American University Law Review

Volume 64 | Issue 1 Article 2

2014

To Read Or Not to Read: Privacy within Social Networks, the Entitlement of Employees to a Virtual Private Zone, and the Balloon Theory

Shlomit Yanisky-Ravid

Follow this and additional works at: http://digitalcommons.wcl.american.edu/aulr

 Part of the Law Commons

Recommended Citation

Yanisky-Ravid, Shlomit. "To Read Or Not to Read: Privacy within Social Networks, the Entitlement of Employees to a Virtual Private Zone, and the Balloon Theory." American University Law Review 64, no.1 (2014): 53-108.

This Article is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University Law Review by an authorized administrator of Digital Commons @ American University Washington College of Law. For more information, please contact fbrown@wcl.american.edu.

To Read Or Not to Read: Privacy within Social Networks, the Entitlement of Employees to a Virtual Private Zone, and the Balloon Theory

Keywords
Right of privacy, Law -- Interpretation & construction, Implied consent (Law), Social networks -- Law & legislation, Internet -- Law & legislation -- United States, Discrimination -- Law & legislation -- United States, Labor laws & legislation -- United States

This article is available in American University Law Review: http://digitalcommons.wcl.american.edu/aulr/vol64/iss1/2

TO READ OR NOT TO READ: PRIVACY WITHIN SOCIAL NETWORKS, THE ENTITLEMENT OF EMPLOYEES TO A VIRTUAL "PRIVATE ZONE," AND THE BALLOON THEORY

DR. SHLOMIT YANISKY-RAVID*

Social networking has increasingly become the most common venue of self-expression in the digital era. Although social networks started as a social vehicle, they have recently become a major source for employers to track personal data ("screening") of applicants, employees, or former employees.

This Article addresses whether this casual business routine harms employees' rights to privacy with regard to data that users post on social networks, what the drawbacks of this routine may be, and why and how privacy rights should be protected to secure private zones within the virtual sphere. The Article suggests that a privacy right exists within the context of employment, even in data posted openly on social networking sites. Antidiscrimination laws, the misleading nature of social networks' privacy policies, cognitive biases, unequal bargaining power, the lack of a right to be forgotten, lost control over data posted by third parties, and psychological reasoning all justify a reconsideration of the current regime.

---

* Visiting Professor, *Fordham Law School*, 2012, 2014; Fellow, *Yale Law School*, Information Society Project (ISP), 2011–2014. Senior Faculty, *Ono Academic Law School*, Israel. Founder and Head of the Shalom Comparative Legal Research Center, *Ono Academic Law School*, Israel. Thanks to Professor Jack Balkin, ISP; Professor Joel Reidenberg, Center on Law and Information Policy (CLIP); *Fordham Law School*; Professor Samuel Estreicher; The Center for Labor and Employment Law, *NYU Law School*; Professor Patricia Sanchez Abril; Dr. Alberto Aronovitz; and the staff of the *Swiss Institute of Comparative Law*, Lausanne, Switzerland. Special thanks to Ms. Elizabeth Ledkovsky for her outstanding research assistance and to the editors of the *American University Law Review* for their devoted work.

The Article further claims that securing a "private zone" for U.S. employees, a concept adopted by several other legal regimes, is justified by a bundle of psychological theories that can be concisely described as the "balloon theory" (or the "magnet field theory"), which encompasses the importance of a private sphere that constantly and permanently surrounds one's persona wherever one goes—including within the public domain and digital spheres.

In this Article, I call for a re-thinking of the current U.S. regime based on tort law (expectation test) and contract law (implied consent based on firms' policies) because the current regime costs applicants and employees a near-total loss of privacy in their virtual postings.

This Article not only argues for a more balanced approach to employees' privacy but also suggests a new desirable model for policymakers to adopt. I propose this challenge be addressed by the adoption of new legal tools. Implementing the Least Invasive Means—a proportionality standard that obeys antidiscrimination laws, maintains transparency, and ensures informed consent and a right to be heard—would lead to a better and more balanced approach to privacy in the workplace. I also contend that this model may be implemented to protect privacy rights in data posted on social networks beyond the context of employment.

TABLE OF CONTENTS

INTRODUCTION

Social networks such as Facebook, Twitter, and LinkedIn have increasingly become a primary venue of self-expression in the digital era, enabling friends and families to connect and stay in touch with one another.[1]

Currently, one-seventh of the world's population has an account with Facebook, the most popular social network.[2] Almost three-quarters of online American adults (seventy-three percent) are Facebook users.[3] Although social networks started in a social context, they have become, as this Article discusses in Parts I.B. and I.C., a significant work tool for employers in everyday practice for "screening" personal data about applicants, employees, or former

---

1. *See* Jocelyn M. Lockhart, Facebook as a Job Screening Tool: Are Sales Employers Discriminating Against Job Applicants based on their Facebook Profiles? 1, 6 (Apr. 2013) (unpublished B.A. thesis, University of Southern Mississippi), *available at* http://aquila.usm.edu/cgi/viewcontent.cgi?article=1142&context=honors_theses (discussing the significant growth in the number of employers that use or "always search" social network data in the hiring process).

2. *See* Mark B. Gerano, Note, *Access Denied: An Analysis of Social Media Password Demands in the Public Employment Setting*, 40 N. KY. L. REV. 665, 665 (2013) (showing that "[s]ocial media is not only 'social,' and isolated to 'non-business' settings, but is also spread across all facets of society"). Notably, blogs have become increasingly prominent, rising from thirty-six million in 2006 to more than 181 million in 2011. *Id.*

3. MAEVE DUGGAN & AARON SMITH, PEW RESEARCH CTR., SOCIAL MEDIA UPDATE 2013 1 (2013), *available at* http://www.pewinternet.org/files/2013/12/PIP_Social-Networking-2013.pdf.

employees that is posted on social networks, websites, and in other virtual spheres. For example, Ellen Simonetti, a flight attendant for Delta Air Lines, was dismissed after posting inappropriate photos of herself in the company's uniform on her blog;[4] Stacy Snyder, a twenty-five year old student teacher, was prevented from obtaining a full-time teaching position after posting a picture of herself on MySpace "wearing a pirate hat and drinking from a plastic cup, with the caption 'Drunken Pirate'";[5] Marina Stengart, the Executive Director of Nursing for a home-care nursing provider, had her e-mails between herself and her lawyer retrieved from her company-issued laptop;[6] and Sandi Lazette, an employee with Verizon, had 48,000 personal e-mails retrieved from her former company-issued Blackberry because the password was saved in the phone.[7]

This transition has created unexpected results for employees, many of whom have lost their jobs, been denied unemployment, or experienced invasions of their privacy while engaged in non-work activities.[8] All of these examples reflect the new era in which people, including employers and employees, use digital media as an integral part of everyday life and, more importantly, as a major, yet basic, means of communication that is preferred to more limiting or inconvenient traditional alternatives (i.e., sending a paper invitation or printing pictures instead of posting them on Instagram or Facebook) as well as a tool for social surveillance.[9]

---

4. *See* Jo Twist, *Blogger Grounded by Her Airline*, BBC, http://news.bbc.co.uk/2/hi/technology/3955913.stm (last updated Oct. 27, 2004, 8:30 AM) (explaining that to Simonetti's knowledge, Delta Airlines did not have a specific policy prohibiting the posting of pictures on the Internet or blogging).

5. *See* Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES (July 21, 2010), http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all&_r=0 (detailing how Snyder's university denied her a teaching degree after viewing the one picture).

6. Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655–56 (N.J. 2010).

7. Lazette v. Kulmatycki, 949 F. Supp. 2d 748, 751 (N.D. Ohio 2013). When Lazette became aware of her employer's actions, she changed her password. *Id.* Among the contents the employer viewed were communications about Lazette's "family, career, financials, health and other personal matters." *Id.*

8. Lockhart, *supra* note 1, at 2 (noting that social networking sites have emerged as a popular "job-screening tool" and that "employers should be intensely concerned with [this]").

9. YOUTH, IDENTITY, AND DIGITAL MEDIA vii (David Buckingham ed., 2008) (stating that digital media and networks have recently become a part of everyday life and the common way to produce communication and knowledge, among other things); Alice E. Marwick, *The Public Domain: Social Surveillance in Everyday Life*, 9 SURVEILLANCE & SOC'Y 378, 382 (2012) (arguing that social surveillance is different

This Article examines the phenomenon and propriety of the invasion of private data within the context of employment. Is the fact that digital and web tools are easily accessible enough to justify surveillance as permissible? Does the feasibility of an action define and draw the lines between right and wrong or legal and illegal? In this Article, I claim that guiding principles stemming from social rationales, notwithstanding technical capability or economic feasibility, should shape the legal norm and strike a balance between conflicting interests.

"In the past twenty years, businesses and private citizens alike have embraced the use of computers, electronic communication devices, the Internet, and e-mail."[10] The overlap between personal spheres and business life spheres has grown significantly with new technological developments.[11] For example, most, if not all, employees access the Internet from work for personal use, at least occasionally.[12] However, even an innocuous instance of using a work computer to check personal e-mail accounts can trigger complicated legal questions, such as whether employers have a right to monitor workers' usage of resources and whether employees may reasonably expect a modicum of privacy in their personal e-mails.[13] In the virtual spaces of the Internet and its ilk, it is difficult to determine the border between workplace property and private domains. Moreover, what is generally accepted as standard means of communicating has changed drastically in just the past two decades with the rise of cellular technology and smart phones. In today's digital age, people (including job applicants and employees) rely on the virtual space for essential as well as other types of communications and use e-mail, text messaging or Short Message Service (SMS), social networks, video tools such as Skype, chat applications, and other media to keep in touch. Many employees today carry the newest portable digital devices, such as mobile phones, tablets, portable computers, or digital rings, wherever they go, including to work (where they can use these devices, when necessary, via the employer infrastructure). Furthermore, employees who spend a tremendous portion of their waking time at the workplace often have no other practical option

---

from traditional surveillance (i.e., by the government) in three ways: power, hierarchy, and reciprocity).

10. *Stengart*, 990 A.2d at 654.

11. *Id.* at 654–55.

12. *Id.* at 655.

13. *See id.* (opining that the modern workplace and technology present novel questions regarding privacy and confidentiality).

than to use their employers' virtual spheres to access basic means of communication, either by visiting social networks or writing e-mails. Employees should not be punished for normative behavior when working long hours by losing their privacy entirely.

In the digital era, there is a tremendous potential for employees' use of virtual spheres to put individuals at risk of compromising their own privacy by exposing themselves to present or future employers. The discussion of privacy within virtual spheres is unsurprisingly broad and perhaps even unlimited as it can embrace many venues and means of employee monitoring.[14] One of the most common violations of employee privacy that has recently increased dramatically is the tracking of private information posted about employees on social networks, either by employees themselves or by a third person, as this Article will discuss in detail.

This Article addresses whether applicants and employees who actively participate in the virtual world and communicate with others actually waive their right to data privacy when it is in any way accessible to their employers. In other words, should the law shield an applicant's and employee's right to privacy within the virtual sphere?

I conclude that there are strong justifications for a paradigm in which a sphere of privacy would be delineated within the virtual workplace and provide employees protection from employer intrusiveness. In other words, employees should have a reasonable "private zone" within the wired/digital/virtual premises that is not accessible to their employers—even when they are using corporate network tools or Internet accounts, even during working hours, and even more so while not using their employers' property. I further claim that under the U.S. regime, the application of an "incorrect" or "incomplete" traditional legal interpretation to the virtual era has caused employees in the public as well as the private sector to lose almost entirely their right to privacy within the workplace.

This Article argues that the loss of employees' privacy rights under the present U.S. legal realm within virtual workplaces neither serves a desirable psychological result nor is well justified by other theoretical rationalizations and, hence, is not inevitable. Securing a "private zone" for U.S. employees, a concept adopted by several other legal

---

14. For example, employers can intervene in employees' private means of communication by tracking online activity through surveillance of web postings or by tracking employees' locations using the Global Positioning System (GPS) or voluntary social media "check-ins" in addition to reading private text messages in e-mail accounts or mobile phones and other devices.

regimes, is justified by a bundle of psychological theories that can be concisely described as the "balloon theory" ("magnet field theory"), a theory encompassing the importance of a private sphere that constantly and permanently surrounds a persona wherever one goes, including within the public domain and digital spheres. Studies have shown that providing "private zones" fosters a sense of responsibility and accountability and, consequently, improves employee productivity.[15] This theory is consistent, but not identical, with laws and court decisions in some jurisdictions outside of the U.S. that have found different venues to secure employees' privacy rights (i.e., European Union (E.U.) regulations).[16]

Some scholars have discussed the question of privacy in the digital sphere in general[17] and in social networks in particular.[18] Other scholars have addressed the question of privacy at the workplace.[19] Most of the works are descriptive, revealing the new virtual spheres and pointing out emerging problems. Some of the scholars have justified and supported employers' usage of information posted by employees. For example, some have explained that using this

15. *E.g.*, CONNOR MILLIKEN, WORKPLACE PRIVACY AND EMPLOYEE MONITORING: LAWS AND METHODS 4–6 (2012) (reporting on several negative consequences for companies and employees following monitoring of employees in workplaces, such as stress and other psychological symptoms that can lead employees to be unable to work); *see also* Laura Pincus Hartman, *The Rights and Wrongs of Workplace Snooping*, 19 J. BUS. STRATEGY 16, 18 (1998) (discussing critiques of workplace monitoring that suggest monitoring employees leads some employees to suffer' psychological and physical problems, such as: stress and tension, anxiety, anger, tiredness, boredom, and depression).

16. *See infra* Part IV.B.5 (analyzing the European approach to privacy in the workplace).

17. *See, e.g.*, DANIEL J. SOLOVE ET AL., PRIVACY, INFORMATION, AND TECHNOLOGY 40 (2006) (explaining that a person's privacy consists of secrecy, anonymity, and solitude); Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 549, 554–56 (1999) (suggesting that the Internet raises unique privacy issues).

18. *See, e.g.*, Katrin Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment*, 24 RUTGERS COMPUTER & TECH. L.J. 1, 51–52 (1998) (stressing the importance of controlling one's online privacy to meaningfully engage in online social interactions).

19. *See* Patricia Sánchez Abril et al., *Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee*, 49 AM. BUS. L.J. 63, 64 (2012) (describing the thin line between private and professional communications while employees are at work and using employer-provided Internet connections or devices); Paul M. Secunda, *Privatizing Workplace Privacy*, 88 NOTRE DAME L. REV. 277, 279–81 (2012) (questioning whether public-sector and private-sector workers deserve the same level of privacy at work); Lisa Smith-Butler, *Workplace Privacy: We'll Be Watching You*, 35 OHIO N.U. L. REV. 53, 53 (2009) (mentioning that when people voluntarily post information on the Internet, they are often surprised at negative reactions from employers).

information in the screening stage provides greater benefits and efficiencies than the old tools such as resumes and interviews as they give employers a more honest and candid look at applicants.[20] Not one of these scholars, however, has justified privacy rights in virtual postings or explained that despite this de facto waiver of privacy in online posts, most users' interest in protecting their data is legitimate. This Article suggests that privacy rights in data posted on social networks by employees *do* exist.

