examined the language of the statute, observing that the privacy provisions of § 12112(d) use the terms “job applicant” and “employee,” while the discrimination provisions of 42 U.S.C. §§ 12112(a) and12112(b) use the broader defined term of “qualified individual with a disability.”191 The court concluded that the language shift was intentional by Congress to broaden the scope of § 12112(d).192

The court held that allowing claims by non-disabled persons under this provision is consistent with the underlying policy and purpose of the ADA “to eliminate disability discrimination.”193 The court reasoned that this policy is best served by allowing all job applicants who are subjected to illegal medical questioning and who are in fact injured thereby to bring a cause of action against offending employers.194 The court explained that the legislative history of the ADA indicates that Congress wished to curtail all questioning that would serve to identify and exclude persons with disabilities from consideration for employment.195 Allowing non-disabled job applicants who are injured to sue

185. Id.
186. Id.
187. Id.
188. Id.
189. Id. at 595.
191. Id.
192. Id.
194. Id.
195. Id. (emphasis added).
will “enhance and enforce this blanket prohibition drafted by Congress.”

Finally, the court reasoned that Congress was also concerned with the potential stigmatizing effect of medical inquiries and examinations independent of the consequences because individuals with diseases such as cancer “may object merely to being identified.”

B. The Qualified Individuals with a Disability Approach

Other courts which have considered this issue have either declined to decide it, resolving their cases on other issues, or have concluded that 42 U.S.C. § 12112(d) does not allow claims by non-disabled individuals. These courts offer several reasons in support of their holdings. First, these courts read the plain language of the statute to suggest that a cause of action must be brought by a “qualified individual with a disability.” Second, they state that the legislative history suggests that the statute does not allow a claim by a non-disabled person. Third, they do not find the EEOC regulations to establish a defense for non-disabled persons. Armstrong v. Turner Industries, Inc. is the seminal case for the "Qualified Individuals with a Disability Approach." Armstrong involved an appeal from a district court holding that the plaintiff, as a matter of law, had failed to demonstrate that he is entitled to relief in the form of damages, and because he lacks standing to seek injunctive or declaratory relief under § 12112(d) because he was not disabled. The plaintiff, Jeff Armstrong (Armstrong), had applied for a position as a pipefitter with defendant,
As part of the application process, Turner asked Armstrong to complete several forms including one titled, “Second Injury Fund Questionnaire.” The Questionnaire contained the inquiry “Are you bothered with or have you ever had the following,” followed by a list of ailments. The form included several broad, general questions regarding the applicant’s medical history, including whether the applicant had ever been “a patient in a hospital or clinic,” had ever had surgery, had ever been hospitalized “for nervous trouble,” and whether the applicant’s had ever filed a worker’s compensation claim. Finally, the form asked, “Have you ever had any injury or condition not mentioned on this form?”

Armstrong indicated that he had not received nor had a claim pending for workers’ compensation and that he did not have any “injury or condition not mentioned” on the form. Although the form cautioned that falsification or misrepresentation would constitute grounds for termination, Armstrong certified that the information was accurate. Turner then subjected Armstrong to a brief medical exam. Armstrong was visually inspected for scars indicating previous surgery or serious injury and was asked to provide a urine sample during which employees ran a background check on his medical information. The background check indicated that Armstrong had experienced a possible asbestos exposure several years earlier. Turner rejected Armstrong for falsifying the form and the providing incorrect and/or incomplete information.

On his appeal from summary judgment, Armstrong did not dispute the conclusion that he was not disabled within the meaning of the ADA; nor did he challenge the determination that he was never “perceived as” or “regarded as” being disabled by Turner. Rather, he argued that the pre-employment medical inquiry and exam to which he was subjected constituted a “facial violation” of the ADA. In rejecting Armstrong’s argument, the court held that damages liability under section 12112(d) must be based on something more than “a mere

205. Id. at 556.
206. Id. (internal quotation marks omitted).
207. Id. (internal quotation marks omitted).
208. Id. (internal quotation marks omitted).
209. Id. (internal quotation marks omitted).
211. Id.
212. Id.
213. Id.
214. Id. at 557.
215. Id.
217. Id.
violation of that provision.”

 Rather, the plaintiff must have a “cognizable injury in fact of which the violation is a legal and proximate cause.” Thus, a plaintiff can only be “injured” by such a violation if that individual was actually disabled. Although the Fifth Circuit did not actually hold that the ADA bars non-disabled individuals from pursuing a section 12112(d) claim, this was the practical effect of its holding. In fact, the court declined to specifically address the question of standing or to overrule the district court’s reasoning that a non-disabled individual does not have standing to make a claim, even though it noted that it would be normal to address the standing issue first.

 The district court in Armstrong set out the analysis for the application of § 12112(d) claims to “qualified individual with a disability” only. First, the court examined the language of the statute and concluded that claims under § 12112(d) are subject to § 12112(a) “which sets forth the general rule prohibiting discrimination against a ‘qualified individual with a disability’ . . . in regard to job application procedures, hiring, advancement, discharge, compensation, job training and other terms, conditions and privileges of employment.” Thus, the court concluded that the limiting language of § 12112(a), which prohibits discrimination only against a “qualified individual with a disability,” applies to all of § 12112. Second, the court examined the legislative history of the ADA and found nothing to support the conclusion that Congress intended a cause of action for violation of the ADA rules for non-disabled persons. Rather, the court held that the “provisions exist to protect qualified individuals with disabilities—those who are disabled within the meaning of the ADA—not job applicants who do not meet any of the definitions of disability in § 12102(2).”

218. Id. at 561.
219. Id. at 562.
220. Behm, supra note 27, at 447.
221. Id. (citing James C. Harrington, Survey Article: Civil Rights, 30 Tex. Tech. L. Rev. 507, 532 (1999) (stating that “to require Armstrong, who was not disabled, to demonstrate an injury causally related to a violation of the ADA amounts to splitting hairs because the company profited from using the illegal questionnaire and searching for information in a pre-employment context that violated the ADA”)).
222. Armstrong v. Turner Indus., Inc., 141 F.3d 554, 559 (5th Cir.1998).
224. Id. at 165.
225. Id. at 167.
226. Id.
227. Id.
IV. THE ALL APPLICANTS AND EMPLOYEES APPROACH BETTER PROMOTES THE ADA’S ANTI-DISCRIMINATION PURPOSE AND BETTER PROTECTS THE MEDICAL PRIVACY OF AMERICAN WORKERS

A. The Plain Meaning of § 12112(d)

In any case of statutory interpretation, the court begins with the language of the statute. Statutory interpretation focuses on “the language itself, the specific context in which that language is used, and the broader context of the statute as a whole.” However, “a provision that may seem ambiguous in isolation is often clarified by the remainder of the statutory scheme... because only one of the permissible meanings produces a substantive effect that is compatible with the rest of the law.” Yet, the courts reviewing § 12112(d) have reached opposite conclusions regarding how to interpret it within the broader context of the ADA. Therefore, courts must look to considerations beyond the plain meaning of the statute to determine whether all applicants and employees or only qualified individuals with disabilities may have a cause of action under the provisions of § 12112(d), such as the EEOC’s interpretation of the statute.

B. Congressional Intent and the EEOC Interpretation of § 12112(d)

Under Auer v. Robbins, courts must defer to an agency’s interpretation of its own regulation unless that interpretation is “plainly erroneous or inconsistent with the regulation.” The EEOC interprets the statutory language as making it “clear” that the ADA’s restrictions on inquiries and examinations apply to all employees, not just those with disabilities. Unlike other provisions of the ADA, which refer to “qualified individuals with disabilities,” these use the terms “applicant” and “employee.” The EEOC interprets the shift in language as

---


reflecting Congress’s intent to cover a broader class of individuals and to prevent employers from asking questions and conducting medical examinations that serve no legitimate purpose. The EEOC has explicitly endorsed the interpretation by the courts employing the “All Applicants and Employees Approach.”

