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, Professor of Law, Yale Law School
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 the questions of whether this casual business routine harms employees' rights to privacy with regard to data users post in 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.

The article further claims that securing a “private zone” to 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”), describing 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 rethinking of the current U.S. regime, based on tort law (expectation test) and contract law (implied consent based on firms' policies), which costs applicants and employees a near-total loss of privacy in their virtual postings.

This article not only argues the case for a more balanced approach to employees' privacy, but also suggests a new desirable model to be adopted by policymakers. 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 at the workplace.

I also contend that this model may be implemented to protect privacy rights in data posted in social networks beyond the context of employment.

1Professor of Law. Yale Law School, Information Society Project (ISP), Fellow, 2011-2013. Fordham Law School, Visiting International Professor, 2012. Ono Academic, School of Law, Israel. The Founder and the Head of the Shalom Comparative Legal Research Center, OAC. Thanks to Prof. Jack Balkin, ISP and to Prof. Joel Reidenberg, Center on Law and Information Policy (CLIP), Fordham Law as well as to the Swiss Institute of Comparative Law, Lausanne, Switzerland. Special thanks to Ms. Elizabeth Ledkovsky for outstanding research assistance.
To Read or Not To Read: Privacy Within Social Networks, The Entitlement Of Employees To A Virtual “Private Zone” And The Balloon/Magnet Field Theory.
Dr. Shlomit Yanisky Ravid, Prof. of Law. Yale Law School, ISP, Fellow

Table of Contents

I. Introduction ................................................................................................................................................. 3

II. Social Networks: A Virtual Sphere Inhabited by Employees
   A. Preface .................................................................................................................................................. 10
   B. Screening Social Networks Data - Prior to Employment................................................................. 12
   C. Tracing Employee Data on Social Networks During Employment ............................................. 17

III. To Read Or Not To Read? The Problems With Employer Invasion of Employee Data In Social Networks ......................................................... 20
   A. Disregarding Antidiscrimination Norms – The Problem Of Irrelevant Data ............................. 21
   B. Misleading Social Network Policies – Intention Expectation of Privacy ...................................... 23
   C. Unequal Bargaining Power ............................................................................................................... 25
   D. Cognitive Biases – The False Perception of Privacy ....................................................................... 26
   E. The Right to be Forgotten.................................................................................................................. 27
   F. Data Posted by Third Parties ........................................................................................................... 28
   G. Dignity and Psychological Reasoning ............................................................................................... 28

IV. The Psychology Balloon / Magnet Field Theory
   A. Introduction .......................................................................................................................................... 29
   B. The Psychological Importance of Privacy ......................................................................................... 31
   C. The Balloon Theory ............................................................................................................................ 33
   D. Personal Health and Welfare ............................................................................................................. 36
   E. The Efficiency Advantage of Privacy ............................................................................................... 37

V. Alternative Legal Tools ................................................................................................................................. 37
   A. Status Quo: Oppression of Employee Privacy in the Virtual Sphere ........................................... 38
      1. The Governmental Sector ............................................................................................................... 40
      2. The Private Sector .......................................................................................................................... 41
   B. A New Horizon: Alternative Legal Tools ....................................................................................... 42
      1. The Least Invasive Means .............................................................................................................. 43
      2. Obeying Other Laws – Antidiscrimination Laws ....................................................................... 45
      3. Transparency and Informed Consent ........................................................................................... 45
      4. Inspection, the Right to be Heard and the Right to Appeal ....................................................... 49
      5. Specific Legitimate Purpose ......................................................................................................... 49
      6. The European Approach to Privacy in the Workplace .............................................................. 50

VI. A Shift to a Different Attitude: Securing a Virtual “Private Zone”
   A. Legislation Forbidding Employer Access to Employee Social Media ....................................... 54
   B. Court Decisions in Favor of Employee Privacy .............................................................................. 56

VII. Summary and Conclusions ..................................................................................................................... 60
I. 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.²

Currently, the most popular social network, Facebook, has over one billion users alone, equating to one-seventh of the world's population.³ Two-thirds of online American adults (67%) are Facebook users.⁴ Although social networks started in a social context they have become a significant work tool for employers in everyday practice, used as a tool for “screening” to track the personal data about applicants, employees or former employees that is posted on social networks, websites, and in other virtual spheres. There is, for example, the case of Ellen Simonetti, a flight attendant for Delta Air Lines who was dismissed after posting inappropriate photos of herself in the company’s uniform in her Blog;⁵ Stacy Snyder, a 25-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,