This Article not only argues for a more balanced approach to employee privacy, but it also suggests a new desirable model for policymakers to adopt. This solution, *inter alia*, should be part of the current governmental and policy discourse about privacy protection within the workplace. The Article concludes with several suggestions for effectively implementing and encouraging workplace privacy in this global digital age. Accordingly, I conclude that we should reconsider the tests relating to privacy in order to secure a "private zone" within the virtual workplace. A new and necessary policy may implement other new tests or make use of existing tools, such as the

---

20. *See, e.g.*, ANDREA BROUGHTON ET AL., THE USE OF SOCIAL MEDIA IN THE RECRUITMENT PROCESS 19–23 (2013), *available at* http://www.acas.org.uk/media/pdf/0/b/The-use-of-social-media-in-the-recruitment-process.pdf (detailing the benefits that employers receive when they use social media to recruit, such as saving on recruitment costs, targeting specific groups, fostering realistic job expectations, and improving external communications); Victoria R. Brown & E. Daly Vaughn, *The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decisions*, 26 J. BUS. & PSYCHOL. 219, 220 (2011) (advising that even small businesses can use this method because social media screening is inexpensive); Saby Ghoshray, *The Emerging Reality of Social Media: Erosion of Individual Privacy Through Cyber-Vetting and Law's Inability to Catch Up*, 12 J. MARSHALL REV. INTELL. PROP. L. 551, 559 (2013) (noting the importance of respecting applicants' privacy while also highlighting the usefulness of searching a candidate's "digital footprint"). *But see* Donald H. Kluemper, *Social Network Screening: Pitfalls, Possibilities, and Parallels in Employment Selection*, *in* SOCIAL MEDIA IN HUMAN RESOURCES MANAGEMENT 1, 11 (Tanya Bondarouk & Miguel R. Olivas-Luján eds., 2013) [hereinafter Kluemper, *Social Network Screening*] (relaying that applicants are more comfortable with selection approaches, such as interviews and tests, and predicting that if applicants become aware that employers have screened their social network profiles, applicants may turn away from those organizations); Ann Marie Ryan & Robert E. Ployhart, *A Century of Selection*, 65 ANN. REV. PSYCHOL. 693, 698, 704 (2014) (explaining that new data sources, such as social media, can help with information validity and quality); Juan M. Madera & Wen Chang, *Using Social Network Sites to Investigate Employees in the Hospitality Industry* 2 (Int'l CHRIE Conference-Refereed Track, Paper No. 20, 2011), *available at* http://scholarworks.umass.edu/ refereed/ICHRIE_2011/Wednesday/20 (reasoning that using social networking sites instead of traditional screening methods to select employees is inexpensive and easy).

"Least Invasive Means" (the "Proportionality Analysis"), rather than abrogate employees' privacy rights, which would have major implications for employees and, therefore, for workplaces.

In the first Part, this Article describes the virtual sphere inhabited by employers. It then focuses on the drawbacks of screening data about employees and applicants, followed by a discussion of psychological perspectives on privacy within the workplace. The psychological discourse further refines the distinction between tangible and virtual workplaces, presenting theories that can be concisely described as the "balloon" or the "magnet field" theory. This theory provides for a private sphere that constantly and permanently surrounds the persona wherever one goes, including within the public domain, the digital spheres, and the employer's "kingdom." The next Part briefly describes the American legal norm, leading to the introduction of a contrasting attitude from a different legal system. This Part suggests policymakers rethink the current U.S. regime and recommends alternative legal tools they should adopt. The Article concludes with a discussion of a new trend in recent U.S. court decisions to protect employees' and applicants' privacy rights. New legislation preventing employers from requesting employees' passwords to social network accounts, as well as certain court decisions reflecting the creation of private zones within the virtual spheres of workplaces, supports this study's conclusion.

I. SOCIAL NETWORKS: A VIRTUAL SPHERE INHABITED BY EMPLOYEES

A. Preface

Social networking sites have emerged as a rich source of candidate information with the tremendous number of online profiles providing users a forum for interacting through a variety of outlets, including, but not exclusive to, wall posts, tweets, hashtags, picture tagging, and the ability to share pictures, videos, and music.[21] Facebook, one of the most commonly used social networks today, is a website that allows its users to create individualized profiles where they can share status updates, photos, wall posts, and more.[22] Users commonly provide personal private data when they create their social

21. *See* Lockhart, *supra* note 1, at 3–4 (illustrating that a candidate's interactions on social media can help reveal her true personality).

22. *See id.* (suggesting that Facebook profiles provide a degree of individualization that is often a more accurate illustration of candidate's' personal characteristics than are traditional employee-seeking methods, such as interviews or resumes).

networks' profiles, such as: their names, leisure habits, party and drinking habits, gender, age, sexual preference, parenthood or relationship status; details about their friends, race, language, location, education, and work history; comments reflecting their inner thoughts, views, and attitudes; and other personal data.[23] Employer use of this data can be contrary to anti-discrimination laws.[24] The public can easily access much of this personal data being posted in virtual spheres.[25]

Today, more than one billion people post information about themselves on social networks; Facebook alone declared 1.23 billion active monthly users as of December 31, 2013.[26] Not surprisingly, employers have devoured this treasure-trove of information about that most valuable and unpredictable commodity: the human resource. Employers review data about potential as well as current employees both in the course of the hiring process and during employment.[27]

Daniel Solove has identified four basic categories of activities that harm privacy interests: "(1) information collection, (2) information processing, (3) information dissemination, and (4) invasion."[28] Policymakers should consider these categories when addressing the boundaries of the permissible regime regarding employer tracking of personal employee data.

Focusing on data posted on social networks, Patricia Sánchez Abril, Avner Levine, and Alissa Del Riego described three ways in which employers are actively screening online employee data: they are "(1) monitoring and surveill[ing] employee social media profiles, (2) evaluat[ing] applicants' social media profiles and online speech

---

23. Jacqueline C. Pike et al., *Dialectic Tensions of Information Quality: Social Networking Sites and Hiring*, 19 J. COMPUTER-MEDIATED COMM. 56, 57 (2013).

24. *See infra* Part II.A (arguing that determining a prospective employee's race, sex, or nationality using social media circumvents Title VII restrictions on asking questions concerning these protected classifications during interviews).

25. *See* Pike et al., *supra* note 23, at 57 (noting that millions of Internet users post personal information on Facebook, Twitter, and LinkedIn); *see also* Rebecca Brown & Melissa Gregg, *The Pedagogy of Regret: Facebook, Binge Drinking and Young Women*, 26 CONTINUUM: J. MEDIA & CULTURAL STUD. 357, 362–63 (2012) (providing examples of real posts by women regarding their drinking habits).

26. Facebook, Inc., Current Report (Form 8-K), at 1 (Jan. 29, 2014).

27. *See* Ghoshray, *supra* note 20, at 558 (noting that a candidate's privacy can now be invaded "at the click of a mouse," thus exposing the intimate details of her private life to potential employers); Pike et al., *supra* note 23, at 57 (discussing the breadth of new information available that can be passively observed by hiring professionals through social media).

28. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 103 (2008) (arguing that privacy has no single definition but rather is a plurality of different things).

in making hiring decisions, and (3) limiting employees' off-duty online activities."[29] In the twenty-first century, both employees and employers use the Internet and, more specifically, social media as substantial tools relative to employment. Employees use these tools while seeking work, whereas employers rely on social media while searching for applicants and gathering information about existing and potential employees.[30] Businesses monitor sites like Facebook and Twitter in search of information that may provide insight about prospective hires, and individuals can use those sites to learn more about what it is like to work at a particular organization.[31]

One of the most problematic and challenging issues relative to the invasion of privacy is corporate tracking of prospective employees and their personal information. The next subsection will focus on this aspect. This infringement of personal privacy starts even before the hiring process begins: many applicants do not even get a chance to make a case for themselves to an inquisitive employer because of this invasion and may never know why they were not hired.

B. Screening Using Social Network Data Prior to Employment

The term "screening" as used by human resource professionals refers to the digital age hiring process.[32] Instead of using old fashioned and inefficient tools such as resumes and interviews, which are under applicants' control, modern hiring managers often rely significantly on information gathered from the Internet without the applicants' awareness or consent.[33] How popular are such screening methods? Research has found that the majority of employers participating in the studies consider online screening a formal part of

---

29. Abril et al., *supra* note 19, at 66–67.

30. *See infra* Part I.B. (discussing the use of social media as a screening function).

31. *See* Laura Lagone, The Right To Be Forgotten: A Comparative Analysis 1, 9–10 (Dec. 7, 2012) (unpublished manuscript), *available at* http://ssrn.com/abstract=2229361 (explaining that both employers and employees view social media as a valuable tool during the hiring process but that this creates a conflict between knowledge and privacy because there is no "right to be forgotten"); *see also* Abril et al., *supra* note 19, at 69 (noting that employers continue to monitor employees' online activities despite evidence of adverse effects).

32. *See, e.g.*, Raluca Druta, *Cream.HR's Solution to Today's Recruiting Challenges*, TECH. EVALUATION CENTERS (Oct. 3, 2013), http://www.technologyevaluation.com/research/article/CreamHRs-Solution-to-Todays-Recruiting-Challenges.html (suggesting that hiring professionals should screen candidates online at the beginning of the hiring process and before reviewing resumes).

33. *Id.*

their hiring process.[34] Sixty-three percent of U.S. recruiters surveyed have rejected applicants due to online content found in a non-business context.[35] Some companies build candidate profiles for employers using information on social networks as well as blogs, shopping lists, participation in events, and memberships in different organizations.[36]

One study examined the extent to which social networks influence hiring managers in their decision making.[37] The study demonstrated that a vast majority of the managers who responded use social networking for recruitment.[38] A similar majority, seventy-three percent, either agreed or strongly agreed that social networking websites provide meaningful insight into prospective employees.[39] Moreover, nearly sixty-four percent of managers surveyed indicated an interest in using social networking sites for recruitment purposes.[40] However, respondents were almost evenly split as to whether a rejected applicant has a right to know or should be informed about the weight afforded to online content in deciding not to extend a job offer.[41] In general, survey participants believed that content on social networking sites provides meaningful information about potential workers.[42] Accordingly, online

34. Lockhart, *supra* note 1, at 1 ("An overwhelming eighty-nine percent of employers are now using social media sites as a means of researching job applicants throughout the interviewing process.").

35. *Id.* at 7.

36. Companies like Social Intelligence Corp. offer employers a "solution" for applicant assessment and staff monitoring with products that provide a "[c]omprehensive picture of an applicant's complete publically available online presence" and "[m]onitoring for enforcement of company policy and protection against insider threat." *Employment Background Screenings*, SOC. INTELLIGENCE, http://www.socialintel.com/products-and-solutions/employment.html (last visited Sept. 1, 2014).

37. *See* Keri Cook, Social Recruiting: The Role of Social Networking Websites in the Hiring Practices of Major Advertising and Public Relations Firms 9–10 (Spring 2012) (unpublished B.A. thesis, Liberty University), *available at* http://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=1317&context=honors ("Twenty-five major advertising and public relations firms were selected as a sample of the entire population of such companies. The criteria for selection included a minimum annual revenue and international status . . . .").

38. *Id.* at 13.

39. *See id.* at 21 (reporting that twenty-seven percent of respondents strongly disagreed or had a neutral reaction to this statement).

40. *Id.* at 13–14.

41. *See id.* at 19–20 (showing that results were scattered between those who strongly disagreed, disagreed, neither agreed nor disagreed, agreed, and strongly disagreed).

42. *See id.* at 12–13.

recruiting is likely to replace more traditional methods of recruiting through in-person and print ads.[43]

Addressing management and legal issues associated with using social media as a tool for recruitment and personnel screening, Ross Slovensky and William Ross concluded that such use of social networking sites offers value to organizations, which can gain a lot of information about applicants by either replacing or supplementing other information, such as a resume.[44] As a screening mechanism, social media could help alleviate legal concerns about potential "negligent hiring" claims. Stating no concern about possible ramifications of data *collection*, the authors did name legal considerations pursuant to the *use* of such data as a main disadvantage, advising that companies review their policies and adjust them to comply with any applicable law.[45]

Adding to the discourse, Jacqueline Pike, Patrick Bateman, and Brian Butler have explained why screening is so attractive to employers and discussed some risks of using information mined from social networking websites.[46] They pointed out that using social network data is advantageous because applicants are aware of neither the process nor the outcomes.[47] Most traditional screening and hiring methods use interactive observation tools such as resumes and formal interviews.[48] The main drawback of these approaches is that

---

43. *Id.* at 5 (reporting that some scholars have "predicted that online recruitment efforts will continue to replace more traditional methods such as job fairs, newspaper ads, word of mouth, and [on-]campus recruiting").

44. *See* Ross Slovensky & William H. Ross, *Should Human Resource Managers Use Social Media to Screen Job Applicants? Managerial and Legal Issues in the USA*, 14 INFO 55, 58 (2012) (concluding also that social networking sites offer employers a comprehensive view of applicants and help employers avoid "negligent hiring" (internal quotation marks omitted)).

45. *See id.* at 63–65 (advising that managers can devise policies that provide the firm with appropriate information while respecting applicant privacy and complying with U.S. legal and ethical expectations).

46. *See* Pike et al., *supra* note 23, at 57 (warning that information on social media could be "outdated, incomplete, or even fraudulent" because it has not been formally submitted).

47. *Id.* (arguing that passive observation, such as searching a candidate's social networking profile, is more informative because the candidate is not explicitly aware of the observation).

48. *Cf.* Robert A. Baron, *Self-Presentation in Job Interviews: When There Can Be "Too Much of a Good Thing,"* 16 J. APPLIED SOC. PSYCHOL. 16, 16 (1986) (discussing the self-preparation necessary for in-person interviews); Robert L. Dipboye & Stacy L. Jackson, *Interviewer Experience and Expertise Effects*, *in* THE EMPLOYMENT INTERVIEW HANDBOOK 259, 263 (Robert W. Eder & Michael M. Harris eds., 2d ed. 1999) ("An interviewer seldom acquires information that could not be obtained from the application and resume." (internal quotation marks omitted)).

candidates know these tools are used for screening and are able to strategically craft information for their specific audience (i.e., hiring managers). Employers consider passive observation to be more richly informative when candidates are not explicitly aware that they are being observed by potential employers. Nevertheless, employers have not typically used such passive observation as it is time consuming, expensive, and sometimes simply impossible to conduct. But times are changing: employers can observe social networks passively at relatively little cost and without the candidate being aware of the observation or its focus.[49] Furthermore, since social network data and postings are persistent, searchable, and replicable, social networks offer a rich source for hiring professionals confronted with otherwise limited information for use in assessing the fit between a candidate and an organization.[50]

Another empirical study, which examined the psychometric properties of personality traits (the "Big Five") assessed through social networking profiles, illustrates the enthusiasm for online screening procedures.[51] The results included a number of

49. Danah Boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*, *in* YOUTH, IDENTITY, AND DIGITAL MEDIA VOLUME 119, 120, 125–26 (David Buckingham ed., 2007) (noting that so-called "networked publics" make individuals' information permanent, searchable, easily copied, and accessible by "invisible audiences"); Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 210, 213, 220–22 (2008) (reviewing research on privacy issues inherent in social networking sites).