Although agency guidelines “constitute a body of experience and informed judgment to which courts and litigants may properly resort for guidance,” they do not bind the courts’ determinations. Yet, Congress gave the EEOC authority to issue regulations implementing the ADA (including rules of construction) consistent with the ADA Amendments Act of 2008. Even though the ADAAA did not change the language of § 12112(d), the EEOC did use its authority to codify its interpretation of the statute in the CFR. In doing so, it referenced Griffin v. Steeltek, Inc. along with the cases of Cossette v. Minnesota Power & Light, and Fredenburg v. Contra Costa County Dep’t of Health Services. Because this interpretation is not “plainly erroneous or inconsistent with the regulation,” courts should follow the Supreme Court precedent in Auer and defer to the guidance of the EEOC on this issue.

C. Privacy of Employee Medical Information in the Digital Era

Perhaps strong regulations of medical and employee records were not necessary in an era when a person had to physically travel to an office and open a file drawer to read an individual’s records. However, today a person can access those same records from halfway around the world with just a few keystrokes. The proliferation of the use of electronic storage of medical records has not only made it easier for employers to gain access to those records but also likely that they will have more records stored in their record systems. Employers should be careful in how they obtain, use, and store electronic medical information.

235. Id.
236. EEOC ENFORCEMENT GUIDANCE, supra note 233.
237. 29 C.F.R. app. § 1630 (2012) (Appendix to Part 1630—Interpretive Guidance on Title I of the Americans with Disabilities Act, App.) (citing the cases of Cossette v. Minn. Power & Light, 188 F.3d 964, 969 (8th Cir. 1999); Fredenburg v. Contra Costa Cnty Dep’t of Health Servs., 172 F.3d 1176, 1182 (9th Cir. 1999); Griffin v. Steeltek, Inc., 160 F.3d 591, 594 (10th Cir.1998), cert. denied, 526 U.S. 1065 (1999), which take the “All Applicants and Employees Approach”).
240. 29 C.F.R. app. § 1630 (2013).
241. Id. at n. 1.
243. See generally id. at 424-28.
Although the ADA and GINA do not specifically address the use of electronic records, employers utilizing electronic records are bound by the same restrictions regarding the access, use, and storage of paper records. First, employers must be careful in how they obtain information because that information is subject to the ADA privacy provisions even if obtained from an online source. For example, an increasing number of employers glean information about job applicants from social media websites through a process known as “scrapping.” However, employers should not seek out information (such as medical information) online that they cannot inquire about in an interview. One way to avoid a potential violation is to have separate personnel tasked with doing background checks from those that make hiring decisions. Second, employers should be careful in using electronic records because the records may not be accurate. Anecdotally, one physician was coding all of his patients as “Albanian” because it was at the top of a pull-down menu in his records system. Because of the ease of electronic records transfer, employers are more likely to request, and providers more likely to send, large amounts of information thereby increasing the odds that employers will receive irrelevant or inaccurate information. Finally, employers could be liable for breach or unnecessary disclosure of electronically stored medical information. In order to avoid unnecessary litigation, employers should consider encrypting and password protecting such data and limiting access to a small group of personnel.

With HIPAA, Congress has implemented strong protections for these very records while they are under the control of medical providers and insurance

244. ADA & GINA: CONFIDENTIALITY REQUIREMENTS, supra note 161.
247. Id.
248. Id.
252. Id. at 423.
companies. However, Congress has failed to extend such strong protections once the records leave the hands of medical providers and insurance companies; creating the potential for others to abuse such records with impunity, especially when such records frequently contain errors. The ADA made it illegal for employers to misuse confidential medical information to discriminate against employees and job applicants or to disclose that information for reasons other than business purposes. The codification of the ADAAA made clear that Congress intended and the EEOC interprets these protections as applying to all individuals, not just those with disabilities.

Limiting challenges of violations to those with disabilities would frustrate Congress’ intent in several ways. First, the “Qualified Individuals with a Disability Approach” places the employer’s focus on an individual’s disability rather than the discriminatory practices of the employer and effectively nullifies the ADA’s “directive that employers evaluate their applicants without regard to disabilities.” Second, if the purpose of these provisions is to prevent discrimination based on disability, that purpose is subverted if a person has to reveal a disability as a precondition to invoking the protection of those same provisions. Forcing individuals to disclose their disability to bring a lawsuit would have a chilling effect on the ADA’s enforcement because individuals, who want to keep their disabilities private and thus have the strongest incentive to enforce the privacy provisions, would be deterred from suing to enforce it. Finally, individuals with disabilities are not the only individuals concerned with protecting their medical information from employers or against whom employers may take adverse action because of their medical history. Thus, the All Applicants and Employees Approach ensures that the private medical data of all job applicants and employees with or without disabilities will receive the fullest protection available under current law. However, this approach is not without its shortcomings.

By limiting recovery to those with “cognizable injuries,” the courts have limited the remedies available under the ADA. 262 A non-injured plaintiff cannot get declaratory or injunctive relief against an employer, no matter if the employer’s practices and policies violate the ADA. 263 Thus, the EEOC or civil rights groups using “testers” cannot take preventative action to challenge employers whose policies and practices violate the privacy provisions of the ADA. 264 Ideally, Congress will amend HIPAA to extend the Security and Privacy Rules to employers, the ADA to limit the collection of medical information to reasons of “business necessity” during the post-offer stage, or both to ensure better protection of medical information. 265 However, a legislative solution does not appear to be on the immediate horizon, especially considering that Congress failed to take such action when it amended the ADA in 2008 and HIPAA in 2009. Therefore, the only logical approach to ensure the greatest protection available under current law of all individuals from unwarranted medical inquiries or disclosures of medical information is for courts to enforce the privacy provisions of the ADA for all job applicants and employees.

V. CONCLUSION

Congress has demonstrated a broad public policy to protect the medical data privacy of the public and to protect workers from discrimination on the basis of disability or genetic information. However, the present law is an uncoordinated patchwork with several significant gaps. The move to electronic storage of medical data by employers and health providers increases the possibility of breach or exploitation of this data. The strongest protection available under current law requires that the ADA protections for employee medical data be available to all employees regardless of disability status. The split of authority provides this protection only in jurisdictions following the “All Applicants and Employees Approach.” Courts should follow this approach, which the EEOC advocates and is codified in the CFR. Although this approach does not allow for preventative action, it provides the best opportunity for all job applicants and employees to obtain remedy for unwarranted medical inquiries or unnecessary disclosures of medical information by employers and best enforces the ADA’s primary purpose of protecting individuals with disabilities from discrimination in the workplace.

262. Harrington, supra note 134, at 532.
263. Id.
264. Id.
ACCESS DENIED: AN ANALYSIS OF SOCIAL MEDIA PASSWORD DEMANDS IN THE PUBLIC EMPLOYMENT SETTING

Mark B. Gerano*

I. INTRODUCTION

Social media usage has become a way of life for people all across the world.1 The most popular social media site, Facebook, has over one billion users alone, equating to one-seventh of the world’s population.2 In addition to various social media sites like Facebook, blogs have increased in popularity,3 growing from 36 million in 2006 to over 181 million in 2011.4 Social media is not only “social,” and isolated to “non-business” settings, but is also spread across all facets of society.5 Because of its increased prevalence in society, problems have arisen, including issues involving the use of social media in the workplace.6 This article discusses one of those problems: how far can a public employer investigate the social media content of a job applicant?