² Jocelyn M. Lockhart, Facebook as a Job Screening Tool: Are Sales Employers Discriminating Against Job Applicants based on their Facebook Profiles?, 1, 6-7 (April 2013) (unpublished honors thesis, University of Southern Mississippi), available at http://aquila.usm.edu/cgi/viewcontent.cgi?article=1142&context=honors_theses (the significant growth in employer that currently use or always search social networks data in the hiring process).
³ Mark B. Gerano, Access Denied: An Analysis of Social Media Passwords Demands in the Public Employment Setting, 40 N. Ky. L. Rev. 665 (2013) (Social media is not only "social," and isolated to "non-business" settings, but is also spread across all facets of society. Because of its increased prevalence in society, problems have arisen, including issues involving the use of social media in the workplace. This article discusses one of those problems: how far can a public employer investigate the social media content of a job applicant? In addition to various social networks like Facebook, blogs have increased in popularity, growing from 36 million in 2006 to over 181 million in 2011).
To Read or Not To Read: Privacy Within Social Networks, The Entitlement Of Employees To A Virtual “Private Zone” And The Balloon/Magnet Field Theory,
Dr. Shlomit Yanisky Ravid, Prof. of Law. Yale Law School, ISP, Fellow

with the caption “Drunken Pirate”,⁶ in Stengart vs. Loving Care, unknownto Stengart, executive director of nursing, certain browser software automatically made a copy of each web page she viewed and saved that information on the computer's hard drive;⁷ in the case of Lazette vs. Verizon, an employee’s supervisor at Verizon read 48,000 of her emails, even after she had stopped working for the company.⁸ All of these examples reflect the new era in which employers and employees use digital media as an integral part of everyday life and, more importantly, as a major and a basic means of communication, preferred to more limiting or inconvenient alternatives (i.e. sending a paper letter of invitation or printing pictures instead of posting them in Instagram or Facebook).⁹

This paper 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 or wrong and legal or illegal? In this paper I claim that guiding principles, notwithstanding technical capability or economic feasibility, but rather stemming from social rationales, should shape the legal norm and strike a balance between conflicting interests.

In the past twenty years, businesses and employees as private people alike have embraced the use of computers, electronic communication devices, the Internet, social networks and e-mail. As those and other forms of technology evolve, the line

---

⁸ Lazette v. Kulmatycki, No. 3: 12CV2416, 2013 WL 2455937 (N.D. Ohio June 5, 2013). (When Lazette was aware of the defendant's actions she changed her password. Among the contents were communications about plaintiff's family, career, financials, and other personal matters).
⁹ Lockhart, supra note 2, at 2.
separating business from personal activities can easily blur. In the modern workplace, for example, occasional personal use of the Internet is commonplace. Yet that simple act can raise complex issues about an employer's monitoring of the workplace and an employee's reasonable expectation of privacy.\(^{10}\) Within the virtual domains, such as the Internet, we can hardly distinguish between workplace property and private “zones.” Standard modes of communication have changed dramatically. Living in the digital era, today’s employees, including applicants and former employees, have few, if any, viable alternatives to communicating with the “world” without using the virtual space (such as e-mail, websites, social networking/Facebook, Skype, and so on and so forth). Many employees today carry the newest portable digital devices, like 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 than to use their employers’ virtual spheres to access basic means of communication, either by visiting social networks or writing e-mails. Under these circumstances, dedication to a job or mere employment does not justify the entire loss of privacy.

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 broader and even unlimited, as it can embrace many venues and means of monitoring employees.\(^{11}\) One of the

\(^{10}\) See Stengart, 990 A. 2d at 654-655.

\(^{11}\) For example, employers can intervene in employees’ private means of communication, in addition to reading private text messages in e-mail accounts or mobile phones and other devices, by tracking on-line activity, through surveillance of web postings, by tracking a person’s location using GPS or voluntary social media “check-ins,” and so on and so forth.
most common violations of employee privacy, which has recently increased dramatically, is the tracking of private information posted about employees on social networks, either by the employee herself or by a third person. This matter is the focus of this article.

The new realm of social networks brought a bundle of new and unexpected challenges stemming from the intersection of the workplace and individual space in the digital era. This paper addresses the question of whether applicants and employees who actively participate in the virtual world and communicate with others actually waive their right to privacy in data when it is in any way accessible to their employers. In other words, should the law shield an applicant 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, providing employees protection from employer intrusiveness. In other words, employees should have a reasonable “private zone” within the wired/digital/virtual premises that are accessible to the employer, even when using corporate network tools or Internet accounts, even during working hours, and even more so while not using the employer 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 resulted in employees in the public as well as private sector almost entirely losing a 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” to 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” (“magnet field theory”), describing 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. This theory is consistent with laws and/or court decisions in some jurisdictions outside the U.S., which found different venues to secure employees’ privacy (i.e. E.U. Regulation).12

Some scholars have discussed the question of privacy at the digital sphere in general13 and in social networks14 in particular. Other scholars have addressed the question of privacy at the workplace.15 Most of the works are descriptive, revealing the new virtual spheres and pointing out new problems emerging in the new era. Some of the scholars have justified and supported employers' usage of information posted by employees. Some explained the

---

12 See infra, Section V.B.6
To Read or Not To Read: Privacy Within Social Networks, The Entitlement Of Employees To A Virtual “Private Zone” And The Balloon/Magnet Field Theory.