50. *See* Boyd & Ellison, *supra* note 49, at 220 (discussing how companies gain meaningful information on naturalistic behavioral data by exploring large-scale social media patterns); *see also* Daniel M. Cable & Timothy A. Judge, *Person-Organization Fit, Job Choice Decisions, and Organizational Entry*, 67 ORG. BEHAV. & HUM. DECISION PROCESSES 294, 294–95 (1996) (focusing on the importance of person-organization fit and how certain perceptions of fit are determined).

51. Donald H. Kluemper et al., *Social Networking Websites, Personality Ratings, and the Organizational Context: More Than Meets the Eye?*, 42 J. APPLIED SOC. PSYCHOL. 1143, 1149 (2012) [hereinafter Kluemper et al., *Social Networking Websites*] (presenting findings that suggest social networking data provides consistent, accurate measures of personality traits and could be used to predict job performance and "hirability"); *see also* Donald H. Kluemper & Peter A. Rosen, *Future Employment Selection Methods: Evaluating Social Networking Web Sites*, 24 J. MANAGERIAL PSYCHOL. 567, 573–75 (2009) (presenting another study demonstrating the usefulness of social networking websites for predicting future job performance). The study used sixty-three judges and six subjects and accumulated a total of 378 ratings. Kluemper & Rosen, *supra*, at 573. The results revealed that the judges were consistent in their ratings of the subjects' "Big Five" dimensions of personality, intelligence, and global performance and were able to differentiate between the top and low performers based on their Facebook profiles. *Id.* at 575. The results of the study suggested that social networking sites might be more reliable than other forms of personality assessments,

conclusions regarding the reliability, consistency, and validity of candidate ratings based on social network profiles, finding, *inter alia*, that such ratings correlated with job performance, hirability, and academic performance criteria and that the magnitude of these correlations was generally larger than for self-ratings.[52] The study suggested that social networks might provide useful information for an organization but that those organizations must consider the limitations posed by various legal and ethical issues.[53]

Indeed, the hiring process is challenging because a lack of quality information does limit the discovery of a candidate's true nature, potentially leading to adverse consequences. "Lost productivity, wasted time, lower morale, and disruption for clients . . . are just a few of the negative consequences of hiring the wrong people."[54] While social networks are potentially useful sources of information, the information they provide is not submitted by candidates through any formal established application process. As a result, the information may be outdated, incomplete, or even fraudulent. This creates a tension around the quality of social network information: social networks may often be a rich resource, but the possibility of inaccurate information reduces the information's reliability, increasing the need for employers to make judgments about its quality. This is part of a larger emerging trend in which employers must either demonstrate "information self-sufficiency" or take responsibility for making determinations about a candidate's quality based on unmediated information. Although scholars have demonstrated a growing awareness of the importance of social network information in employment contexts, the relevant literature has largely been limited to anecdotal accounts and speculative discussions of how social networks might be used.[55]

---

such as interviews or resumes, because candidates are more truly themselves on Facebook than in professional settings. *Id.* at 570. Facebook reveals enough information about a person's interaction with others and personal information to offer a fairly accurate illustration of an individual's' personality. *Id.*

52. *See* Kluemper et al., *Social Networking Websites*, *supra* note 51, at 1148–49 (concluding from the study that ratings from social networks correlate with a person's job performance and "hirability," meaning social networks are a useful tool for hiring).

53. *See id.* at 1164 (noting that one legal issue is that while employers cannot ask questions in interviews regarding their race, religion, sexual orientation, or marital status, employers can often determine these characteristics through social media).

54. Pike et al., *supra* note 23, at 56 (adding that the cost of replacing a bad hire ranges from twenty-five to five hundred percent of that employee's salary).

55. *See* Slovensky & Ross, *supra* note 44, at 55–56 (stating that even though social networks have become a popular writing topic, there is a lack of academic writing on

Pike, Bateman, and Butler, while not challenging employers' data gathering at all, declared their concern regarding the quality that results when hiring professionals use social network information. They pointed out that a lack of quality information inherent in hiring decisions based on social network data makes it impossible to discover the true candidate ability prior to employment.[56]

While risks exist in using social network data, Donald Kluemper nonetheless found the practice of using LinkedIn or Facebook to select or reject candidates to be widespread among hiring managers.[57] As an emerging employment selection tool, screening via social networking sites demonstrates potential as a rich source of applicant information,[58] but research has struggled to keep up with the rapid changes in social media sites.[59] Therefore, Kluemper offers human resources practitioners a wide range of considerations toward developing an effective social network screening policy while also making the case for academics to pursue further research in this nascent area.[60]

Undoubtedly, the hiring process has changed dramatically since the advent of social networks. The position of courts regarding the validity of employers monitoring and screening would, of course, be very important. However, since the process of social network mining for insights on job applicants remains unknown and therefore non-examinable, there can hardly be cases on point for this issue. However, tracking data posted on social networks does not end with the hiring process. Instead, employers review data posted by and about employees throughout the employment period. This phase will be the focus of the next subsection.

---

the advantages and disadvantages of human resource managers accessing applicants' social media information and seeking to fill that void).

56. *See* Pike et al., *supra* note 23, at 57 (categorizing three types of information quality issues, including accessibility, contextual, and intrinsic quality issues).

57. *See* Kluemper, *Social Network Screening*, *supra* note 20, at 2 (sharing that in a 2009 CareerBuilder.com study, forty-five percent of employers used social networking websites to research job applicants and that this was a rising number).

58. *See id.* (explaining that social media screening provides valuable information to employers such as the applicants' communication skills, creativity, awards, and accolades).

59. *See id.* (labeling the use of social networks in hiring decisions as a "rare moment in staffing research" and "a new paradigm to research").

60. *See id.* (noting that this issue is of interest to many disciplines, including psychology, management, law, and information technology).

C. Tracking Employee Data on Social Networks During Employment

The practice of tracking information posted by employees on their private social network accounts gives rise to even more legal questions vis-à-vis screening because it affects working conditions and may lead to dismissals and loss of positions. Employees have recently brought cases—in addition to those described in the first part of this Article—over dismissals or denials of employment benefits due to data posted on social networks. For example, Bernadet Guevarra, a nurse employed at a California hospital, was fired after posting a Facebook status from her home to various "friends" in which she virulently complained about having to work on her birthday and on holidays.[61] When one of her Facebook "friends" (a co-worker) shared the content of these posts with her employer, Guevarra, who had received no prior notice or disciplinary actions, was first placed on administrative leave and then terminated the following day.[62] Not only was she discharged, but she was also denied unemployment benefits—all because of her Facebook post.[63] An administrative law judge and an appellate board reviewed Guevarra's posts; both found the posts were a breach of her obligations to her employer and therefore constituted misconduct connected with employment.[64] Guevarra had violated the employer's policy because her posting was visible beyond what could be considered "a private communication conducted outside of work . . . such as one made in confidence to a family member."[65] Consequently, the U.S. District Court for the Northern District of California granted the employer's motion to dismiss with prejudice for lack of subject-matter jurisdiction.[66] The

---

61. Guevarra v. Seton Med. Ctr., No. C 13-2267, 2013 WL 6235352, at *1 (N.D. Cal. Dec. 2, 2013) ("Instead of spending my birthday celebrating, I will be working all night cleaning up feces. . . . Thanks to the [administrator], . . . not only am I working Mothers [sic] Day, my birthday and my anniversary. And this Friday, I will be getting the smallest paycheck I had in 12 years due to the 17 percent pay cut we had to endure."). The nurse also threatened her supervisors in her Facebook posts. *Id.*

62. *Id.*

63. *Id.*

64. *See id.* at *1–2 (reasoning that Guevarra's Facebook post was more than a "hotheaded remark" because she had published it to a broad audience, including co-workers).

65. *Id.* at *2 (labeling Guevarra's Facebook statement as "incendiary, derogatory, and serv[ing] to undermine the morale of the employer's workforce").

66. *Id.* at *8.

decision, while discussing various legal questions including freedom of speech, did not mention any privacy issues.[67]

Other courts have also avoided discussing privacy rights when they have validated actions against employees based on the employees' Facebook posts, even those posts believed to be semi-private (thought to be exclusively available to "friends" or private groups). For example, a U.S. Court of Appeals for the Seventh Circuit decision written by Judge Richard Posner upheld the lower court's judgment in favor of a daycare center that had dismissed an employee on the basis of hostile and profane Facebook posts.[68] The Seventh Circuit did not challenge the tracking of data on social networks. The court stated that even if the daycare center's reason for checking the employee's online profile was not a good one, the reason was irrelevant "if the [c]enter honestly believed that the [employee] wrote the post."[69]

The U.S. Court of Appeals for the Eleventh Circuit reached a similar result for the public sector during the same time period. A police department employee sued the police department, claiming that she was not promoted in retaliation for Facebook postings in which she had criticized her colleague for unethically interfering with her investigation of a person she had arrested for fraud and financial identity theft.[70] Although her Facebook page was set to private, the court reasoned that her "friends" were able to distribute the comment beyond the intended audience.[71] After reviewing the Facebook post, the police department launched an investigation, alleging that the employee had violated the department's rule requiring "any criticism of a fellow officer [to] 'be directed only

---

67. *See id.* at *7 (opining that the First Amendment cases Guevarra cited were not helpful to her case because they involved state actors or private actors who had opened their property to the public). Comparatively, in *Edmonds Dental Co., Inc. v. Keener*, an employee who was fired for using Facebook on company computers—in violation of a company policy that prohibited using company computers for personal business—was allowed to receive unemployment benefits in Missouri. *See* 403 S.W.3d 87, 88–89 (Mo. Ct. App. 2013) ("The conduct for which Mr. Keener was discharged included using company computers to make posts on Facebook, perform job searches, and otherwise conduct his own personal business."). But, he was not discharged based on the content of the posts themselves. *See id.* at 88 (remanding the employer's appeal due to a question of fact regarding the employment).

68. Smizer v. Cmty. Mennonite Early Learning Ctr., 538 F. App'x 711, 713–15 (7th Cir. 2013).

69. *Id.* at 714.

70. Gresham v. City of Atlanta, 542 F. App'x 817, 818 (11th Cir. 2013) (per curiam).

71. *Id.*

through official department channels.'"[72] The court upheld the lower court's grant of summary judgment for the police department, finding that the police department's legitimate interests in requiring that any employee grievances be addressed internally and privately outweighed the employee's First Amendment rights.[73]

Further, in *Ehling v. Monmouth-Ocean Hospital Service Corp.*,[74] the U.S. District Court for the District of New Jersey commented that "[p]rivacy in social networking is an emerging, but underdeveloped, area of case law" with consistency in case law at two extremes, one that allows Internet users *no* expectation of privacy, and the other that says "there *is* a reasonable expectation of privacy for individual, password-protected online communications."[75] The court did not mention, however, the option of protecting privacy in social network publications up to a certain level.

II. TO READ OR NOT TO READ? THE PROBLEMS WITH EMPLOYER INVASION OF EMPLOYEE DATA IN SOCIAL NETWORKS

Given the apparent advantage that employers seem to have over employees both with respect to controlling the screening process and in courts, the clash between privacy and the Internet generates a basic set of legal concerns. Interesting but problematic interconnections in relation to employment and social networks can arise any time before, during, or after employment. These interconnections include the following.

A. Disregarding Antidiscrimination Norms

This subsection illustrates one of the main problems that screening bears: obliviousness to antidiscrimination laws. Antidiscrimination laws at workplaces are obvious, accepted, and well adopted legal norms in the U.S. Employers cannot ask job applicants questions about their sexual orientation, number of children, their religion, or other discriminative factors, and they cannot base a decision in the

---

72. *Id.*

73. *Id.* at 819–20.

74. 872 F. Supp. 2d 369 (D.N.J. 2012).

75. *Id.* at 370, 373–74. In this case, a New Jersey hospital employee prevailed in her suit alleging common law invasion of privacy where her employer had demanded that 'her co-worker, who had "friend" privileges to 'her Facebook profile, display the profile to management. *Id.* at 370. The employer subsequently took disciplinary action against the employee on the basis of statements the employer found in her Facebook profile and which the employee had believed were protected by high privacy settings. *Id.* at 370–71.

workplace on these factors. Nevertheless, employers can easily obtain this data in the digital sphere and implement biased and discriminative factors within decisions relevant to job applicants and employees.

Over many years, U.S. law has established and shaped the framework for antidiscrimination laws in the context of workplaces. Under Title VII of the Civil Rights Act of 1964, employers are prohibited from discrimination based on religion, sex, nationality, or race.[76] Many employer actions and measures are limited and even forbidden under Title VII and other antidiscrimination laws. The hiring process is no exception. Therefore, employers cannot ask applicants or use factors such as race, sex, or nationality, but employers can easily discern much of this protected information from data posted on social media, including individual profile pictures.[77]

Moreover, employers cannot avoid making value judgments about potential employees, which leads to inadvertent discrimination. Research shows that most employers form biases when they view inappropriate content on social networking sites; nearly half of employers discriminate against individuals whose social networking content suggests they abuse alcohol or drugs.[78] Exposure to this social network data is irreversible. Once a hiring manager sees a profile photo, for instance, it may be very difficult to disassociate that image from the applicant's name. Use of social media in the hiring process blurs the lines of existing employment regulations to the point where they have become ineffective.[79]

Because of its unique social features, using social networks as databases for information about job applicants and employees is even worse from an antidiscrimination law point of view. People use social networks mainly for social purposes. According to Joy Peluchette and Katherine Karl, "students make a conscious effort to portray themselves with a certain light on Facebook."[80] In other words,

---

76. Civil Rights Act of 1964, Pub. L. No. 88-352, § 703(a), 78 Stat. 241, 255 (codified as amended at 42 U.S.C. § 2000e–2(a) (2012)).

77. *See* Cook, *supra* note 37, at 8 (highlighting that every action by human resources is subject to Title VII, including the hiring process).

78. Lockhart, *supra* note 1, at 1.

79. *See* Cook, *supra* note 37, at 9 (advising that because the use of social media in hiring decisions is still a gray area, applicants should be especially cautious of what they post).