Imagine being in the shoes of a job applicant hoping to land the highly coveted position at the local police department. Only two candidates remain in the process and the police department informs the candidates they must disclose whether they have social media accounts. If the applicants indicate they have social media accounts, then they must disclose their passwords. The candidates know the purpose of the inquiry is to dig up everything that might have an effect on the hiring decision. To protect their private content from the general public, the applicants have their information password protected so only their “friends” can see it. Because neither are “friends” with the police department, the

* J.D. candidate 2014 at the Salmon P. Chase College of Law at Northern Kentucky University. The author is also the executive editor for the 2014-15 Northern Kentucky Law Review.
4. Id.
6. Id. at 223.
department is unable to view the content. The police department’s actions present a number of questions for applicants and place the applicants in a very difficult position. Because of this dilemma, states and the federal government have begun to consider and pass laws to forbid such a practice. The problem that remains, however, is whether such laws adequately address the problem.

The above situation presents job applicants with a choice: either provide the password or be kicked out of the hiring process. Employers also overlook the fact that the above situation might place them in an undesirable situation as well. If both candidates are equal and the public employer checks the social media accounts, discovers something adverse, and uses it, the employer might open itself to potential liability based upon anti-discrimination statutes or other protections in place to ensure fair hiring practices. Additionally, if the public employer conducts an unreasonable search, it might be in violation of the applicant’s Fourth Amendment rights. The issue has become whether a public employer can demand access to an applicant’s private social media content in order to make a hiring decision.

This issue is new and courts have not squarely addressed it. Existing, potentially analogous decisions indicate that the courts would hold a public employer to a relevance or reasonableness standard to determine whether this practice should be allowed. In Tompkins v. Detroit Metropolitan Airport, the United States District Court, Eastern District of Michigan, applied a relevance standard in deciding whether the private information is discoverable in a private employment setting. Tompkins does not directly discuss the specific issue of governmental viewing of private content, but it provides insight on how a court might handle the issue of an unauthorized party who wants access against the wishes of the account owner. If a government is seeking access, the Fourth Amendment comes into play.

---

9. See infra Section II(D)(1). See also Bradley R. Johnson, Untagging Ourselves: Facebook and the Law in the Virtual Panopticon, 13 T.M. COOLEY J. PRACT. & CLINICAL L. 185, 189-201 (2011) (discussing application of Fourth Amendment to government searches of Facebook content in various situations).
13. U.S. CONST. amend. IV. The Fourth Amendment provides: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,
demonstrates how the Supreme Court might handle the Fourth Amendment issue of the reasonableness of a search of a user’s private social media content. The Supreme Court applied a reasonableness standard in Quon to uphold a search of a police officer’s text messages on a government issued pager.

Because of the absence of a judicial precedent with respect to social media content in pre-employment matters, at least two state legislatures have enacted and Congress has introduced legislation to regulate employers that demand passwords to social media accounts prior to making hiring decisions. In their attempt to solve the problem, the legislatures have created additional issues. The current legislative approaches strongly protect job applicants. However, they fail to recognize that certain employment contexts may necessitate a more invasive, but still limited, look into an applicant’s private social media life when proportionate to the government’s need to fully screen or monitor employees in positions of trust.

This article argues that an outright ban is not the best approach because it fails to address special concerns in the public employment context where a more thorough background check is justified. Instead, this article argues that exceptions are necessary for certain public employment positions such as police officers, prison guards, and others in positions of high public trust. This article begins in Part II (A) by reviewing the basics of social media usage in the United States. Part II (B) outlines situations involving employers demanding passwords. Part III describes the statutory approaches being taken across the United States, as well as the judicial approaches taken in relation to both government and non-government searches of private electronic content. Part IV of this article analyzes the pros and cons of both the statutory and judicial approaches and advocates for exceptions to the statutory approaches as the best-reasoned way to deal with the issue of public employers demanding social media passwords from prospective employees.
II. BACKGROUND AND FACTS

A. Social Media Overview

Social media has developed a significant place within modern society.\textsuperscript{19} It has become entrenched in many areas of life, including social, business, and political fields.\textsuperscript{20} As social media’s prominence within society continues to rise, so will its role in legal issues in American society.

1. What is Social Media?

Merriam-Webster defines “social media” as “forms of electronic communication (as Web sites for social networking and micro blogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos).”\textsuperscript{21} People use social media for many purposes including communicating with one another, for viewing video clips, and for gaming.\textsuperscript{22} In addition to the “social aspects” of social media, it is used in a number of business and political settings.\textsuperscript{23} In one recent example, social media played a central role in the social movement to overthrow Hosni Mubarak’s thirty-year government in Egypt.\textsuperscript{24}

Social media is a concept that has been around since the early 1990s.\textsuperscript{25} The modern social media trend began with Facebook, which was initially so popular that nearly half of the 19,500 students at Harvard signed up for it within the first month.\textsuperscript{26} A number of social media sites currently exist, including Facebook, MySpace, LinkedIn, Twitter, Google+, and Pinterest to name a few.\textsuperscript{27} Unlike

\textsuperscript{19} See Arno, supra note 1.
\textsuperscript{20} Sashe Dimitroff, Social Media and Discovery in THE ROLE OF TECHNOLOGY IN EVIDENCE COLLECTION: LEADING LAWYERS ON PRESERVING ELECTRONIC EVIDENCE, DEVELOPING NEW COLLECTION STRATEGIES, AND UNDERSTANDING THE IMPLICATIONS OF SOCIAL MEDIA 39, (Jo Alice Darden ed., 2011).
\textsuperscript{22} Dimitroff, supra note 20, at 40.
\textsuperscript{23} Id. at 40-41.
\textsuperscript{24} Id. (citing Noha El-Hennawy, We are all Khaled Saeed: Redefining political demonstration in Egypt, EGYPT INDEPENDENT (Apr. 8, 2010, 12:53 PM), http://www.almasryalyoum.com/en/news/we-are-all-khaled-saeed-redefining-political-demonstration-egypt) (“In 2011, the Facebook page ‘We are all Khaled Saeed’ attracted hundreds of thousands of people from all over the world.”).
\textsuperscript{26} Id.
\textsuperscript{27} See Dimitroff, supra note 20, at 40; Arno, supra note 1.
other types of media, such as print and television, social media provides an especially easy means of access and operation.\textsuperscript{28}

Social media does not require a large amount of time or money to “publish” ideas.\textsuperscript{29} Instead, with a few keystrokes, a user can make any information publicly viewable.\textsuperscript{30} Because of its “ease of operation,” social media has become a platform in which many users are posting a significant amount of information and sharing that information with great frequency.\textsuperscript{31} Social media usage has sky-rocketed, especially in the United States.\textsuperscript{32} Facebook has maintained its early popularity and is considered the largest stakeholder in the social media business with over one billion users.\textsuperscript{33} Other social media providers are lagging a bit behind Facebook, including Twitter with 190 million users, MySpace with 54.5 million, and LinkedIn with 65 million.\textsuperscript{34} Social media sites have also gained immense popularity overseas.\textsuperscript{35} In China, “QZone,” a social media network similar to Facebook has nearly 380 million members.\textsuperscript{36}

2. Social Media Privacy Policies and Terms of Use

As a part of registration for a social media network, users generally must acknowledge privacy policies and agree to the site’s terms of service.\textsuperscript{37} This section specifically addresses the contents of the most popular, and most widely used social networking site: Facebook.