Dr. Shlomit Yanisky Ravid, Prof. of Law. Yale Law School, ISP, Fellow

benefits and efficiency of using this information, for example in the screening stage (without the awareness of the candidate), compared to the old tools of resumes and interviews.\(^{16}\) Not one of the scholars, however, explained the contradiction between this de facto waiver of privacy in online posts and the reasoning behind most user’s interest in protecting their data. This article suggests, innovatively, that privacy rights in data posted on social networks by employees do exist.

This article not only argues the case for a more balanced approach to employee privacy, but it also suggests a new desirable model for policymakers to adopt. Inter alia, this solution should be part of the current governmental discourse about privacy protection within the workplace. It concludes with several suggestions, including adding hard law attributes to the proposed instruments, toward effective implementation and genuine progression of attitudes protecting/securing/enabling workplace privacy in this global, digital age. Accordingly, I conclude that we should reconsider the tests relating to privacy in order to secure a threshold of “Private Zone” within the virtual

workplace. A new and needed policy may implement other new tests or make use of existing tools, such as for example the “Least Invasive Means” (the Proportionality Analysis), instead of barring this important right with its major implications on employees and, therefore, on workplaces.

In the first part, after the introduction, the article describes the virtual sphere inhabited by employers. The next discussion 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 can be concisely described as the “balloon” or the "magnet field" theory which describes an important 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 describes briefly the American legal norm, leading to the introduction of a contrasting attitude from a different legal system. This part suggests a rethinking of the current U.S. regime regarding privacy and discusses recommendations for alternative legal tools to be adopted by policy-makers. I conclude with attention to a new tendency of recent U.S. holdings protecting privacy right of employees and candidates. New legislation preventing employers from requesting employees’ passwords to social network accounts as well as certain court decisions reflect the creation of private zones within the virtual spheres of workplaces, strengthening the conclusion of this study.
We start with explanations and demonstrations of violations of employees’ privacy within the virtual spheres.

II. SOCIAL NETWORKS: A VIRTUAL SPHERE INHABITED BY EMPLOYEES

A. Preface

Social networking sites have emerged as a rich source for candidate information with the tremendous number of online profiles, providing users a forum for interaction through a variety of outlets, including but not exclusive to wall-posts, tweets, hash tags, picture tagging and the ability to share pictures, videos, and music.\(^\text{17}\) Facebook, arguably 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.\(^\text{18}\) When creating profiles, users provide essential information about themselves, including their name, gender, date of birth, preferred language, interests, relationship status, sexual preferences, location, education, and other personal information.\(^\text{19}\) In these publicly accessible virtual spaces, users disclose information about themselves and all kinds of thoughts by posting notes, pictures and other media sources about what they do or think, their drinking habits, parties, trips, updating profile information, commenting on articles, and sharing media.\(^\text{20}\)

\(^{17}\) Lockhart, supra note 2, at 4.
\(^{18}\) Id.
Today, more than 1 billion people have information about themselves published on social networks; Facebook alone declared 1.23 billion users. Not surprisingly employers have devoured this source of information as a 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.

Daniel Solove has identified four basic categories of activities which harm privacy interests: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion. When addressing the questions of the boundaries / margins / limits of the permissible regime regarding employer tracking of employee personal data, all of these categories should be considered.

Focusing on data posted on social networks, Sánchez Abril, Levine and Del Riego described three ways in which employers are actively screening on-line data of employees: (1) monitoring and surveillance of employee social media profiles, (2) evaluation of applicants’ social media profiles and online speech in the hiring process, and (3) limiting employees’ off-duty online activities. 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 this tool while seeking work, whereas the employers rely on social media while searching for applicants and

---

22 Pike et al., supra note 19, at 57; Ghoshray, supra note 16, at 558.
23 DANIEL SOLOVE, UNDERSTANDING PRIVACY 103 (2008) (arguing that privacy has no single definition but rather is a plurality of different things).
gathering information about existing and potential employees. Businesses monitor sites like Facebook and Twitter in search of information that may provide insight about prospective hires, while individuals can learn more about what it is like to work at a particular organization.\(^{25}\)

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 might never know why.