80. *See* Lockhart, *supra* note 1, at 7 (reporting that students create their desired images using both comments and photos); Joy Peluchette & Katherine Karl, *Social Networking Profiles: An Examination of Student Attitudes Regarding Use and Appropriateness of Content*, 11 CYBERPSYCHOLOGY & BEHAV. 95, 96 (2008) (reporting that "[m]ales [are] significantly more likely than females to place self-promoting and risqué pictures

individuals' specific purposes guide the types of material they post online. For example, those who aim to present a professional image are unlikely to post the same type of material as those who see themselves as sexual, wild, or inappropriate and who tend to upload "problematic" information (from the employer perspective).[81] Peluchette and Karl found that "approximately fifty percent of the students in the study "ha[d] profiles that exemplif[ied] a party lifestyle . . . includ[ing] profanity as well as comments and photos involving alcohol."[82] Many students believe that no person who is not a "friend" will read or view their posts and end up posting negative content on Facebook. However, the situation is totally different from this assumption. As stated previously, studies reveal that sixty-three percent of employers who declared they use social networks in the hiring process decided not to hire a person based on what they found on a candidate's social networking site.[83]

Antidiscrimination rules trump screening habits and workplace policy. Employers should be required to follow antidiscrimination laws when searching and monitoring data in social networks about applicants and employees. In other words, in accordance with antidiscrimination laws, screening should not include discriminative factors, and decisions should not rely on discriminative factors. The resulting legal complications from making snap judgments based on social media profiles necessitates employers taking extra precautions to ensure they do not violate any laws relating to their industry or geographic location. Companies should ideally establish standard hiring procedures with reliable techniques for quality candidate selection, thus avoiding the need to turn to social media.[84]

To conclude, with decisions based on and biased by prejudice and unfair judgment, the current situation bears the risk of illegal discrimination.

B. Misleading Social Network Privacy Policies: Intention and Expectation of Privacy

The main question that this Article addresses is the contradiction between, on one hand, social network users' waiver of privacy by

---

or comments (involving sex or alcohol) . . . whereas females [are] significantly more likely than males to post romantic or 'cute' pictures and/or information").

81. Lockhart, *supra* note 1, at 7.

82. *Id.* (citing a 2008 study by Peluchette and Karl).

83. *Id.*

84. Cook, *supra* note 37, at 9.

posting on the web and, on the other hand, their claimed right to privacy in this data as well as the importance of maintaining private zones in public. Apparently, the discourse about privacy in data posted on social networks is much more complicated. The misleading and vague privacy policies of social network websites is primarily influenced by their business method, which is to commercialize the private information posted by users to other commercial or governmental entities.[85] Certain social network corporations purposely post an unclear and flexible privacy policy and frequently change the policy.[86] This gives great latitude to the company, enabling it to promote its own interest in gaining profit by exploiting users' unprotected privacy.[87] A lack of transparency regarding commercialization of personal data by social network entities encourages users to post personal data.[88] The term "privacy policy" in itself creates a false illusion of privacy among users who believe they can protect personal data. For example, student members of the Queer Chorus at the University of Texas, who kept their Facebook accounts private, had their sexual preferences

85. *See* Avi Goldfarb & Catherine Tucker, *Online Advertising*, 81 ADVANCES COMPUTERS 289, 294 (2011) (noting that social network websites, particularly Facebook, allow advertisers to target consumers more effectively); Sharon Hannes & Lital Helman, *Corporate Responsibility of Social Networking Platforms* 3, 5–11, 13, 16 (forthcoming) (indicating that social networks use personal data for selling personally tailored marketing messages to commercial entities but keep their privacy policies unclear to encourage users to provide personal data).

86. Facebook, for example, settled a lawsuit brought by the Federal Trade Commission (FTC) that alleged it deceived consumers by repeatedly making users' information public despite having a privacy policy that suggested such information would remain private. *See* Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges that It Deceived Consumers by Failing to Keep Privacy Promises (November 29, 2011), *available at* http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep. *See generally Fact Sheet 35: Social Networking Privacy: How to be Safe, Secure and Social*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/workplace-privacy-and-employee-monitoring#4a (last updated Aug. 2014) (warning that privacy policies are subject to dramatic changes).

87. Hannes & Helman, *supra* note 85, at 12–15 (demonstrating how advertisers use personal data from social networking sites to more effectively target their customer base).

88. *See generally Facebook Privacy*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/facebook (last visited Aug. 4, 2014) (noting that, by preselecting the information a user will share with an application, Facebook encourages users to allow third party to applications access to troves of information).

exposed to hundreds of their Facebook friends when the president of the chorus added them to a public Facebook group.[89]

Information, particularly photographs, posted by a job applicant or by third parties in social networks is usually in a context totally outside of employment, often exhibiting different phases and periods of the applicant's life, such as when the applicant was a teenager or spending time out of the business or educational sphere at parties or on vacation. As applicants for employment, users of social networks do not intend to expose their personal lives to potential employers, yet the unexpected and unintuitive result of creating an account that is not always protected results in combining multiple pieces of information together to paint a holistic picture of an individual. In general, users assume while posting that their data will be exposed only to the group they intend, especially if they are diligent in controlling privacy settings. They do not assume it will be disclosed to third parties such as employers. This issue raises the question of whether social networking corporations should be responsible for taking added precautions to ensure employers do not have access to this data or whether employers should be responsible for exercising restraint. However, as the previously cited cases[90] and scholarship have established, U.S. employers can and do look at employees' social media profiles whether the employees realize it or not.

C. Unequal Bargaining Power

Imagine you are a hopeful job applicant. The employer asks whether you have social network accounts. You know the purpose of the inquiry. Assume you have taken cautious steps to protect information posted by you by making it visible only to "friends." Even though the employer does not ask you for your password, you know that you had better become a "friend" with the employer.[91] Due to the gap in bargaining power between applicant and hiring employer, the employer in this scenario places the applicant in a very difficult position.[92]

---

89. Geoffrey A. Fowler, *When the Most Personal Secrets Get Outed on Facebook*, WALL ST. J. (October 13, 2012), http://online.wsj.com/articles/SB10000872396390444165804578008740578200224 ("The Facebook era, however, makes it possible to disclose private matters to wide populations, intentionally or not.").

90. *See supra* Part I.C (discussing approvals of U.S. courts to dismissals of employees based on their postings).

91. Gerano, *supra* note 2, at 665.

92. *Id.* at 665–66.

That awkward moment might even evolve into something worse upon hiring if the employer demands the password to all of your e-mail and social network accounts. Indeed,

> there's really not much difference between demanding the keys to your apartment and demanding the password to your email or social media account. In both cases, the other party is demanding the right to investigate almost everything about you—who your friends and romantic partners are, what you do when you are not at work or at school, your health concerns, religious activities and political affiliations, and much, much more.[93]

Being aware of this dilemma, Congress and several states have begun passing laws to forbid employers from requesting personal passwords from employees.[94] Will such laws adequately address the problem? Due to the unequal bargaining power, the laws may help but will not cure the entire issue. Job applicants will still face the dilemma of either voluntarily becoming a prospective employer's online "friend" and of exposing their social lives outside of a professional context or of being excluded from the hiring process.[95] Mark B. Gerano examined the extent to which *public* employers may investigate the social media content of a job applicant and also discussed the new legislation about employers' access to passwords. He concluded that in some cases (i.e., with police officers) there should be no restrictions.[96]

Based on the previous studies discussed, recent technological changes have made it easier, faster, and cheaper than ever before for employers to engage in surveillance of their workers. Many employers efficiently use technology to monitor and, more

---

93. Chris Conley, *California Social Media Privacy Laws Give Students, Employees Online Rights*, AM. C.L. UNION (Oct. 1, 2012, 11:15 AM), https://www.aclu.org/blog/technology-and-liberty/california-social-media-privacy-laws-give-students-employees-online.

94. Gerano, *supra* note 2, at 675; *see Employer Access to Social Media Usernames and Passwords*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx (last updated Sept. 28, 2014) (providing descriptions of and links to state laws that, beginning in 2012, have sought to prevent employers from requesting job applicants' passwords). Some states have taken this further. For example, in 2013, the State of Washington enacted legislation banning, *inter alia*, "friend requests" or other access to employee social networking sites by employers. WASH. REV. CODE § 49.44.200 (2013).

95. *Cf.* Gerano, *supra* note 2, at 666 (highlighting a trend in college sports where athletes must "friend" a coach in order to participate in the sport).

96. *See id.* at 667 (arguing that exceptions are appropriate for positions that would merit thorough background checks, such as police officers and prison guards).

fundamentally, to control their employees' behavior at a granular level that was not previously possible. Compounding the problem is the indubitable fact that it is hard in these times of widespread economic distress for employees to take a stand against intrusive monitoring by their employers.[97] As a society, we must consider the idea that adults passively submit to routine surveillance of their activities simply "to hold the jobs they need to pay their bills and provide for their families."[98]

Eventually, information asymmetries might cause a market inefficiency failure.[99] Applicants and employees as social network users are poorly positioned against employers and social network corporations to take a stand for their rights because of bargaining power asymmetry and because they lack information.[100] In addition, applicants and employees neither know nor have ways to find out what personal information employers have gathered or when and how often the employers will use that information.

D. Cognitive Biases: The False Perception of Privacy

What perceptions and expectations do people—especially young people—hold regarding privacy on the Internet? Cognitive biases may serve as the basis of irrational behavior by users who expect privacy in personal data on social networks. For example, the "Optimism Bias" can explain the irrational trust a person can display in third parties relying on an irrational belief that this party would avoid using the users' personal data.[101] Other biases, such as those regarding short-term and long-term risk, loss aversion, or crowd bias, all lead users to fallaciously trust policymakers, social networks'

---

97. *See supra* Part I.A–C (discussing the ubiquity of social networking sites and employers' use of these sites to screen potential employees).

98. Catherine Crump, *Your Boss Shouldn't Read Your Email*, AM. C.L. UNION (July 16, 2012, 5:02 PM), https://www.aclu.org/blog/technology-and-liberty/your-boss-shouldnt-read-your-email.

99. *See* ROBERT COOTER & THOMAS ULEN, LAW & ECONOMICS 47 (4th ed. 2004) (defining information asymmetries as "an imbalance of information between parties to an exchange, one so severe that exchange is impeded").

100. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1250 (1998) (noting that we do not live in a world with "perfect information" or "perfect competition").

101. *See* Christine Jolls et al., *A Behavioral Approach to Law and Economics*, 50 STAN. L. REV. 1471, 1541 (1998) (explaining that over optimism leads people to underestimate risk). *See generally* Daniel Kahneman & Amos Tversky, *On the Psychology of Prediction*, 80 PSYCHOL. REV. 237, 237–38 (1973) (discussing cognitive biases that affect individuals' ability to predict future events).

fairness, and the law, particularly because most imaginations are restricted to current known risks.[102]

E. The Right To Be Forgotten

The recent discussion on the right to be forgotten is relevant to the discourse about screening and monitoring of digital data about job applicants and employees:

> Unlike paper documents that can be discarded easily, "purged" electronic documents may still exist in some sort of archival media where they can stay for an indefinite period of time. Even when archived tapes are removed for reuse and the information has been finally overwritten, such documents may still be recoverable.[103]

The right to be forgotten, meaning a legitimate request for erasing data, is not recognized in the U.S. Users of social networks in the U.S. have no legal right to erase data they make available on social networks. The data remains permanently at the site, even if users delete it, and even after they quit or disconnect from the social network services.[104] The European Court of Justice's decision in *Google Spain SL v. Agencia Española de Protección de Datos*[105] regarding the right of a user (and the duty of Google Spain) to delete irrelevant data reveals a totally different point of view.[106] The case of data

---

102. *See, e.g.*, Ian Weinstein, *Don't Believe Everything You Think: Cognitive Bias in Legal Decision Making*, 9 CLINICAL L. REV. 783, 784 (2003) (discussing the prevalence of cognitive biases and how they affect decision making).

103. Betty Ann Olmsted, *Electronic Media: Management and Litigation Issues when "Delete" Doesn't Mean Delete*, 63 DEF. COUNS. J. 523, 527 (1996).

104. *See* Robert Kirk Walker, Note, *The Right to Be Forgotten*, 64 HASTINGS L.J. 257, 262–69, 270–73 (2012) (arguing that current U.S. laws—such as for intellectual property, defamation, and tort—do not provide proper control over personal data and that the traditional First Amendment freedom of speech should prevail); *see also* Hannes & Helman, *supra* note 85, at 5 (reporting that "data provided on social networks remain with the site permanently"); Lagone, *supra* note 31, at 1 (comparing U.S. and European responses to privacy concerns related to social networking and suggesting that Europe's proposed "right to be forgotten" could be implemented in the U.S. without violating the First Amendment (internal quotation marks omitted)).

105. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065 (May 13, 2014).

106. *Id.* at ¶ 92 (reasoning that the right to privacy prevails when the information is "inadequate, irrelevant[,] or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary unless they are required to be kept for historical, statistical[,] or scientific purposes"); *see also* Jeffery Rosen, *The Right to Be Forgotten*, 64 STANFORD L. REV. ONLINE 88, 91 (2012) (describing the decision's "chilling" consequences on social networks like Facebook as well as on search engines and third parties); Scott D. Goss,

posted by third parties is even worse, as the user cannot, in many cases, delete the data even when aware of its presence.[107]

F. Data Posted by Third Parties

Users of social networks might control their own posts. However, third parties post a lot of written and pictorial data. Users essentially relinquish control over private details about their lives when third parties post personal information to a social network. Thus, employees (or future employees) lose control of private details about themselves. Here, even changing the setting to one of anonymity is not an option.[108]

G. Dignity and Psychological Reasoning

Among other risks and harms caused by invasion to someone's privacy is the detriment to personal traits, such as autonomy, freedom, and dignity. People whose privacy has been invaded and who have had personal information used against them have often experienced mental injury and helplessness.[109] Research suggests

---

Data Protection Law Errors in Google Spain LS, Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez, FUTURE PRIVACY F., http://www.futureofprivacy.org/2014/09/04/data-protection-law-errors-in-google-spain-ls-google-inc-v-agencia-espanola-de-proteccion-de-datos-mario-costeja-gonzalez (last visited Oct. 23, 2014) (identifying several potential legal implementation issues associated with the *Google S.L.* decision, such as that the data does not disappear but just makes the search more difficult, and arguing that Google should not be the "controller" of the process of deleting); Daniel Solove, *What Google Must Forget: The EU Ruling on the Right to Be Forgotten*, LINKEDIN.COM (May 13, 2014), https://www.linkedin.com/today/post/article/20140513230300-2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten (suggesting that the right to be forgotten appearing in the European Court of Justice case is focused on fundamental principle of privacy and raises serious First Amendment questions).

107. Lagone, *supra* note 31, at 8–9 (indicating that a user has to contact the company directly to request the deletion of third-party data). Lagone posits that compliance with such a request effectively turns a purportedly neutral company into a censor. *Id.* at 9.

108. The Facebook privacy policy describes the ripple effect of third party posts, tags, "likes," and other interactive tools. *Sharing and Finding You on Facebook*, FACEBOOK.COM, *available at* https://www.facebook.com/about/privacy/your-info-on-fb (last visited Oct. 23, 2014).

109. *See, e.g.*, Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2087 (2001) (discussing the "sense of violation" Monica Lewinsky must have felt when her private sexual life was "forcibly made public"); *see also* James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 13 (2003) (describing the sense of helplessness that results when strangers collect and have the ability to use private information against an individual).

that, in the workplace, employees who feel their employers have breached their trust may experience emotional distress, feelings of betrayal, anger, and other emotions that affect their overall behavior and sense of loyalty to the organization.[110]

Acknowledging these problems, we have to understand the value behind the right to privacy. The Article thus now turns to a discussion of a psychological approach as the main source of the right and justification for its protection.