\begin{itemize}
\item \textsuperscript{28} Dimitroff, supra note 20, at 39.
\item \textsuperscript{29} Id.
\item \textsuperscript{30} Id.
\item \textsuperscript{31} Id. at 1-2.
\item \textsuperscript{32} Id. at 2.
\item \textsuperscript{33} See Vance, supra note 2.
\item \textsuperscript{35} KAI LUKOFF, CHINA’S TOP FOUR SOCIAL NETWORKS: RENRENG, KAIXI001, OZONE, AND 51.COM, VENTUREBEAT SOCIAL (APR. 7, 2010, 7:00 AM), HTTP://VENTUREBEAT.COM/2010/04/07/CHINA%E2%80%99S-TOP-4-SOCIAL-NETWORKS-RENREN-KAIXIN001-OZONE-AND-51.COM/.
\item \textsuperscript{36} Id.
\end{itemize}
a. Promise from the Site to Not Disclose Private Material

Facebook’s terms of service provide that it will not release the personal information contained on a user’s private account to anyone else, although there are a number of exceptions.\(^{38}\) The terms state, “you own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings.”\(^{39}\) Despite this commitment, Facebook also provides three exceptions for when it will release the user’s private content: 1) when the user has granted permission; 2) when the site has given the user notice that it can release certain information (contained in the policy); 3) when the site has removed the name and any identifying information from the content.\(^{40}\) These exceptions are very broad, and allow significant leeway to the site in releasing information. The privacy and application settings allow users to control who sees their information.\(^{41}\) Aside from certain information, a user is able to password-protect nearly all of the content on the user’s social media account.\(^{42}\) Types of information that can be password-protected include photo sharing, comment sharing, and other activities conducted via the social network website.\(^{43}\) The user has some assurance from the site that the information will remain private; but as is apparent, the exceptions might be larger than the protection, and in reality the site might release some of the information rather easily.

b. User’s Promises to the Site

In addition to the network’s promise to not disclose the user’s private information, the user agrees to not disclose his or her password to anyone else.\(^{44}\) The “Statement of Rights and Responsibilities” includes the following provision: “You will not share your password, (or in the case of developers, your secret key), let anyone else access your account, or do anything else that might jeopardize the security of your account.”\(^{45}\) Thus, the user cannot arbitrarily disclose his account password to someone else without breaching the terms of service agreement.\(^{46}\)

\(^{38}\) Id.
\(^{39}\) Id.
\(^{41}\) Id.
\(^{42}\) Id. Certain content is always public consisting of name, profile picture, networks, gender, username, and user ID. Aside from this information, the user has the ability to control whether or not the user wishes to make all other content public or private.
\(^{43}\) Id.
\(^{44}\) Statement of Rights and Responsibilities, supra note 37.
\(^{45}\) Id.
\(^{46}\) Id.
Employers have attempted to get around this provision in different ways.\textsuperscript{47} In one case, an employer utilized what is called an “over-the-shoulder” method to view an applicant’s private content.\textsuperscript{48} Although “over-the-shoulder” gets around the letter of the provision, it may not get around the spirit of it with respect to the protected information.\textsuperscript{49} Facebook seems to suggest that the spirit of the provision might not allow such an approach: “If you violate the letter or spirit of this Statement, or otherwise create risk or possible legal exposure for us, we can stop providing all or part of Facebook to you.”\textsuperscript{50} Yet, it is unclear what the exact “spirit” of the statement really is. For instance, does it include parents looking over the shoulder of minors while on Facebook? By its direct language, it seems to suggest that this practice would not be permissible. Although the method might violate the “spirit” of the provision, this provision does not seem to protect the applicant firmly.

In addition to the provision banning users from distributing their passwords to other people, Facebook’s “Statement of Rights and Responsibilities” prohibits users from attempting to access the private areas of another user’s account.\textsuperscript{51} Users are required to promise that they “will not solicit login information or access an account belonging to someone else.”\textsuperscript{52} This promise presents a number of problems for the employer seeking to look at the applicant’s Facebook page. If the person conducting the applicant’s background investigation was a user of Facebook, that person would not be permitted to “solicit” the applicant’s password.\textsuperscript{53} If the investigator was acting under the employer’s authority and the employer is a Facebook user, the solicitation theoretically would not be allowed.\textsuperscript{54} Because Facebook has over one billion users,\textsuperscript{55} there is a high likelihood that either the investigator or the company itself would also be a user.

\begin{itemize}
\item \textsuperscript{48} See \textit{id.} (discussing the “over the shoulder” method as being where the employer does not require the applicant to give up its password but rather where the interviewer directs the applicant during the interview to log on to the social media site so the interviewer can visually look through the private content).
\item \textsuperscript{49} \textit{id.}
\item \textsuperscript{50} Statement of Rights and Responsibilities, \textit{supra} note 37 (emphasis added).
\item \textsuperscript{51} \textit{id.}
\item \textsuperscript{52} \textit{id.}
\item \textsuperscript{53} See \textit{id.}
\item \textsuperscript{54} See \textit{id.}
\item \textsuperscript{55} Vance, \textit{supra} note 2.
\end{itemize}
B. Situations of Employers Compelling Password Disclosure and Their Reasoning

Employers and other information seekers have come across what they consider a “treasure trove” of information related to potential job applicants via their social media pages.\(^\text{56}\) Although a number of potential problems exist, companies and government employers have found the temptation to view the private material overwhelming.\(^\text{57}\) As a result, many have acted upon it by requiring job applicants to disclose passwords so that the company can review the private material prior to making a hiring decision.\(^\text{58}\) Employers have different reasons for wanting the information.\(^\text{59}\) This section of the article describes two situations in which organizations have attempted to compel social media users to provide passwords: one in the pre-employment context and another in the educational context.

1. Maryland Prison Guard Hiring

In 2011, the Maryland Department of Corrections (MDOC) created a policy requiring prison guard applicants to surrender their social media passwords in order to complete the hiring process.\(^\text{60}\) Under the older policy, prison guard applicants would have to provide their passwords to background investigators so investigators could view the applicant’s private information.\(^\text{61}\) An American Civil Liberties Union (ACLU) complaint ensued, and the Maryland Department of Corrections changed its policy to a “shoulder surfing” method of review.\(^\text{62}\) Although “shoulder surfing” does not provide a background investigator with “full access” to an applicant’s social media account, such conduct might still violate the site’s terms of use and give rise to a number of the issues discussed above.\(^\text{63}\)

The Department of Corrections asserted that it had a compelling reason to search the private content.\(^\text{64}\) The reason asserted was it did not want to hire

\(^{56}\) Sullivan, supra note 47.  
\(^{57}\) Id.  
\(^{58}\) Id.  
\(^{59}\) See id.  
\(^{60}\) Id.  
\(^{61}\) Id.  
\(^{62}\) Sullivan, supra note 47.  “Shoulder surfing” is when a background investigator forces the applicant to log in to the applicant’s social media account during the interview and allows the background investigator to view the personal information while the applicant is still present rather than providing the password to for future use.  
\(^{63}\) See Statement of Rights and Responsibilities, supra note 37.  
\(^{64}\) Sullivan, supra note 47. In a response to the ACLU concerns, a spokesperson of MDOC stated the reason of stopping persons with gang ties from becoming prison guards.
prison guards with verified ties to prison gangs. MDOC provided data to support its policy. At the time of its assertion, MDOC had already denied employment to seven applicants because of evidence that the applicants were involved in prison gangs. All seven individuals had photographs of themselves on their private social media accounts displaying gang signs and making other gestures indicative of prison gang membership.

The department of corrections defended its policy by claiming the searches were “voluntary” and cited data that five out of the last eighty people hired by MDOC did not disclose their social media passwords and were hired anyway. After the ACLU raised a complaint, the policy was suspended, and eventually MDOC adopted the shoulder-surfing approach. Although MDOC called its policy “voluntary,” the applicants were in a “Catch-22” situation to the extent that if they refused to disclose their passwords, they might not get the jobs they sought. The real question that remains is whether the special circumstances associated with the hiring of a position, such as a prison guard, warrants this added background scrutiny. If a strictly cursory background investigation is all that is undertaken, the possibility exists that the employer might be liable for failure to conduct a thorough investigation.

2. Password Demands in the Educational Context

A number of academic institutions are also making password demands. University athletic departments, in particular, are obtaining access to student athletes’ social media accounts by forcing the student athletes to either “friend” a coach or be banned from participating in sports. The University of North Carolina added a section to its student-athlete handbook requiring the following: “Each team must identify at least one coach or administrator who is responsible for having access to and regularly monitoring the content of team members’ social networking sites and postings . . . . The athletics department also reserves the right to have other staff members monitor athletes’ posts.”

65. Id.
66. Id.
67. Id.
68. Id.
69. Id.
70. Sullivan, supra note 47.
71. See Peebles, supra note 8 at 1404-09.
72. See Sullivan, supra note 47.
73. See, e.g., Full Data Use Policy, supra note 40. When a user “friends” another user, private content is normally accessible to the other user. This is contrary to when two users are not “friends.” When two users are not friends, only a user’s publicly viewable information is accessible to the other user.
74. See Sullivan, supra note 47.
75. Id. (internal quotations omitted).
Although student athletes have the right to refuse to “friend” a coach, under the policy such a refusal would mean a ban from activity. These policies reflect the view that schools have an interest in maintaining order among student athletes, and that monitoring social media accounts is a necessary means to achieve that goal. In one instance, the school’s concerns were corroborated when a football player from the University of North Carolina tweeted online about his expensive purchases. The NCAA investigation that followed was a major motivation behind the school’s adoption and implementation of the policy requiring surrender of social media passwords.

Opponents of social media monitoring raise several arguments against educational institutions obtaining access to their students’ private social media accounts. First, opponents analogize the password surrender requirement to one that would force athletes to permit unbridled surveillance of their activities, even at their off-campus apartments. Second, legitimate concerns have been raised regarding the liability of schools that aggressively monitor student posts for future conduct of the athletes. For example, if a school adopts an aggressive monitoring policy but “misses” indicators of dangerous behavior, such as warning signs of a school shooting, the school could potentially be held liable for failing to act. This situation places coaches, particularly, in a difficult position. Coaches are not perfect, and certainly might miss one of these crucial indicators. Third, the monitoring of student posts might violate a student’s right to free speech if it has the result of actually chilling speech. For example, the U.S. Supreme Court’s landmark decision in Tinker v. Des Moines Independent Community School District held that a public school unlawfully denied students their rights to free speech by prohibiting the students from wearing armbands to protest the Vietnam War. Similarly, the “coach friending” requirement could be seen as analogous to the situation in Tinker because if student athletes are required to friend coaches, and have their posts monitored, there would likely be a chilling effect on their ability to speak freely via their social-media accounts.

There are situations in which it might be appropriate for a coach to look at a student athlete’s social-media content, for example, if a coach were informed that a student-athlete was engaged in some type of wrongdoing. This scenario

76. Id.
77. Id.
78. Id.
79. Id.
80. See Sullivan, supra note 47.
81. Id.
82. Id.
83. Id.
85. See Sullivan, supra note 47.
recognizes that special circumstances could exist to suggest that proportionality in determining the level of intrusion is a better approach than the “all or nothing” tactic of enabling blanket surveillance of athletes' social media activity. If coaches and teachers had the right to view content when a specific act made the search warranted, and then narrowly tailored their search of the content to be relevant to the act, both the student and coach would have their interests protected. With such a standard, a coach might avoid undertaking the duty (and corresponding liability) to closely monitor a student’s every online action. At the same time, a student would not be subject to regular and unwarranted intrusions into his or her private social-media content.

III. CURRENT APPROACHES

As the debate regarding whether an organization can require access to private social media content has heated up, states, and the federal government, have started to take legislative action. Two states, Illinois and Maryland, have already passed legislation barring employers from forcing applicants to provide social media account access. In addition to the state legislation, Congress is reviewing the “Social Networking Online Protection Act,” which would create a federal law prohibiting the imposition of conditions on a job applicant to disclose his or her personal password to online content. All of these approaches would be inclusive of public employees.

In addition to legislative action on the issue, the judiciary has taken action regarding intrusions on private social media content by issuing important decisions in the civil discovery context. One federal district court in particular has addressed the discoverability of private social media content in a civil proceeding.

A. Illinois’ “The Right to Privacy in the Workplace Act.”

On May 22, 2012, the Illinois Senate passed HR 3782, “The Right to Privacy in the Workplace Act.” The governor of Illinois signed the bill into law on

87. Social Networking Online Privacy Act, H.R. 537, 113th Cong. § 2 (as introduced on Feb. 6, 2013).
89. Tompkins, 278 F.R.D. at 387-88.
August 1, 2012. The Illinois bill amended a previous bill that prohibited employers from inquiring whether prospective applicants have ever filed a worker’s compensation claim or a claim under an occupational disease law. The bill’s sponsor indicated a two-fold reasoning for the legislation. First, the bill extends a prospective employee’s reasonable expectation of privacy to the social networking sphere. Second, because employers cannot ask about certain characteristics, such as race, sex, gender and sexual orientation in job applications, the employers should not be allowed to glean the same information from social networking profiles of applicants.

The bill has two main provisions. First, it makes it “unlawful for any employer to request or require any employee or prospective employee to provide any password or other related account information in order to gain access to the . . . account or profile on a social networking website.” This section of the bill prohibits employers from both demanding and making a simple “request” for the password, thus keeping employees from being in a difficult situation when they need to decide between giving up the password or being passed over for a job. Second, the bill makes it illegal for an employer to “demand access in any manner to an employee’s or prospective employee’s account or profile on a social networking website.” This part of the bill would prohibit the “over-the-shoulder” method of investigation discussed above, where an interviewer demands that the interviewee log in to a social networking website so the interviewer can view the applicant’s private content.

The Illinois bill also expressly provides some limitations to the applicant and employee’s rights. Employers are not prohibited from monitoring use of their own electronic equipment or from monitoring applicant’s information that is already in the “public domain.” The bill does not provide any exceptions to this rule for special situations, such as the situation involving the Maryland Department of Corrections’ interest in ensuring it did not hire a prison guard.

91. Id.
94. Id.
95. Id.
97. Id. (emphasis added).
98. Id.
99. Id.
100. See supra note 63 for discussion of “shoulder surfing.”
102. Id.
who is affiliated with a prison gang. Under the Illinois bill, such acts would be illegal. 103

B. Maryland Senate Bill 433

On May 2, 2012, the governor of Maryland signed Senate Bill 433 into law, which made Maryland the first state to ban the employer practice of requiring surrender of applicants’ social media passwords as a prerequisite to employment. 104 The Maryland bill is set to become law on October 1, 2012. 105

The Maryland bill contains three main provisions. First, it provides that “an employer may not request or require that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device.” 106 Unlike the Illinois bill that bans employers from “demanding access in any manner,” 107 this section of the Maryland law creates an open door for the over-the-shoulder method of review because an employer can view the information in a manner that does not require the applicant to disclose its password. 108 Second, the bill provides, “an employer may not . . . fail to or refuse to hire any applicant as a result of the applicant’s refusal to disclose any information . . . .” 109 This provision effectively precludes the employer from penalizing an applicant for refusing to provide his or her password. 110 By contrast, the Illinois approach is stricter and does not permit the employer to even ask for the applicant’s personal password. 111 The Maryland bill still permits the employer to request the password, but simply prohibits the employer from penalizing the applicant for any refusal to provide it. 112 Crucially, the bill also expressly provides that an employer may not avoid liability under the statute by hiring an agent or a third party to do background investigations and ask questions that the employer would be otherwise prohibited from asking. 113 The Maryland bill specifies that the term “[e]mployer’ includes an agent, a representative, and a designee of the employer.” 114