III. THE PSYCHOLOGY "BALLOON" OR "MAGNET FIELD" THEORY

A. Introduction

"I felt total incomprehension, I was stunned," said Ms. Paulin, a twelve-year employee of the Swedish home furnishings group IKEA and its Deputy Director of Communications and Merchandising in France when she was forced out of her job after the company was said to have provided her Social Security number, private cell phone number, bank account details, and other personal data to a private detective and then accused her of falsely claiming to be ill.[111] She left the dismissal meeting emotionally disturbed and felt her soul and her dignity had been breached.[112] A few days later, Ms. Paulin attempted suicide.[113]

---

110. *See, e.g.*, Sherri Coultrup & Patrick D. Fountain, *Effects of Electronic Monitoring and Surveillance on the Psychological Contract of Employees: An Exploratory Study*, 19 PROC. ASBBS ANN. CONF. 219, 222 (2012) (presenting several such studies).

111. Nicola Clark, *Revelations that Ikea Spied on Its Employees Stir Outrage in France*, N.Y. TIMES (Dec. 15, 2013), http://www.nytimes.com/2013/12/16/business/international/ikea-employee-spying-case-casts-spotlight-on-privacy-issues-in-france.html?pagewanted=all.

112. *Id.*

113. According to one report of this incident,

> One of the emails from [Ikea France's head of risk management], dated Dec. 11, 2008, was addressed to a private detective, Jean-Pierre Fourès. He was asked to confirm whether Ms. Paulin had traveled to Morocco over the preceding several months and if she owned property there.
>
> Mr. Fourès' reply confirmed both to be true and included a startling attachment: scanned images from Ms. Paulin's passport, showing her Moroccan entry and exit stamps. To obtain those, the court documents show, Mr. Fourès had arranged for someone posing as an employee of Royal Air Maroc to persuade Ms. Paulin to fax copies of her passport in order to claim a free ticket offer. . . . Subsequent messages to the detective also disclosed details of Ms. Paulin's personal bank account.

Id. Furthermore, "The going rate charged by the private investigators was 80 to 180 euros, or $110 to $247, per inquiry, court documents show. Between 2002 and 2012,

IKEA's investigation was not the result of coincidence. It was designed to gain personal information about employees and job applicants, to store the information, and to use it against the employees when necessary.[114]

The abundant diversity of Internet and virtual tools provides more than just a new means of expression. The pervasive use of virtual instruments such as e-mail, Facebook, Twitter, WhatsApp, Skype, and others, combined with the growing popularity of these tools among future employees, reflects a new reality. Access to culture, education, knowledge, and human relationships are conducted primarily by active and constant use of these virtual instruments.

Indeed, digital technology has revolutionized the vehicles of social interaction. Future generations of employees, such as students,

> are cognizant of their reputational vulnerability on digital media but are not willing to sacrifice Internet participation to segregate their multiple life performances. Lacking the technological or legal ability to shield [certain aspects of their lives that might once have been exclusively private], Millennials rely on others, including employers, to refrain from judging them across contexts.[115]

In other words, "[d]espite granting employers access to information about their private lives by participating online, respondents expect that work life and private life should be generally segregated—and that actions in one domain should not affect the other."[116] Furthermore, portable electronic devices are now pervasive and increasingly dominate everyone's life.[117] Some people who are aware of the potential outcomes of a possible violation of their privacy pay a

---

the finance department of Ikea France approved more than €475,000 in invoices from investigators." *Id.*

114. The case caused public outrage in France because it "occurred in a country that, in the digital age," was reported to pride itself on having "elevated privacy to a level nearly equal to the national trinity of Liberté, Égalité and Fraternité." *Id.*

115. Abril et al., *supra* note 19, at 66.

116. *Id.* at 66–67 (describing the paradoxical expectation of privacy among millennial employees—they generally want privacy yet still share personal information online aware it may be available to employers).

117. *See* Michael Z. Green, *Against Employer Dumpster-Diving for Email*, 64 S.C. L. REV. 323, 326 (2012) (arguing that the rise to ubiquity of portable electronic devices—Blackberries, iPhones, iPads, Androids, and etcetera—blurs the workspace with private spaces, blends work-time and private-time, and calls for a re-thinking of traditional distinctions and a new emphasis, not on employees' reasonable expectations but, rather, on employers' reasonableness in monitoring workers). *But see* United States v. Ziegler, 456 F.3d 1138, 1146 (9th Cir. 2006) (finding no objective expectation of privacy in a workplace computer where the employer's policy included monitoring provisions).

price by avoiding any kind of Internet expression, becoming virtually paralyzed, and choosing to stay behind as popular means of communication advance.[118]

Whether employers' common practices of tracking employees' private information within the virtual sphere is desirable can be discussed from several points of view. The following section will focus on the psychological need for privacy.

B. The Psychological Importance of Privacy

Virtual tools play an essential role in the definitions of a person's identity, "self," "self-expression," and "self-identification."[119] Works about intrinsic motivation, from the psychological perspective, reveal that privacy is a notion perceived entirely within a person's consciousness and not in the external world.[120] Therefore, the perceived notion of privacy is equally relevant in virtual spheres as it is in other spheres where it is already recognized. The virtual spheres influence this consciousness of privacy because privacy does not depend on or stem from tangible assets or physical reality. Privacy actually exists within our minds and souls. Privacy is the way we perceive privacy. In other words, privacy is an internal illusion and it is intangible. Social media is also intangible. Thus, it does not make sense to try to think about privacy in terms of tangible spheres only. Quite the contrary, privacy matters might be more important and more suitable to the virtual intangible spheres. Differentiating between tangible and virtual spheres and their legitimate influences on the privacy rights discourse or on an expectation of privacy may be misleading.

Perceiving consciousness as the intermediary between the cause of violated privacy and the psychological outcomes thereof (as has been made in legal literature) justifies the interconnection between the right to privacy (including within a virtual sphere) and important

---

118. Hannes & Helman, *supra* note 85, at 13–15 (describing the future harm of people avoiding posting personal data from a different perspective because of firms that do not internalize privacy matters).

119. Green, *supra* note 117, at 339–40 (quoting City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010)).

120. *See* Mihaly Csikszentmihalyi, *Introduction*, *in* OPTIMAL EXPERIENCE: PSYCHOLOGICAL STUDIES OF FLOW IN CONSCIOUSNESS 3, 10, 17 (Mihaly Csikszentmihalyi & Isabella Selega Csikszentmihalyi, eds., 1988) (describing consciousness as "an informational system that could differentiate among a great variety of stimuli, that could choose certain stimuli and focus selectively on them, and that could store and retrieve the information in a usable way").

values embedded in psychological concepts such as freedom, dignity, autonomy of the persona, selfhood, and human relations.[121]

Scholars and jurists have suggested many definitions of privacy without having settled on any one as the "right one."[122] From a psychological/personhood perspective, privacy is the personal information and emotions that remain personal when the person is exposed in public. It can also be considered the ability of individuals to differentiate themselves or information about themselves and thereby reveal themselves selectively to others. We refer to private "issues" as information that is considered emotionally or personally sensitive or inherently important or special.[123] The levels, boundaries, or content of what is considered private differs among situations, cultures, and individuals but shares basic common themes. One of them is the wish to remain unnoticed or unidentified in the public realm: anonymity.[124]

C. The Balloon/Magnet Field Theory

The sphere of privacy consists of our perceptions about information and emotions. This can be analogized to the concept of an intangible "balloon" (or magnetic field) that always accompanies a person wherever she goes within the public domain, including during perceived or actual interactions with others. The size of the "balloon" differs according to the interaction. When we are with

---

121. *See* SOLOVE ET AL., *supra* note 17, at 40 (citing Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980)); *see also* Gary T. Marx & Sanford Sherizen, *Monitoring on the Job: How to Protect Privacy as Well as Property*, 89 TECH. REV. 62, 63 (1986) ("Privacy is an essential component of individual autonomy and dignity. Our sense of liberty is partly defined by the ability to control our own lives—whether this be the kind of work we undertake, who we choose to associate with, where we live, the kind of religious and political beliefs we hold, or the information we wish to divulge about ourselves.").

122. The most famous definition is "the right to be let alone." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

123. SOLOVE, *supra* note 28, at 34–35 (discussing theories that consider privacy a type of intimacy).

124. *See* Jed Rubenfeld, *Anonymity and the Digital Revolution* 1 (forthcoming) (on file with author) (differentiating anonymity and privacy and pointing out legal difficulties associated with anonymity). *But see* Alessandro Acquisti, *Nudging Privacy: The Behavioral Economics of Personal Information*, 7 IEEE SECURITY & PRIVACY 82, 82 (2009) (noting that "many seek notoriety at the price of embarrassment, a tarnished reputation, or even infamy"); Laura Brandimarte et al., *Misplaced Confidences: Privacy and the Control Paradox*, 4 SOC. PSYCHOL. & PERSONALITY SCI. 340, 345 (2013) (finding that people tend to release more private information when they exercise greater control over its release).

family and friends, we consciously shrink the "balloon" and share part of it with them. When we are with strangers or employers, we save the "balloon" in order to preserve our personal sovereignty. Each person may choose the time, place, and level of disclosure of personal information, experience, and emotion as well as the company before whom such disclosures are made.

The state of privacy is related to the act of concealment.[125] The reality of employees staying at the premises of employment and using the employer's tools—both tangible tools such as computers and virtual ones such as Internet accounts—is a classic example of the balloon theory in action: where the need to protect privacy is generated by a situation or encounter. Persons differ from one situation to another.[126] Different sets of social norms control distinct social settings.[127] Thus, among friends and family, one acts according to one set of social behaviors, whereas the same behavior is not acceptable in a different setting and may be subject to sanction for visible deviation from patterned role behavior.[128] While drinking with friends or at a festive celebration is welcome, drinking at the workplace or while driving is typically punished.

Today, the Internet has blurred the borders between social contexts and mixed these different situations, creating a blend, and sometimes a clash, of rights and wrongs. It is acceptable to take pictures with friends at a costume party, but once posted on the web, those same pictures can bring about a person's dismissal. A person should have adequate freedom to build the "self" and to choose how that self will be represented. Similarly, this choice requires that individuals be able to limit others' access to aspects of their online persona.[129]

In contrast, one of Jed Rubenfeld's main claims is that privacy exists within a private sphere.[130] This idea is based on the traditional

---

125. *See* Brandimarte et al., *supra* note 124, at 340 (describing privacy decision making as suboptimal and as having "perverse effect[s]," causing individuals to reveal less in less risky situations and reveal more when such revelations could be risky).

126. Shlomit Yanisky-Ravid, *Will the Wolf Dwell with the Lamb? Psychological Relationships in the Workplace*, in LIBER AMICORUM ELISHEVA BARAK-USSOSKIN 233, 235–38 (Guy Davidov & Guy Mundlak eds., 2012).

127. Sidney M. Jourard, *Some Psychological Aspects of Privacy*, 31 LAW & CONTEMP. PROBS. 307, 308 (1966).

128. *See id.* (noting that deviation from social roles may result in criminal punishment, social banishment, or a label of "mentally ill").

129. *See* SOLOVE ET AL., *supra* note 17, at 40.

130. Rubenfeld, *supra* note 124, at 3 & n.5 (differentiating between privacy in private and the lack of privacy in public).

distinction that led to the famous U.S. Supreme Court statement in *Katz v. United States*[131] that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[132] I suggest that the real meaning of privacy does not exist when others are not around, as the meaning of privacy and the need for privacy is established when other people may be perceived as invading into this conceptual privacy sphere. This invasion can be physical, such as seizure, scrutiny, or rape, but most of the time it happens when others find personal information (e.g., surveillance or tracking of personal data) or ask personal questions (e.g., investigation). Privacy, then, is the outcome of a person's wish to withhold from others certain knowledge as to her past, present, or future.[133] The concept of privacy as intrusion upon seclusion is too narrow and inaccurate and misses the more conflicting and more common intrusion that, according to my claim, should be protected.[134] Therefore, the classic traditional definition of privacy as "the right to be let alone"[135] should be adjusted to recognize a protected sphere against disclosure of certain facts within any public realm.[136] This shift from the state of merely alone to the protection of one's personality explains and justifies privacy in the virtual spheres.[137] "Although the home is the quintessential 'private' space

131. 389 U.S. 347 (1967).

132. *Id.* at 351.

133. Jourard, *supra* note 127, at 307 (noting "[t]he wish for privacy expresses a desire to be an enigma to others or, more generally, a desire to control others' perceptions and beliefs" by monitoring the exposed information about one's self).

134. RESTATEMENT (THIRD) OF EMPLOYMENT LAW § 7.01 cmt. a (Tentative Draft No. 5, 2012) ("At the core of the privacy concern is information about the person—information that the person wishes to shield to a certain extent, if not completely."). The vast majority of jurisdictions have adopted four common law privacy torts: "(1) intrusion upon seclusion, (2) public disclosure of private facts, (3) publicity placing a person in a false light, and (4) misappropriation of a person's name or likeness." *Id.* William L. Prosser initially described these four contexts. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960). Tort law is different from employment law as employees and employers are contractual partners. RESTATEMENT (THIRD) OF EMPLOYMENT LAW § 7.01 reporters' notes, cmt. a.

135. Warren & Brandeis, *supra* note 122, at 193.

136. *See, e.g.*, RESTATEMENT (THIRD) OF EMPLOYMENT LAW ch. 7, intro. note (explaining the "right to be left alone" as the "right to keep certain areas and activities free from intrusion by others" and protected against outside interference as some activities are sufficiently part of an individual's personality).

137. *See id.* § 7.01 reporters' notes, cmt. b (noting that whereas "[t]he intrusion-upon-seclusion tort has played an important role in the protection of privacy in the employment context" in the U.S., "the tort is not limited simply to the employer's observation of the employee's home, or the employer opening employees' mail").

in the American legal lexicon, employees have important privacy interests in their private information" outside of the home, too.[138]

D. Personal Health and Welfare

People generally maintain better physical, psychological, and spiritual health when they have private space—"some locus that is inviolable by others except at the person's express invitation."[139]

People disclose themselves to those they trust, and it is reasonable to expect trust to be built before the disclosure. Nevertheless, electronic communication is different from traditional communication. Writing by computer or keypad is perceived as impersonal.[140] Consequently, electronic "messages are depersonalized," often resulting in "stronger or more uninhibited text and more assertiveness in return."[141] In other words, today's electronically transmitted communications are more likely than traditional forms of communication to be even more personal and, as perceived by the creator, private in nature. Yet, "[d]espite documented adverse effects" from psychological and business perspectives, employers continue to routinely monitor their employees.[142]

E. The Efficiency Advantage of Privacy

Having a private sphere in the workplace might bring better results from the employers' point of view. In place of suspicion and mistrust, privacy and trust might encourage employee motivation, followed by higher productivity levels, an improved sense of responsibility toward work, an increased likelihood of employee initiative, and improved worker health.[143] This would advantage not only the employer but society as a whole.[144]

---

138. *Id.*

139. Jourard, *supra* note 127, at 310.

140. Sara Kiesler et al., *Social Psychological Aspects of Computer-Mediated Communication*, 39 AM. PSYCHOLOGIST 1123, 1125 (1984).