103. Id.
104. Bradley Shear, Maryland’s Facebook Username and Password Law is a Win For Employers, Employees, and Job Applicants, SHEAR SOCIAL MEDIA (May 2, 2012), http://www.shearsocialmedia.com/2012/05/marylands-facebook-username-and.html.
106. Id.
109. Id.
110. Id.
112. Id.
114. Id.
Like the Illinois bill, the Maryland bill contains two express limitations. First, it expressly provides for an employer’s right to conduct investigations regarding usage of computers for business purposes. Second, it provides employers with the right to conduct investigations regarding the downloading of the company’s proprietary information to a social media website or other personal website. Unlike the Illinois law, the Maryland law contains a section regulating “employees,” in which employees are prohibited from downloading unauthorized proprietary information or financial data to an employee’s personal website or social media account. If the employer receives information that such a downloading has taken place, it may conduct an appropriate investigation into the personal website.

C. Federal Legislation: The Social Networking Online Protection Act

On April 27, 2012, House Resolution 5050, The Social Networking Online Protection Act (SNOPA), was introduced in the United States House of Representatives. The bill died in committee, but was re-introduced on February 6, 2013, and re-referred to the House Education and the Workforce Committee. Although SNOPA is not the first federal attempt at addressing the issue, it is the first federal legislation aimed directly at addressing the privacy interests contained in personal password-protected social media accounts.

SNOPA contains four main provisions. First, it makes it unlawful for any employer to “require or request that an employee or applicant for employment provide the employer with a username, password, or any other means for accessing a private email account of the employee . . . or any social networking website.” This provision is analogous to the section of the Illinois bill that
makes it illegal to both demand and request access.\textsuperscript{126} Second, SNOPA protects employees who do not wish to provide passwords.\textsuperscript{127} SNOPA makes it illegal 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 the employee or applicant does not provide its social media password.\textsuperscript{128} Third, SNOPA expressly applies to educational institutions and their conduct as it relates to students.\textsuperscript{129} SNOPA amends the Higher Education Act of 1965 by making it illegal for an educational institution to “require or request that a student or potential student provide the institution with a user name, password, or any other means of accessing . . . a social networking website.”\textsuperscript{130} Fourth, SNOPA amends the Elementary and Secondary Education Act of 1965 to give similar protections to students of local schools receiving funds under the Act.\textsuperscript{131} The bill establishes a $10,000 civil penalty for employers who violate the statute.\textsuperscript{132} The Secretary of Labor can enforce the statute by directly raising violations of SNOPA to the United States District Courts.\textsuperscript{133}

Unlike the legislative acts in Maryland and Illinois, SNOPA does not contain any express limitations.\textsuperscript{134} Likewise, there are no exceptions contained in the bill at this stage in the legislative process, but it is likely that some changes will occur as the bill moves through Congress.\textsuperscript{135} Proponents of the bill contend that “[w]e must draw the line somewhere” and that the bill is necessary to protect personal privacy rights.\textsuperscript{136}

\textbf{D. Judicial Treatment of Private Social Media Content}

Because the question of whether an employer may request or demand social media passwords from job applicants is relatively new, the United States Supreme Court has not yet addressed it. However, federal courts are beginning

\begin{itemize}
\item \textsuperscript{127} Social Networking Online Privacy Act, H.R. 537, 113th Cong. § 2(a)(2) (as introduced on Feb. 6, 2013).
\item \textsuperscript{128} Id.
\item \textsuperscript{129} Id. at § 3.
\item \textsuperscript{130} Id.
\item \textsuperscript{131} Id. at § 4.
\item \textsuperscript{132} Id. at § 2(b)(1)(A).
\item \textsuperscript{133} Social Networking Online Privacy Act, H.R. 537, 113th Cong. § 2(b)(2) (as introduced on Feb. 6, 2013).
\item \textsuperscript{134} See id. at § 2.
\item \textsuperscript{135} The Legislative Process, U.S. HOUSE OF REPRESENTATIVES, http://www.house.gov/content/learn/legislative_process/ (last visited July 1, 2013).
\end{itemize}
to deal with the issue of accessibility of private social media content in other areas of law. This section begins by reviewing a case in which the Supreme Court handled a government agency’s search of electronic content. Then the discussion will explore how a federal district court has addressed the issue of private social media content in the context of a discovery request. These court decisions taken together shed light on how a court may deal with the specific issue of compulsory password disclosure in the public employment context.

1. Government Searches of Personal Communication Devices

When a government actor is involved, a search of private electronic content generates concerns about whether such a search is reasonable under the Fourth Amendment. In City of Ontario, California v. Quon, the Supreme Court held that a police department’s search of a police officer’s text messages on a government issued pager was reasonable.

In Quon, the Ontario (California) Police Department issued a police officer (Quon) an alphanumeric pager in the course of his employment. After receiving higher than normal bills, the department looked at the content of the messages the officer was sending and receiving. The stated purpose of the inquiry was to “determine whether the existing character limit was too low—that is, whether officers such as Quon were having to pay fees for sending work-related messages—or if the overages were for personal messages.” After finding that many of the messages were merely personal, the city disciplined Officer Quon. The officer then filed suit, alleging violations of his Fourth Amendment right to be free from unreasonable searches.

In its analysis, the Court reversed the Ninth Circuit and held that because the search was reasonable, the city did not violate the officer’s Fourth Amendment rights. The Court began by confirming that the Fourth Amendment applies to situations when the government is acting as an employer. In its holding, the Court relied primarily on Ortega v. O’Connor to determine that no Fourth


139. Tompkins, 278 F.R.D. at 387.

140. See, e.g., Quon, 130 S. Ct. at 2619.

141. Id. at 2633.

142. Id. at 2624-25.

143. Id. at 2625.

144. Id. at 2626.

145. Id.


147. Id. at 2633.

148. Id. at 2627 (citing Treasury Emps. v. Von Raab, 489 U.S. 656, 665 (1989)).
Amendment violation had occurred.\textsuperscript{149} The \textit{Quon} Court explained the \textit{O’Connor} plurality two-step approach:

First, because “some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable,” a court must consider “[t]he operational realities of the workplace” in order to determine whether an employee’s Fourth Amendment rights are implicated. On this view, “the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.” Next, where an employee has a legitimate privacy expectation, an employer’s intrusion on that expectation “for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances.”\textsuperscript{150}

The Court also cited Justice Scalia’s concurring approach from \textit{O’Connor} that although the Fourth Amendment extends to government offices, “government searches to retrieve work-related materials or to investigate violations of workplace rules—searches of the sort that are regarded as reasonable and normal in the private-employer context” are usually reasonable.\textsuperscript{151}

Before applying the tests to this situation, the Court assumed that “(1) Quon had a reasonable privacy expectation; (2) petitioners’ review of the transcript constituted a Fourth Amendment search; and (3) the principles applicable to a government employer’s search of an employee’s physical office apply as well in the electronic sphere.”\textsuperscript{152} The Court determined that the department had a “legitimate work purpose” to review the content of the messages in order to determine that neither the employee nor the city was incurring unnecessary expenses.\textsuperscript{153} The Court also determined that a review of the transcripts of the messages was a reasonable limitation on the scope of the search “because it was an efficient and expedient way to determine whether Quon’s overages were the result of work-related messaging or personal use.”\textsuperscript{154} Thus, the Court held that the search was reasonable under the Fourth Amendment because it “was motivated by a legitimate work-related purpose, and because it was not excessive in scope.”\textsuperscript{155}

\textsuperscript{149} Id. at 2628-29 (citing Ortega v. O’Connor, 480 U.S. 709 (1987)).
\textsuperscript{150} Id. at 2628 (quoting \textit{O’Connor}, 480 U.S. at 717-18, 725-26).
\textsuperscript{151} City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2629 (2010) (quoting \textit{O’Connor}, 480 U.S. at 732 (internal quotations omitted)).
\textsuperscript{152} Id. at 2623.
\textsuperscript{153} Id. at 2631.
\textsuperscript{154} Id.
\textsuperscript{155} Id. at 2632 (concluding that applying either of the \textit{O’Connor} tests would produce the same result).
The decision of the Court in *Quon* shows that although a warrantless search under the Fourth Amendment is presumptively *per se* unreasonable, there are some exceptions, and a search in the workplace for “a legitimate work-related purpose” is one of those exceptions. The only requirements are that the search must be “justified at its inception” and “reasonably related in scope to the circumstances which justified the interference in the first place.” These precedents hint that pre-employment searches in some instances are permissible if they are justified and narrowly tailored.

2. Private Social Media Content and Discoverability in Civil Proceedings

In a recent decision entitled *Tompkins v. Detroit Metropolitan Airport*, the U.S. District Court for the Eastern District of Michigan considered whether private social media content was discoverable in the context of a civil suit. Although the case did not involve a request for a job applicant’s private social media content, it provides insight on the proper standard for determining whether or not compulsory disclosure of private social media material is permissible.

The plaintiff in *Tompkins* alleged a back injury due to a slip-and-fall accident in December of 2005 at the Detroit Metropolitan Airport. Plaintiff claimed she was unable to work or fully enjoy life due to her injuries. The airport requested that plaintiff sign an authorization for the release of the records from her entire Facebook account. The court distinguished the state court opinions, however, because the situations before the state courts involved the plaintiff’s public Facebook content, which “was clearly inconsistent with the plaintiffs’ claims of disabling injuries.” In fact, the plaintiff’s Facebook

156. *Id.*
159. See *id.* at 388.
160. *Id.*
161. *Id.*
162. *Id.*
163. *Id.*
165. *Id.*
account in McMillen included references to a fishing trip and attendance at the Daytona 500 despite his claim of “inability to enjoy certain pleasures in life,” while the plaintiff’s Facebook and My Space accounts in Romano demonstrated an “active lifestyle” and travel in contradiction to her claim of confinement to house and bed.166

In Tompkins, the plaintiff argued that because the airport lacked any reason to suspect that the private material of her Facebook account contained similar content, the information was not discoverable.167 The former employee further argued that the proper result in his case should be consistent with the decision reached by the New York Appellate Division in its case, McCann v. Harleysville Ins. Co. of New York—to not permit the defendant to “conduct a fishing expedition” into the plaintiff’s Facebook account in hopes of finding something.168

The Tompkins court applied the standard relevancy test in denying the motion to compel discovery of the private content,169 and held that “there must be a threshold showing that the requested information is reasonably calculated to lead to the discovery of admissible evidence.”170 In its decision, the court discussed its view that if this type of discovery tactic were to be allowed, a defendant would be free to engage in the fishing expedition described in McCann.171 Here, the court recognized the fact that some situations require the release of private information, but there must be some threshold showing of relevance in order to do so.172 The only evidence offered by the airport to support its suspicion from the public area of the plaintiff’s Facebook page was a picture of her at a birthday party holding a small dog of approximately five pounds, which “could be lifted with minimal effort.”173 The court concluded that, here, there was not a sufficient showing that the requested information was “reasonably calculated to lead to the discovery of admissible evidence” and the motion was denied.174

Despite social media’s immense popularity, the ability of an employer to access employees’ private online content has not commonly been at issue in the courts.175 Cases suggest that a relevancy standard would best address the

166. Id.
167. Id.
169. Id. at 389
171. Id. See also McCann, 78 A.D.3d at 1525.
172. Id. at 388-89.
173. Id. at 389.
174. Id.
175. Dimitroff, supra note 20, at 45.
questions regarding what material is discoverable. 176 The general rule for
discovery of social media content is that the court is likely to allow discovery of
such content only if the material is relevant. 177 If a party has no reason to search
the private social media content and is engaging in a mere “fishing expedition,”
courts are more reluctant to allow discovery of the content. 178

IV. ANALYSIS

Currently, no uniform standard exists for whether public employers can
request or demand social media passwords from job applicants. 179 The issue of
social media password provision is not specific to any particular state or
geographic area, but instead is a problem that is present all across the United
States in both private and public employment contexts. 180 Because of the wide
spectrum of the issue, a uniform standard needs to be developed to provide the
rules of engagement to both public employers and job applicants. However, this
uniform standard must also provide for exceptions in order to permit reasonable
inquiries to match certain special circumstances. This section argues that a
federal, statutory approach with exceptions is the best way to deal with the
problem.

A. Advocating for a Federal Statutory Approach with Exceptions

Because an outright ban on allowing employers to look at private social
media content creates “black holes” in an employer’s ability effectively to screen
employees in positions where such screening is warranted, a statutory relevance-
based standard must be developed. There are three important components to this
statutory approach.

First, to effectively deal with the need for uniformity, a federal statute should
be passed. A uniform federal statute provides consistency among the states,
which benefits both public employers and applicants by laying out the “rules of
the game” prior to the parties stepping onto the field. Also, public employers
frequently conduct business in multiple states and if the statutory approaches

176. Id. at 8.
12, 2011)).
178. Id. at 9 (citing Mackelporang v. Fid. Nat’l Title Agency of Nev., Inc., No. 2:06-cv-00788,
Assemb., Reg. Sess. (Md. 2012); Social Networking Online Privacy Act, H.R. 537, 113th Cong. §
2012).
180. Sullivan, supra note 47.
were different in each state, employers would be forced to conduct hiring practices differently depending on the location of the job.

Second, the federal statute should allow an employer to request or demand a password when two conditions are met: necessity of the information is demonstrated, and relevance of the private information is shown. Once necessity and relevance have been demonstrated, the search should be only as extensive as is required by the circumstances of the situation. By proving necessity and relevance, and then limiting the search to achieve only its specific objective, an employer would also satisfy the reasonableness requirements on which the U.S. Supreme Court relied in Quon.\(^{181}\) The prison guard example is a good illustration of how an employer can accomplish these three elements of reasonableness.

The first element, necessity, is likely met. The job of a prison guard is to ensure that prisoners are kept out of society, and that while confined, the prisoners themselves are also kept safe from other inmates. Because of the nature of the guard’s duties, a prison can demonstrate necessity in obtaining assurance that the person is not a member of a gang. Prison gang members who are placed in a position of guarding prisoners could expose both society to potential harm by having prisoners set free, as well as other prisoners to harm by allowing gang enterprises to run rampant in prison.

The second element, relevance, would be more difficult to meet. The relevance element is essentially that the prison should not be allowed to do a completely unjustified search of the person’s social media account. There must be some other type of information to lead an investigator into the account. This mirrors the situation in Quon where the private electronic content was only accessed one there was a “reason to look.”\(^{182}\) If a background investigator found out information that gave the investigator a reasonable belief that the applicant was involved in gang activity, then the investigator would be able to look at the content. Some examples of this type of material would be the presence of gang tattoos, information provided by the applicant about gang ties, or information obtained elsewhere that seemed to indicate the presence of a gang affiliation. If the investigator has a reason to look, the search of the social media content would be relevant.