141. *Id.* (positing the use of electronic communication brings new social psychological norms of behavior because of the associated feeling of anonymity).

142. Abril et al., *supra* note 19, at 69; Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 286 (2011).

143. *See* Ciocchetti, *supra* note 142, at 286–87 (noting that excessive employee monitoring may lower employees' trust in their employers and decrease morale); *see also* Ethan S. Bernstein, *The Transparency Paradox: A Role for Privacy in Organizational Learning and Operational Control*, 57 ADMIN. SCI. Q. 181, 205 (2012) (suggesting that creating "zones of privacy" may improve performance); Jourard, *supra* note 127, at

IV. ALTERNATIVE LEGAL TOOLS

Given an understanding of the right to privacy as framed by the above-mentioned justifications, policymakers and scholars ought to re-think the current legal regime regarding employee privacy within the digital sphere in general and with respect to data posted on social networks in particular, using modern principles to replace or at least reshape the traditional approach. The new tools suggested herein leave enough room for judicial flexibility to respond in a world of constant and often rapid changes. First, this Part describes the traditional approach that led to the new reality of an almost total loss of privacy for information posted on social networks about applicants or employees in both the public and private sectors. This is followed by a description of suggested legal principles that should govern employee privacy rights and shape its limits.

A. Status Quo: Oppression of Employee Privacy in the Virtual Sphere

Current prevailing practice regarding privacy at the workplace often exposes American employees to trespass by their employers via the unwelcome reading of private e-mails or text messages in mobile phones and other devices, tracking of employee location, tracking of Internet activities, and surveillance of social network postings (e.g., on Facebook). Indeed, courts and lawmakers around the world are "having trouble conceptualizing privacy in new technologies."[145] The prevailing attitude in the U.S. is that the digital sphere (i.e., social networks) is not protected from employer intrusion of employee privacy.[146]

By applying an "incorrect" or "incomplete" traditional legal interpretation to the virtual era, the U.S. regime has caused American employees to almost entirely lose their right to privacy within the workplace. The reasonable expectation of privacy test

---

308 (arguing that, in order to avoid the punishment that results from deviating from one's role, individuals have an interest in their outward appearances).

144. Pauline T. Kim, *Electronic Privacy and Employee Speech*, 87 CHI.-KENT L. REV. 901, 931 (2012) ("Because employee privacy plays a crucial role in nurturing socially valued employee speech, protecting that privacy also promotes the broader public values advanced by that speech.").

145. *See* Abril et al., *supra* note 19, at 65 ("The shared unease among lawmakers around the world suggests that they need more information to gauge privacy and behavioral norms for new technologies.").

146. *See Fact Sheet 7: Workplace Privacy and Employee Monitoring*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/workplace-privacy-and-employee-monitoring (last updated Aug. 2014) (warning that company e-mail, private e-mail, and instant messaging applications, if accessed through a company terminal, are subject to monitoring).

implemented by the public sector virtually eliminates employees' privacy rights when applied within a modern virtual workplace realm.[147] The same drained privacy rights result has been diagnosed in the private sector by Christine Jolls, who found that non-governmental workers overwhelmingly lose their rights when courts apply a test that examines explicit or implicit consent because all employees "agree" to waive the right to privacy.[148] Therefore, moving toward "opt-in" employee "consent" policies would not change this result. Even in cases where courts have respected an employee's privacy in a private sector job, they have not held that employers cannot monitor or regulate the use of workplace computers. Instead, they have held that companies can adopt and enforce lawful policies relating to computer use to protect the assets, reputation, and productivity of a business, to ensure compliance with legitimate corporate policies, and to enable employers to discipline or terminate employees for violating workplace rules that are not inconsistent with a clear public policy mandate.[149] The outcome is that employees have almost totally lost their privacy rights within the virtual spheres of workplaces.

Consequently, the current U.S. legal posture, stemming mainly from court decisions that distinguish between privacy within tangible premises of the workplace and virtual spheres, should be reconsidered and refined. The traditional test, as set forth by the U.S. Supreme Court in *O'Connor v. Ortega*,[150] should be applied to today's virtual workspaces extending the law so as to integrate it with the realities of the digital era.[151] The employee expectation of privacy test as well as other contract and tort theories should be either replaced or adjusted to this notion of virtual workplace privacy zones.

---

147. For an explanation of the reasonable expectation of privacy test, see *infra* note 153 and accompanying text.

148. Christine Jolls, *Privacy and Consent Over Time: The Role of Agreement in Fourth Amendment Analysis*, 54 WM. & MARY L. REV. 1693, 1696–97 (2013).

149. *See* Hennessey v. Coastal Eagle Point Oil Co., 609 A.2d 11, 21 (N.J. 1992) (holding random drug testing of employees in positions that could affect public safety does not violate public policy); Woolley v. Hoffmann-La Roche, Inc., 491 A.2d 1257, 1258 (N.J.) (holding enforceable against an employer an implied promise in an employment contract that employee may only be fired for cause), *modified*, 499 A.2d 515 (N.J. 1985); Pierce v. Ortho Pharm. Corp., 417 A.2d 505, 512–13 (N.J. 1980) (holding that an employee must identify a specific public policy that was violated by termination before she or he can prevail in wrongful discharge action).

150. 480 U.S. 709 (1987).

151. *See id.* at 718 (recognizing that employees' tangible workspaces—such as desks, cubicles, or offices—in a public workplace may be deemed private spaces).

1. The governmental sector

American law differentiates between employees who work in governmental institutions and those who work in the private sector because the U.S. Constitution (specifically, with respect to privacy by its Fourth Amendment) limits the government, including in its capacity as an employer.[152] Public sector monitoring of employee usage of employer Internet tools and other communication devices is subject to a test of the employee's *reasonable expectation of privacy*,[153] whereas private sector workers are governed mainly by explicit or implicit contracts.[154] The prevailing attitude in the U.S. workplace and courts is that e-mail privacy (and general Internet usage less explicitly) and tracking of private information on employee Internet posts is *not* protected, whether originating in the physical workplace or from the virtual sphere, and especially when employees use employer computers and networks. Courts have held that employees cannot have a reasonable expectation of privacy in e-mail or other electronic communications, and federal law is limited and generally leans away from affording employees privacy, especially when it comes to the specific issue of e-mail.[155]

Physical instruments and spaces have traditionally defined privacy law in the United States. The reasonable expectation of privacy

---

152. That distinction notwithstanding, the practice of permitting employer intrusion upon employee electronic communication and digital tool usage is prevalent within both sectors. *See* Secunda, *supra* note 19, at 278–82 (offering a clear delineation of the differences between the private and the public employment sectors and arguing that there are sound public policy interests in providing greater protection for government workers). Absent government intervention or involvement as an employer, the law affecting private employers and their employees is based mainly in tort and is evolving. *Id.* at 279.

153. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) *expectation of privacy* and, second, that the expectation be one that society is prepared to recognize as '*reasonable*.'" (emphasis added)). But the Court subsequently held that privacy rights "do not rise or fall with the *Katz* formulation," noting that common law understandings of trespass, including the particular concern of "government trespass upon the areas ('persons, houses, papers, and effects') it enumerates," was not repudiated by *Katz* but, rather, supplemented by the ruling. United States v. Jones, 132 S. Ct. 945, 950 (2012).

154. *See* Christine Jolls, Rationality and Consent in Privacy Law 11–14 (Dec. 10, 2010) (unpublished manuscript), *available at* http://www.law.yale.edu/documents/pdf/Faculty/Jolls_RationalityandConsentinPrivacyLaw.pdf (discussing cases where consent to various terms of employment bound consenting employees).

155. Lisa Smith-Butler, *Workplace Privacy: We'll Be Watching You*, 35 OHIO N.U. L. REV. 53, 67–68 (2009) (suggesting that although federal laws "appear to protect employees' e-mail privacy, they generally do not").

analysis, endemic to privacy jurisprudence, is firmly rooted in the experience of physical space and its surrounding normative circumstances. Policymakers have thus far failed to adjust privacy norms to the new reality that most workers function within a virtual sphere in a way that at least partially protects individual privacy.

2. The private sector

The public sector reasonable expectation of privacy test nearly eradicates employees' privacy rights when applied within a modern virtual workplace realm.[156] The same result of drained privacy rights has been diagnosed in the private sector by Jolls, who found that non-governmental workers overwhelmingly lose their rights when courts apply a test that examines explicit or implicit consent since all employees "agree" to waive the right to privacy.[157] "Consent" policies, clearly, are not the answer to safeguarding employee privacy rights within virtual workplaces.

Chapter seven on Employee Privacy and Autonomy of the Restatement (Third) of Employment Law summarizes the legal rules concerning employee privacy in the private sector.[158] The legal rules are based mainly in two fields. One is the law of contracts, in which the most relevant legal tool is the employer policy.[159] The contracts law regime views company policy (often expressed in the form of an employee handbook) as a valid contract, subject to the general conditions that validate contracts.[160] Employees often give implied or explicit consent to surveillance by their employer or prospective employer, even though using social media to screen job applicants may not meet the condition of a contract when applicants do not know that their data is being scrutinized at this stage.[161] The other

156. *See* Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979, 1016 (2011) ("Absent specific state laws limiting intrusive employee monitoring—which tend to be few and narrowly drafted—employers are free to destroy U.S. employees' expectations of privacy via detailed notices, and without an actual expectation of privacy, employee privacy is not protected against monitoring under federal law and general state privacy laws.").

157. Jolls, *supra* note 154, at 11–14.

158. RESTATEMENT (THIRD) OF EMPLOYMENT LAW ch. 7, intro. note (Tentative Draft No. 5, 2012).

159. *Id.* § 3.01 cmt. e.

160. *Id.*; *see also* Jolls, *supra* note 154, at 11–14 (noting that courts often view consent to terms of employment as binding on the consenting employee).

161. *See generally* RESTATEMENT (THIRD) OF EMPLOYMENT LAW § 7.03 cmt. j. (discussing express and implied privacy policies).

realm upon which employment privacy laws draw heavily is the law of torts, from which the expectation of privacy test is drawn. This brings the public sector test to the private sector.[162] The ultimate result in both employment sectors is the same: employees maintain no actual protection of their privacy with respect to personal data on social networks.

B. A New Horizon: Alternative Legal Tools

The importance of privacy rights does not skip over employees in the workplace. It is time to reconsider the legal tools and privacy policies within workplaces in order to secure "private zones" for employees using the virtual sphere, such as within social networks.

The mere existence of technical surveillance tools capable of tracing and tracking personal data does not make the *use* of those tools to violate privacy a permissible norm. There is a gap between what can be done technically and what *should* (or should *not*) be done. Bringing American policy in line with the realities of digital age society will benefit employers by fostering trust, encouraging workplace creativity, and improving productivity. According to the main principle of this Article—that employees have the right to a secured "private zone" that protects data about them posted on social networks—policymakers should re-think the existing legal tests and consider replacing them with alternative tools that balance legitimate interests with employee rights.

1. Obeying other laws: Antidiscrimination laws

Any employer action, including an instance of legitimate surveillance, is subject to existing laws, including antidiscrimination laws that are applicable to workplaces.[163] The fact that certain information is accessible and easily read does not justify the violation of antidiscrimination laws. Therefore, employers should not look for discriminative data. If seen, it should not be taken into consideration in hiring, promoting, or firing employees or in any other workplace context. For example, information about gender,

---

162. *See id.* (applying the reasonable expectation of privacy test to hypothetical workplace scenarios).

163. *See supra* Part II.A (explaining that while employers cannot overtly discriminate against job applicants by asking them certain questions, they can uncover information about private data in the virtual sphere).

age, sexual preference, or religion should be irrelevant to the workplace in most cases.[164]

The same rule that prevents employers from asking applicants questions about their sexual habits[165] should be applied in the context of social networks. Given the accessibility of information in social networks, combined with the discriminatory nature of some of the information typically posted and the irreversibility of exposure to such data, online profile tracking should be permitted only when necessary to achieve specific legitimate goals. Therefore, "red lines" that limit the tracking and the usage of social network information should be established.

2. Transparency and informed consent

Current employees as well as applicants should not only be aware of an employer policy and its effects, but they should also explicitly agree to it. Therefore, as a first step, employers should adopt a transparent policy regarding privacy at the workplace that conforms to all other conditions described in this subsection. This policy ought to be written, clear, detailed, and include, *inter alia*, the different aspects of privacy incursion by the employer, including Internet surveillance on social networks, e-mail monitoring, and computer usage. It should be published and accessible to all applicants and employees. If the company has an employee handbook, the policy should be included. However, all of these measures, which represent today's norm relating to privacy policies at workplaces, are necessary but not sufficient to create a valid agreement concerning employees' privacy rights in the virtual sphere. Applicants and employees should explicitly agree to data tracking (under any of the different conditions) and should have a right to refuse these actions.[166]

One of the most important components of a reasonable privacy policy is employee consent. However, there are several levels of

---

164. *See* Civil Rights Act of 1964, Pub. L. No. 88-352, § 703, 78 Stat. 241, 255 (codified as amended at 42 U.S.C. §§ 2000e–2000e-17 (2012)) (providing exceptions for, *inter alia*, bona fide occupational requirements, certain religious schools, and national security positions).

165. *See, e.g.*, *Best Practices for Employers in a Hiring Interview*, FINDLAW, http://files.findlaw.com/pdf/smallbusiness/smallbusiness.findlaw.com_employment-law-and-human-resources_best-practices-for-employers-in-a-hiring-interview.pdf (last visited Sept. 30, 2014) (noting that such questions are not only in bad taste but also run afoul of state or federal antidiscrimination laws).

166. *See generally* Jolls, *supra* note 154, at 21 (comparing drug screening cases in which employees complain about positive results and cases in which employees withdraw their agreement prior to testing).

consent. The first is implied consent, derived from the existence of the employee—employer relationship. The second is informed consent, created by potential or actual prior knowledge about the privacy policy. The third is express consent, in which employers obtain employees' informed, willing, written, and signed consent to any invasion of privacy. In order to meet the "informed signed consent" requirement, the employer must disclose to the employee, in writing, the matters set forth in the policy, such as the nature of any monitoring tools, the purpose of monitoring, and the period for which monitored data will be retained. The policy should also be attached to individual employment agreements and approved by each employee with his signature. The fourth type of consent is one which conforms to a valid judicial definition.[167]

There are two types of employee consent with regard to the details of the violation of privacy: (1) general consent to a policy, and (2) specific consent to each instance of monitoring.[168] Is implied consent sufficient for authorizing monitoring data from social networks by employers?

Courts have stated that under the private party consent to surveillance provision of the Electronic Communications Privacy Act of 1986 (ECPA), consent does not have to be explicit: it may be implied.[169] In a case involving a claim of implied consent under this subject, the U.S. Court of Appeals for the First Circuit explained that "implied consent is 'consent in fact' which is inferred 'from surrounding circumstances indicating that the [party] *knowingly agreed to the surveillance*.'"[170] "Thus, implied consent—or the absence of it—may be deduced from 'the circumstances prevailing' in a given situation."[171] This decision does not align with the main argument of

---

167. *See id.* at 14 (delineating between implied consent, express consent, and express consent provided by "each party"). *But see* YOAN HERMSTRÜWER & STEPHAN DICKERT, TEARING THE VEIL OF PRIVACY LAW: AN EXPERIMENT ON CHILLING EFFECTS AND THE RIGHT TO BE FORGOTTEN 3 (2013) (arguing that consent to disclosure of personal information creates a risk of a chilling effect that increases people's propensity to comply with social norms and "induce[s] them to forego benefits from norm deviations," such as the exercise of civil liberties).

168. *See* Jolls, *supra* note 154, at 63 n.195.

169. Pub. L. No. 99-508, § 101(b), 100 Stat. 1848, 1850 (1986) (codified as amended at 18 U.S.C. § 2511(2)(d) (2012)); Williams v. Poulos, 11 F.3d 271, 281 (1st Cir. 1993); *see also* Lazette v. Kulmatycki, 949 F. Supp. 2d 748, 757 (N.D. Ohio 2013) ("Negligence is, however, not the same as approval, much less authorization. There is a difference between someone who fails to leave the door locked when going out and one who leaves it open knowing someone [will] be stopping by.").

170. Griggs-Ryan v. Smith, 904 F.2d 112, 116–17 (1st Cir. 1990) (alteration in original) (emphasis added) (quoting United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987)).

171. *Id.* at 117.

this Article. Indeed, to secure the necessary "private zone" as justified by psychological reasoning presented in this study, the adoption of more restrictive levels of consent would be preferable.

Relying on a policy of consent bears risks as employees are likely to sign any agreement in order to be employed.[172] Therefore, employers should consider informed and express consent when the broader policy includes components for securing a privacy minimum that will not be subject to contractual waiver. This would be a significant change from the prevailing legal reality in which implied consent is, in many cases, sufficient.

Knowledge of the capability of monitoring alone cannot be considered implied consent. In *Deal v. Spears*,[173] the U.S. Court of Appeals for the Eighth Circuit held an employee did not impliedly consent to monitoring of her phone calls when her employer only told her that it might monitor phone calls.[174] Similarly, in *Lazette v. Kulmatycki*,[175] the U.S. District Court for the Northern District of Ohio concluded that there was no reason for the plaintiff to predict that her employer would monitor future e-mail messages sent from her personal Gmail account.[176]

Furthermore, employees should not be penalized for refusing their employers' requests to monitor their data in social networks, a concept some states have codified through laws prohibiting employers from asking for employees' private passwords.[177]

3. Inspection, the right to be heard, and the right to appeal

All data gathered legitimately should be reported to the applicant and employees. Following notification, employees must have the right to explain, comment, and even appeal.

4. Proportionality and reasonability

Rights of employers and the constitutional right to freedom of speech conflict when employers seek data in digital spheres about

---

172. *See* Jolls, *supra* note 154, at 11 (noting cases in which employees consented to polygraph and drug tests as prerequisites to employment).

173. 980 F.2d 1153 (8th Cir. 1992).

174. *See id.* at 1157 (finding the possibility of monitoring insufficient to infer implied consent).

175. 949 F. Supp. 2d 748 (N.D. Ohio 2013).

176. *Id.* at 757–58 ("Random monitoring is one thing; reading everything is another.").

177. *See supra* note 94 and accompanying text (describing the state action in response to concerns of employer's overreaching by requesting prospective employees for their Facebook passwords and providing an example from the State of Washington).

employees or applicants. The "proportionality" test and the "least restrictive means" specifically provide an example for an alternative legal tool that can help policymakers.[178] Proportionality analysis has evolved over the past fifty years and "is today an overarching principle of constitutional adjudication . . . [and] the preferred procedure for managing [certain] disputes . . . as a multi-purpose, best-practice standard."[179]

"The core of necessity analysis is the deployment of a 'least-restrictive means' test" in which the court "ensures that the measure does not curtail the right any more than is necessary . . . to achieve its stated goals."[180] The idea behind this principle is simple. When there are two or more ways to safeguard a legitimate employer interest, the permissible infringement upon a right would be the one that achieves the interest in the least restrictive, least offensive way. The policy that better protects the right will be adjudicated as the proper one.[181]

Applying this constitutional principle to the workplace context, in both the public and private sector, a least *invasive* means analysis should be the applicable test for maintaining virtual privacy of data posted on social networks. If an applicant's curriculum vitae (CV), interview, or any other data provided voluntarily is available as a means for ascertaining the candidate's qualifications, then violating privacy in order to gather this information (even from public spheres) would be impermissible. A proportionality rule such as this could be implemented quite efficiently with respect to employee privacy. Employers should limit incursion of employee "private zones" to legitimate circumstances in which severe and immediate damage may be caused to the employer's legitimate interests (such as harmful criminal activity by an employee) when there are no other alternatives available to achieve the same goal. Invasion into employee privacy may only take place to the extent that there are no

178. *See generally* AHARON BARAK, PROPORTIONALITY: CONSTITUTIONAL RIGHTS AND THEIR LIMITATIONS 10–11 (Doron Kalir trans. 2011) (exploring four components of proportionality: proper purpose, rational connection, necessity, and proportionality *stricto sensu*).

179. Alec Stone Sweet & Jud Mathews, *Proportionality Balancing and Global Constitutionalism*, 47 COLUM. J. TRANSNAT'L L. 72, 73–74 (2008) (opining that "proportionality-based rights adjudication now constitutes one of the defining features of global constitutionalism, if global constitutionalism can be said to exist at all").

180. *Id.* at 75.

181. Jud Mathews & Alec Stone Sweet, *All Things in Proportion? American Rights Review and the Problem of Balancing*, 60 EMORY L.J. 797, 803 (2011) (discussing the American "narrow tailoring" test (internal quotation marks omitted)).

other less invasive alternatives to achieve the same result, and if proportional, measured in light of the potential harm to the employees. Employers should also use the least invasive technology available. For example, legitimate software can provide alternative sources of data that are less invasive than human monitoring of information posted on social networks.[182]

Tracking of any data on employees or applicants beyond the business context should be considered an invasion of privacy. Information must only be tracked for specific, clear, and legitimate purposes. Employers should not use information gathered from monitoring for any purpose other than the purpose for which the monitoring was performed.[183]

5. The European approach to privacy in the workplace

This final subpart discusses some global trends that have contributed to recent shifts in U.S. legal norms toward the notion that more private zones within virtual spheres ought to be secured for employees and job applicants.

Europe enjoys one of the most protective privacy systems based on the European Convention on Human Rights,[184] the Council of Europe Convention 108,[185] various European Union (EU) instruments, and case law from the European Court of Human Rights and the Court of Justice of the European Union.[186] There is no specific EU

182. Ariana Levinson, focusing specifically on the Electronic Communication Privacy Act, provides a detailed analysis of limitations courts have placed on intrusive practices, both within and outside the context of employment law. *See generally* Ariana R. Levinson, *Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees*, 114 W. VA. L. REV. 461, 467–69 (2012).

183. *See id.* at 525 (interpreting the requirement in the Wiretap Act that employers are not to circumvent code-based restrictions to prevent "voyeuristic" employers from using information without a legitimate business purpose).

184. Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, E.T.S. No. 005 (outlining the right to respect for private and family life, home, and correspondence).

185. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, art. 5, Jan. 28, 1981, E.T.S. No. 108.

186. *See* EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS & COUNCIL OF EUR., HANDBOOK ON EUROPEAN DATA PROTECTION LAW 3 (2014) [hereinafter HANDBOOK ON EUROPEAN DATA PROTECTION LAW]. The European Union Agency for Fundamental Rights and the Council of Europe jointly prepared this handbook for the purpose of serving as the main point of reference in this field. *Id.* ("With the entry into force of the Treaty of Lisbon in December 2009, the Charter of Fundamental Rights of the EU became legally binding, and with this the right to the protection of personal data was elevated to the status of a separate fundamental right.").

legal framework that governs data processing with respect to employment. In the Data Protection Directive, employment relations are specifically referred to in Article 8, which concerns the processing of sensitive data.[187] With regard to the Council of Europe, the 1989 Employment Data Recommendation[188] is currently being updated.[189]

A few of the following recommendations serve as core principles of European law, as set out by the Council of Europe Committee of Ministers' Employment Data Recommendation:

(1) Personal data collected for employment purposes should be acquired from individual employees directly.[190]

(2) Personal data collected for recruitment must be limited to information necessary to evaluate candidate suitability.[191]

(3) Judgmental data must be based on fair and honest evaluations, must not be "insulting" in its formulation, and must be made in accordance with principles of fair data processing and data accuracy.[192]

(4) Employees should be informed about the processing of their personal data, including the purpose of processing, the type of personal data stored, the entities to which data is regularly communicated, and the purpose and legal basis of such communications. Employers also should inform employees in advance about any automated systems for the processing of personal data or for monitoring the movements or the productivity of employees.[193]

(5) Employees have a right of access to their employment data as well as a right to rectification or erasure. If a judgment is issued on the basis of data, employees have a right to contest the judgment, although these rights may be temporarily limited for the purpose of internal investigations. If an employee is denied access to review data, or is unable to rectify or erase the data, the Council of Europe recommends that national law requires appropriate procedures to contest such denial.[194]

(6) Consent is a significant legal basis for processing employment data, but there is awareness of the economic imbalance between

---

187. Council Directive 95/46, art. 8, 1995 O.J. (L 281) 1, 10 (EC).

188. Council of Eur., Comm. of Ministers, On the Prot. of Personal Data Used for Emp't Purposes, Recommendation No. R (89)2 (Jan. 18, 1989).

189. HANDBOOK ON EUROPEAN DATA PROTECTION LAW, *supra* note 186, at 171.

190. Council of Eur., Comm. of Ministers, On the Prot. of Personal Data Used for Emp't Purposes, Recommendation No. R (89)2 § 4.1.

191. *Id.* § 4.3.

192. *Id.* § 5.3.

193. *Id.* § 3.1.

194. *Id.* § 12.1–.5.

employers requesting consent and employees giving it. The circumstances surrounding a request for consent should be carefully considered when assessing the validity of such consent in the employment context.[195]

(7) Even when data is relevant, there are limitations on its collection. For example, employers may ask employees or job applicants about their state of health or conduct medical examinations only if necessary to assess suitability for employment, to fulfill requirements of preventative medicine, or to grant social benefits. Health data may not be collected from sources other than from the employee concerned except when express and informed consent is obtained or when national law so provides.[196]

The European approach emphasizes the widening gulf between U.S. and European data protection laws and creates challenges for multinational businesses and other organizations operating in Europe. For example, the European Court of Human Rights expanded the basis of protection for personal data in the workplace by ruling that Internet monitoring of employees, even for the sole purpose of analyzing web sites visited including date, time, and duration of visits, violated Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.[197] According to this attitude, business e-mail, Internet usage, and telephone calls affect the private lives of employees and may contain personal information that is protected by data protection laws. French courts have held that finding erotic photos on an employee's desk was insufficient to justify a search of the entire computer, only

---

195. *Id.* § 10.1; *see also* Article 29 Working Party, *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, at 11, 2093/05/EN, WP 114 (November 25, 2005) [hereinafter WP 114] (inviting employers to use more than just consent of their employees to transfer data to ensure valid consent was given considering the hierarchical relationship of an employer and employee).

196. Council of Eur., Comm. of Ministers, On the Prot. of Personal Data Used for Emp't Purposes, Recommendation No. R (89)2 § 10.2–.6; *see* WP 114, *supra* note 195, at 15–16 (discussing an exception to this rule in the case of medical necessity).

197. Copland v. United Kingdom (No. 62617/00), 2007-I Eur. Ct. H.R. 317, 322, 326, 332 (2007) ("The applicant alleged that the monitoring activity . . . amounted to an interference with her right to respect for private life and correspondence under Article 8, which reads as follows: '1. Everyone has the right to respect for his private and family life, his home and his correspondence.'"); *see* Fred H. Cate, *European Court of Human Rights Expands Privacy Protections:* Copland v. United Kingdom, AM. SOC. INT'L L. INSIGHTS (Aug. 6, 2007), http://www.asil.org/insights/volume/11/issue/21/european-court-human-rights-expands-privacy-protections-copland-v-united (asserting that Internet and e-mail monitoring by employers is generally prohibited).

to discover a personal file that contained downloaded pornographic images that gave the employer cause to terminate the employee.[198] Accordingly, courts have found that the existence of particularized suspicion that an employee was freelancing on company time while using company resources alongside the existence of an explicit policy are irrelevant.[199]

Unlike Western Europe, which has robust employee privacy protection even in the private sector, the U.S. does not.[200] This Article challenges the wide gulf between these two parts of the world and asks: should it be so wide?

V. A SHIFT TO A DIFFERENT ATTITUDE: SECURING A VIRTUAL "PRIVATE ZONE"

A. Legislation Forbidding Employer Access to Employee Social Media

With increasing numbers of people using social media both at and away from their workplaces, employers seeking information about employees or applicants have started asking for usernames and passwords for personal social networks and e-mail accounts.[201] Employers have justified such requests by arguing that access to personal accounts is needed to protect proprietary information or trade secrets, to comply with federal financial regulations, or to prevent the employer from being exposed to legal liability.[202] However, policymakers throughout the U.S., in accordance with the position expressed in this Article, have considered requiring access to personal accounts to be an invasion of employee privacy. Since 2012, legislative bodies in many states have begun creating laws to prevent

198. *See* Cate, *supra* note 197 (summarizing the French high court's rationale that the erotic photos "did not present the type particular risk that could justify the search of the computer").

199. *See id.* (discussing a case from the Court of Cassation).

200. *See* Yohei Suda, *Monitoring E-Mail of Employees in the Private Sector: A Comparison Between Western Europe and the United States*, 4 WASH. U. GLOBAL STUD. L. REV. 209, 209, 212–13, 240, 249 (2005) (asserting that various factors contribute to the difficulty in the United States to provide more robust privacy protections, including the lack of recognition that privacy is a fundamental right, private companies' lack of trust in the government to protect employee privacy, and the precedence given to explicit rights guaranteed by the Constitution, such as First Amendment rights, at the expense of implicit rights to privacy under the Fourth Amendment).

201. *See Employer Access to Social Media Usernames and Passwords*, *supra* note 94.