Last, the search should not exceed the scope of what is necessary to either confirm or deny the potential presence of gang ties. In the case of the guards, if the search is relevant because it is based on the presence of some evidence of gang ties, the scope of the search would be permissible as long as it was furthering that inquiry. If an investigator looks at pictures of the applicant’s

\(^{182}\) Id.
political involvement, this would likely exceed the permissible scope. On the other hand, if the investigator looks at pictures of the applicant posing with known gang members, the search would be within the proper scope. In cases where the necessity of the search is low, and the relevance that led to the search is minimal, the scope should also be minimal. This scope requirement also follows in line with Quon where the search was reasonable partially because its scope was not excessive.183

With respect to the prison guards, a search would be permissible as long as the following conditions are met. First, there is a necessity to search the content. This element is met strictly by the nature of the job and the associated risks. Second, there must be some type of relevance to the search. The investigators must possess some type of reason to look as opposed to just going on a “fishing expedition.” Third, the search must not exceed the scope of what is being looked for. As long as the three elements are met, the search is reasonable and should be allowed.

Third, the provision should prohibit the request or demand for password information in all other situations and should contain a penalty for violators to serve as a deterrent. If there is no deterrent effect, public employers can simply violate the statute and then hope they do not get sued. If employers were allowed to act at will and wait to see if someone has the time or money to sue them, the law would not carry any true weight. For this reason, a deterrent provision must be a part of the law. In addition to this deterrent provision, a public employer who violates the statute would likely not meet the threshold standard of a reasonable search under the Fourth Amendment.

B. Advantages and Disadvantages of the Statutory Approaches

There are two primary advantages to using a statutory approach in dealing with the problem. First, a statutory approach provides a uniform set of rules laid out in advance of a dispute, as opposed to the rules crafted after the dispute has started. Early statutory approaches, up to this point, have laid out what is allowed and not allowed for both public employers and employees.184 In theory, legislative action has included a significant amount of time and deliberation by a large body of representatives and other legislators. Also, in theory, a legislative body is best positioned to assess the “best way” to do things. Second, the statutory approaches currently in effect have not left any grey area for employers to self-interpret and circumvent.185 They adequately protect against the practice

---
183. Id.
185. Id.
of compelling password provision. Both state statutory schemes, as well as SNOPA, are highly protective of employees in that they do not allow an employer to view the information contained in private social media areas for hiring activities. In addition, the Fourth Amendment protects applicants applying for government jobs to some degree.

The first major disadvantage of both the state and federal statutory approaches is that they do not leave any wiggle room for a situation in which a more intrusive background investigation may be warranted. In some cases, such special circumstances may justify a more intrusive background check. One example is the prison guard situation. If a gang member slipped through the cracks and was hired as a prison guard, the gang member could supply contraband, drugs, and other dangerous items to prisoners, who could in turn endanger their safety and the safety of others. The heart of the entire issue is balancing the rights of the job applicant against the needs of the organization. Although prison guard applicants have privacy interests in protecting their private social media content, there is an obligation on the part of the hiring entity to ensure that the persons hired are not going to place other lives in jeopardy. If a state law prohibits the prison from conducting a more thorough background investigation, it creates a "black hole" of potentially serious consequences. This article suggests that when there is a threshold showing of relevance, a narrowly tailored search is permissible into an applicant’s private Facebook content. The Court in Quon allowed a search of an otherwise private piece of equipment for legitimate government purpose based upon the relevance and scope of the search. A similar standard is important for positions that require higher levels of public trust and inquiry.

The second disadvantage is the lack of uniformity with the current state and federal statutory approaches. One example of this lack of uniformity involves the over-the-shoulder method. The over-the-shoulder investigative method is allowed under the Maryland law, but not under the Illinois law. Additionally, in one state an employer may not so much as even “request” the social-media password, but in other states the employer can make a request, just not a demand. The statutes have created varying levels of security and have created a system in which a large national problem, spread all around the county, is

186. Id.
187. Id.
189. Quon, 130 S. Ct. at 2633.
being handled differently based upon being situated on different sides of a state boundary. Federal legislators have tried to fix the problem and attempted to create a uniform standard; however, it is still pending in Congress.192

C. Advantages and Disadvantages of the Judicial Approach

Although the Supreme Court has not ruled on this specific issue, the holdings in the Tompkins and Quon cases discussed above give clues as to the type of approach a court may use in dealing with this pre-employment situation.193 Like with the statutory approaches, there are advantages and disadvantages to a judicial approach in dealing with the problem.

The first major advantage of the judicial approaches discussed above is that they allow the court to deal with the problem on a case-by-case basis. This case-by-case approach fills the “black holes” created by the complete bans in the statutory approaches. As discussed above, certain positions warrant higher degrees of scrutiny into an applicant’s background than others do. For instance, it would be more reasonable to investigate deeply an applicant for a school teaching job because of the high amount of contact that a teacher has with children. On the other hand, less scrutiny may be warranted for the hiring of a person who has a position that is not of such high public trust.

The second advantage of the judicial approach is that it allows parties to advance their arguments independently in each case, as opposed to the legislative approach where the door is shut and the line is drawn after the issue had been debated by the legislature and passed. Each hiring situation is unique, and the legislature may not have considered the specific reasoning invoked in each unique case, where some relevancy and necessity could be present. Frequently, circumstances change. Thus having a legislative standard set in stone does not allow any flexibility. Having an “all or nothing” law closes the door to parties that did not participate in the legislative process but still have a compelling reason on one side or the other because of the relevancy to their situation.

The judicial approach in Quon is more desirable, especially in the public employment context. It forces government employers to provide a reasonable justification for looking at the private information. This would allow for employers to conduct reasonable and proportionate investigations when deemed necessary, such as in the situation of police officers or prison guards, but it would not allow a such an invasive inquiry into positions like secretaries or janitors who are public employees not placed in positions of high public trust.

---

192. Social Networking Online Privacy Act, H.R. 537, 113th Cong. § 2 (as introduced on Feb. 06, 2013).
The judicial approach also has two disadvantages. First, it could lead to varying judgments on similar issues. This is a typical problem with a common law approach to any situation. If judges are allowed to make decisions on a case-by-case basis, there is a high potential for different standards being created all across the country. This varying law issue suggests the need for a uniform set of rules. Second, although each judicial precedent creates applicable case law for an employer to follow, it does not provide an adequate, immediate remedy to an employee who is unnecessarily compelled to produce her Facebook password. The fact that a court later determines the request or demand for the password was not reasonable does not do anything for the employee who is forced to make a difficult decision at that very moment. An employee who is up for a job and who does not want to provide a password has two options: give up the possibility of getting the job, or spend a significant amount of money to fight the issue in court. In most cases, employers and applicants will both just walk away from the situation and not spend a lot of money to fight it out, thus making it a somewhat counterintuitive system anyway. The “provide now, litigate later” approach does not squarely protect the public employees involved because it does not provide an immediate remedy to the situation for the applicant faced with a difficult choice.

V. CONCLUSION

The problem of public employers requesting or demanding the social media passwords of job applicants is an evolving problem that requires a definitive solution. The statutory approaches currently employed do not adequately address the problem, because they do not allow an employer any leeway in special situations and leave “black holes” out there into which bad applicants could find their way. The judicial approach used in similar situations also does not adequately address the problem because of the potential for extremely inconsistent judgments and the high cost of applicants to litigate their disputes. As a result, a uniform federal statute should be created that generally bans the practice but allows it when the employer has a necessity to see the information, the information is relevant to the background investigation, and the scope of the inquiry is only so broad as to achieve the purpose being sought. The statute also needs to have a penalty attached to serve as a deterrent, because without it employers would have no incentive to follow the rules.