202. *See* WASH. REV. CODE § 49.44.200 (2013) (permitting employers to request social networking content under certain circumstances, including, *inter alia*, for investigations into employees stealing trade secrets).

employers from asking or forcing employees to disclose passwords to personal accounts.[203] Some states have enacted similar laws to protect students, primarily in public colleges and universities, from being forced to provide the school access to their social networking accounts.[204] It is impressive that legislation has been initiated in at least twenty-eight states in 2014, and as of September 2014, twenty states have enacted legislation of this type.[205]

For example, Washington State's bill concerning personal social networking accounts passed unanimously by both branches of the state legislature and was signed into law. This law bans employers from requesting or requiring any employee or prospective employee to submit any password or other related account information in order to gain access to the individual's personal social networking website, account, or profile.[206] Pending legislation in New York similarly "prohibit[s] an employer or educational institution from requesting or requiring that an employee, applicant or student disclose any . . . means for accessing a personal account or service through specified communications devices."[207]

In California, "[e]xisting law prohibits a private employer from requiring or requesting an employee or applicant for employment to disclose a username or password for the purpose of accessing personal social media, to access personal social media in the presence of the employer, or to divulge any personal social media."[208] California law also "prohibits a private employer from discharging, disciplining, threatening to discharge or discipline, or otherwise retaliating against an employee or applicant for not complying with a request or demand that violates these provisions."[209] A current bill

---

203. *See Employer Access to Social Media Usernames and Passwords*, *supra* note 94 (providing examples of bills in California, Connecticut, and Georgia).

204. *Id.* (providing examples of bills in Hawaii and Rhode Island).

205. *See id.* (listing Arkansas, Colorado, Illinois, Louisiana, Nevada, New Hampshire, New Jersey, New Mexico, Oklahoma, Oregon, Rhode Island, Tennessee, Utah, Vermont, Washington, and Wisconsin as having enacted legislation of this type in 2013 and 2014); *Employer Access to Social Media Usernames and Passwords, 2012 Legislation*, NAT'L CONF. ST. LEGISLATURES (Jan. 17, 2013), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords.aspx (listing California, Delaware, Illinois, Maryland, Michigan, and New Jersey as having enacted legislation of this type in 2012).

206. *See* WASH. REV. CODE § 49.44.200(1).

207. S. 02434D, 2013–14 Reg. Sess. (N.Y. 2013).

208. Assemb. B. 25, 2013–14 Reg. Sess. (Cal. 2012).

209. *Id.*

would apply these provisions to public employers as well.[210] Directing these provisions toward the private sector might be justified because public employees are operating within protections not always applicable to private sector employees.[211]

Similar legislation has failed in states such as Texas, North Dakota, and West Virginia.[212] Nonetheless, the legislative initiatives in so many states represent significant progress and recognition of the complexity of relations within workplaces and the right of employees to privacy within virtual spheres. These state laws have the potential to substantially increase privacy protections of employees concerning social networking. On the other hand, these laws might be difficult to implement in workplaces where employees agree to explicit but also implicit demands.

The main problem persists where the laws "do not limit an employer from accessing social media" either on its own or through an individual.[213] Moreover, even the most progressive legislation does not differ from common law rules that rely specifically on the traditional expectation of privacy test (which may not be fulfilled in a "closed" social networking group that does not include the employer's representatives). Therefore, these tools cannot be applied to a social network profile that is not limited to a very specific group or to data posted by third parties. Privacy is not viewed as an absolute human right.[214] In the same manner, the taking of information from open social networks should be protected to a certain level and, hence, at least partially limited.

---

210. *Id.*

211. *See* William A. Herbert, *Can't Escape from the Memory: Social Media and Public Sector Labor Law*, 40 N. KY. L. REV. 427, 434 (2013) (arguing that "a *de jure* regulatory structure for government employment is necessary to check the powers of the state and partisan politics").

212. *See Employer Access to Social Media Usernames and Passwords*, *supra* note 94 (noting four failed bills in Texas, one in North Dakota, and one in West Virginia).

213. Herbert, *supra* note 211, at 433.

214. RESTATEMENT (THIRD) OF EMPLOYMENT LAW § 7.01 cmt. d (Tentative Draft No. 5, 2012) ("It is well recognized that the right to privacy is not an absolute right, but is rather a set of . . . interests that the common law protects against wrongful intrusion by others . . . . [T]he basic claim of [wrongful] invasion of the employee right of privacy [by employers] requires not only (a) an intrusion upon the employee's protected privacy interest, but also that (b) the employer intrusion upon that interest is highly offensive in scope or manner.").

B. Court Decisions in Favor of Employee Privacy

Recent U.S. court decisions have deviated away from the traditional legal inclination to validate firms' policies by upholding employees' expectations of privacy in data posted within virtual spheres. Even though these court decisions do not always refer to tracking data on social networks, they pertain to other "realms" within the virtual world used by employees (such as private e-mails) that share in some aspects the same logic and are applicable to the study.

In *Ehling v. Monmouth-Ocean Hospital Service Corp.*, the plaintiff asserted a common law invasion of privacy claim alleging unauthorized access of her private Facebook post about the Holocaust Museum shooter in which she expressed a personal view.[215] One of the questions discussed was whether an employee has a reasonable expectation of privacy in Facebook posts.[216] The plaintiff argued that "she had a reasonable expectation of privacy in her Facebook posting because her comment was disclosed to a limited number of people who she had individually invited to view a restricted access webpage."[217] The defendants argued that there cannot be a reasonable expectation of privacy in a comment disclosed to many people.[218] The court ruled that the plaintiff had a reasonable expectation that her Facebook posting was private because she ensured her privacy settings protected her page from public view.[219]

In 2010, the New Jersey Supreme Court adopted another pro-employee privacy decision and opposed an employer's explicit policy.[220] The employee was provided a company laptop computer for business purposes.[221] The employee was allowed to use the laptop for company e-mails and to use the Internet through the company's server.[222] Without the employee's knowledge, a copy of every Internet page the employee visited was saved onto a "cache" folder on her computer's hard drive.[223] The files remained on the hard drive unless they were manually deleted or overridden.[224] The employee

---

215. 872 F. Supp. 2d 369, 372 (D.N.J. 2012).
216. *Id.*
217. *Id.* at 374.
218. *Id.*
219. *Id.*
220. *See* Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010) (finding a reasonable expectation of privacy in the plaintiff's personal e-mail account).
221. *Id.*
222. *Id.*
223. *Id.* at 655–56.
224. *Id.* at 656.

communicated to her attorney about her situation at work through her personal Yahoo e-mail account, where she entered her password and user information.[225] After returning her laptop, she filed a complaint alleging harassment and other claims.[226]

The defendant employer hired a computer forensic expert to retrieve data from the plaintiff's laptop in preparation for discovery.[227] The defendant's attorneys discussed and analyzed the data that was retrieved by the forensic expert.[228] The company argued that it had the right to review the information according to its written and well known policies.[229] The New Jersey Supreme Court ruled that the employee had a reasonable expectation of privacy in the correspondence, affirming the Appellate Division's ruling that the employer had violated the employee's privacy by reading and using the documents.[230]

In another case, *Lazette v. Kulmatycki*, the plaintiff worked for Verizon, which provided her with a phone for business purposes and for her personal use.[231] After the plaintiff stopped working for Verizon, her supervisor read over 48,000 of the plaintiff's personal e-mails via the phone Verizon had given to her.[232] The court held in favor of the employee's right to privacy, ruling that the employer had no right or authority to read the plaintiff's personal e-mails.[233] The fact that the plaintiff had used a company phone to access her

---

225. *Id.*
226. *Id.*
227. *Id.*
228. *Id.*
229. *Id.* at 657 ("The proffered Policy states, in relevant part: 'The company reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the company's media systems and services at any time, with or without notice. . . . E-mail and voice mail messages, internet use and communication and computer files are considered part of the company's business and client records. Such communications are not to be considered private or personal to any individual employee. . . . Abuse of the electronic communications system may result in disciplinary action up to and including separation of employment." (internal quotation marks omitted)).
230. *See id.* at 663–64 (noting that the employer's policy did not give a reasonable person any cause to anticipate that the agent would be looking over the employee's shoulder as the employee opened private e-mails on her private account.).
231. 949 F. Supp. 2d 748, 751 (N.D. Ohio 2013).
232. *See id.*
233. *See id.* at 757–58 (holding that negligently leaving access to a personal account is not consent, nor is knowledge that the employee's e-mail will be monitored considered implied consent).

personal e-mail did not give her employer automatic authority to access and read her private e-mails.[234]

Even more cases reflect this pro-employee privacy tendency. In *Smith v. Hillshire Brands*,[235] the U.S. District Court for the District of Kansas limited the extent to which litigating parties can demand access to Facebook accounts for purposes of pre-trial discovery.[236] Magistrate Judge O'Hara did not accept the defendant's position on the relevancy of the discovery requests and denied the argument that everything is relevant.[237] The judge used Facebook posts as an example claiming that not every post involved in the decision to terminate the plaintiff is relevant.[238] Thus, employers are not entitled to access employees' social networks and other forms of communication, such as personal e-mail, because this is equivalent to a search of tangible objects in a plaintiff's home.[239]

These cases, like the legislative initiatives described earlier, represent significant progress in the discourse on employee privacy in the workplace with respect to electronic media.

While not related to social media and employees, the U.S. Supreme Court recently issued what has been referred to as a landmark opinion regarding privacy rights, clearly demonstrating a shift toward recognizing the importance of privacy in the digital age. In *Riley v. California*,[240] the Court unanimously held that a cell phone may not be searched or seized without a warrant.[241] Chief Justice Roberts wrote about the pervasive use of smart phones:

> Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. . . . A decade ago police officers searching an arrestee might have occasionally stumbled across a highly personal item such as a diary. . . . Today, by contrast, it is no exaggeration to say that many of the more than [ninety percent] of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. Allowing the police to scrutinize such

234. *See id.* at 758 (advising that having access to the plaintiff's e-mails does not mean that the plaintiff gave implied consent for her employer to read them).
235. No. 13-2605, 2014 WL 2804188 (D. Kan. June 20, 2014).
236. *Id.* at *1, *4–5.
237. *Id.* at *4–5.
238. *Id.* at *5.
239. Ogden v. All-State Career Sch., 299 F.R.D. 446, 450 (W.D. Pa. 2014).
240. 134 S. Ct. 2473 (2014).
241. *Id.* at 2485.

> records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.[242]

Nonetheless, the status of protection for employee and prospective employee personal data as published within social networks and other sources remains far from ideal.[243]

CONCLUSIONS

Social networks are public digital environments where people can gather via mediating technologies. They support social interaction[244] by allowing users to create personal profiles, identify lists of associates, send messages, and participate in discussion forums.[245]

Denying or diminishing this virtual sphere can be equal to and as drastic as forbidding a person from speaking, as these mechanisms are the digital era's basic means of communication. Nowadays, other alternatives are not viable and therefore cannot be considered "real" alternatives.

Privacy in social networking is an emerging, but underdeveloped, area of case law.[246] There appears to be some consistency in the case law on the two ends of the privacy spectrum. On one end of the spectrum, cases hold that there is *no* reasonable expectation of privacy for material posted to an unprotected website that anyone can

---

242. *Id.* at 2490 (citations omitted).

243. *See, e.g.*, Kanawha Cnty. Bd. of Educ. v. Kimble, No. 13-0810, 2014 WL 2404322, at *1–4 (W. Va. May 30, 2014) (upholding a school district's dismissal of a school employee who had posted pictures to her MySpace account of herself cavorting in a hot tub with students). The students were topless and the employee had captioned the photograph with the derogatory term "hoes," a slang term meaning "whores." *Id.* at *1. The appellate court, overturning a lower decision that reversed the employee's dismissal, found this language to be evidence of immoral behavior. *Id.* Moreover, the court found that the employee had no expectation of privacy because the photo was taken in the context of the employment—even though the photograph was taken off of school premises and not during school hours—because it was taken in the context of an activity (albeit an unsanctioned one) involving the students entrusted to the employee for an overnight trip. *Id.* at *2–4.

244. *See* Adam N. Joinson, *'Looking at,' 'Looking up' or 'Keeping up with' People? Motives and Uses of Facebook*, *in* 1 CHI 2008 CONFERENCE PROCEEDINGS 1027, 1028 (Margaret Burnett et al. eds., 2008), *available at* http://digitalintelligencetoday.com/downloads/Joinson_Facebook.pdf (contrasting social media from "old media").

245. *See* Boyd, *supra* note 49, at 1 (creating a public forum for kids to be seen as cool in school).

246. *See* 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) (discussing the undefined legal boundary between public and private communications on social networking websites).

view.[247] On the other end of the spectrum, cases hold that there *is* a reasonable expectation of privacy for individual password-protected online communications.[248] U.S. courts, however, still use traditional tests and rely either on the reasonable expectation of privacy standard or on contract law governing company policy statements.

The most deep-seated problem of all is the societal attitude and consequential legal posture, which has yet to develop a consistent opinion or coherent approach toward data posted with restrictive measures (e.g., defined as private or aimed at a specific group of "friends"). Although most courts hold that a communication is not necessarily public just because it is accessible to a number of people, courts differ dramatically regarding how far this theory extends. What is clear is that privacy determinations are still made on a case-by-case basis in light of all the facts presented.[249]

A different perspective on the issue of employee privacy concerns the question of the legal rules regarding employers as a database holder. Employers collect a lot of information about their employees and keep it in their possession. New legal rules should address questions like: Who can hold this data? Where can it be held it and for how long? What data can be stored? Who can have access to the data? Should employees be aware of this data? And so on and so forth.

As the new era of international commerce gives rise to new considerations, the answers to questions about the right of employees

---

247. *See* 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. 2004) ("[I]t 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, *without taking any measures to protect the information*."); Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 44 (Minn. Ct. App. 2009) (holding that privacy was lost when private information was posted on a publicly accessible Internet website and "[a]ccess to [the publication] was not protected").

248. *See, e.g.*, Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 561 (S.D.N.Y. 2008) (holding that the employee had a reasonable expectation of privacy in personal, password-protected e-mail messages stored on a third party's server even though the employee had accessed that outside server while at work).

249. *See* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 939 (2005) (explaining that most courts have adopted the concept of "limited privacy," which is "the idea that when an individual reveals private information about herself to one or more persons, she may retain a reasonable expectation that the recipients of the information will not disseminate it further"). *Compare* Multimedia WMAZ, Inc. v. Kubach, 443 S.E.2d 491, 493–94, 496 (Ga. Ct. App. 1994) (finding that the plaintiff's disclosure of facts over the air did not render them public), *with* Fletcher v. Price Chopper Foods of Trumann, Inc., 220 F.3d 871, 878 (8th Cir. 2000) (finding that the plaintiff's disclosure of facts to two coworkers deprived her of a reasonable expectation of privacy).

to private virtual zones also emerge through multinational firms. American companies abroad and foreign firms located throughout multiple countries might incorrectly assume that American policy prevails. This could result in breaches of local policy regarding privacy in the workplace.

In many of the social network intrusion cases, the main justifications for legitimate invasion in employees' privacy are inapposite. Neither the employer's "need to examine the work of the employee to determine the quantity, quality, and timely provision of service" nor the claim that "employers generally own and control the workplace and its instrumentalities"[250] can justify using personal information in social networks per se. It is time for American employment law and social policy to catch up with the reality of the virtual sphere and to permit employees, whether current or prospective, to enjoy privacy within their social network without fear of intrusion or professional reprimand over private matters.

250. RESTATEMENT (THIRD) OF EMPLOYMENT LAW § 7.01 cmt. b (Tentative Draft No. 5, 2012).