**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.\(^{26}\) Instead of just using old fashioned and inefficient tools like resumes and interviews, which are an applicant’s control, hiring managers nowadays often rely dramatically on information gathered from the internet, without the awareness or consent of the person subject to the surveillance. How popular are such screening methods? Research found that the majority of employers participating in the studies consider online screening a formal part of their hiring process; an overwhelming eighty-nine percent (89\%) of employers use social media sites as a
means of researching job applicants throughout the interviewing process. Sixty-three percent (63%) of U.S. recruiters surveyed have rejected applicants due to online content found in a non-business context. Professional entities are available to build candidate profile based mainly on social networks but also on different forums, including blogs, shopping lists, participation in events and memberships in organizations.

An empirical study examined the question as to what extent social networking websites actually influence the decisions of hiring managers. The results reveal that the majority of respondents of the study (72.7%) strongly agreed that they had used a social networking website within the past twelve months to recruit a prospect. Seventy-three percent (73%) either agreed or strongly agreed that social networking websites provide meaningful insight to prospective employees. Eighty two percent (82%) of respondents strongly agreed or agree that they would be likely to increase their use of social networking websites to recruit prospects within the next twelve months. Equal votes were declared for the statement that a rejected applicant has the right to know / should be informed of online content’s contribution to his or her rejection. In general, according to survey results, participants believed to a reasonable degree that the content available on social networking websites provides meaningful

27 Lockhart, supra note 2, at 1.
28 Id. at 7.
29 Companies like Social Intelligence Corp. offer a “solution” for applicant assessment and staff monitoring to employers, offering products that provide a “comprehensive picture of an applicant’s complete publicly available online presence” and “Continuous Insight: Monitoring for enforcement of company policy and protection against insider threat.” See http://www.socialintel.com/products-and-solutions/employment.html, last visited March 22, 2013.
30 Cook, supra note 4, at 9-10 (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. Managers involved directly in hiring decisions were the ones contacted and selected for participation).
information about potential workers. Accordingly, scholars have predicted that online recruitment efforts will continue to replace traditional methods, such as job fairs, newspaper ads, word of mouth, and on-campus recruiting.

Ross Slovensky and William Ross described managerial and U.S. legal issues associated with using social networking web sites for personnel selection. They also concluded that using social networking web sites to screen applicants offers great benefits to organizations, in the form of gaining a large amount of information about applicants, which may replace other information (e.g. a resume) or be used to supplement other tools. It may also help a firm address legal concerns about potential “negligent hiring” claims. While the authors are not concerned about data collection, they stated that the main disadvantage was pursuant to legal considerations of using such information. Therefore, they suggest a solution of checking and adjusting company policy to comport with the law.

Pike, Bateman and Butler continue the discussion, explaining why screening is so attractive and beneficial to employers as well as the risks of using social network data. They pointed out that the information in social networking websites is efficacious because the applicants are not aware of the process as well as the outcomes. Most of the common methods traditionally used for hiring use interactive observation strategies such as resumes and formal interviews. The main drawback

---

31 Cook, supra note 4, at 9-10.
32 Id. at 5.
33 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 (2012) (Managers can devise policies that provide the firm with appropriate information while respecting applicant privacy and complying with U.S. legal and ethical expectations.).
34 Pike et al., supra note 19.
of these approaches is that the candidate is aware of the observation and has the opportunity to strategically craft information for the specific audience. Passive observation is considered to be more informative because candidates are not explicitly aware that they are being observed. However, passive observation has not been typically used because it is time consuming, expensive, and sometimes simply impossible to conduct. Social networking sites are changing this. Social network-based information can be passively observed by hiring professionals with relatively little effort and without the candidate being aware of the observation or its focus.37

Furthermore, since information within social networks is persistent, searchable, and replicable, social networks are a valuable source for hiring professionals confronted with otherwise limited information for assessing fit between a candidate and an organization.38

Enthusiasm for online screening procedures continues with another empirical study, which examined the psychometric properties of personality traits (“the Big Five”) assessed through social networking profiles.39 The results included a number

---

of 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. The study suggested that social networks may provide useful information for use in organizational research and practice with one broad limitation taken into consideration: various legal and ethical issues.

Indeed, the hiring process is challenging, as a lack of quality information does limit the discovery of a candidate’s true nature, potentially leading to adverse impacts. Lost productivity, wasted time, lower morale, and disruption for clients are just a few of the negative consequences of hiring the wrong people. While social networks are a potentially useful source, the information available through most of them is not submitted by candidates through any formal, established application process. As a result, it may be outdated, incomplete, or even fraudulent. This creates a tension around the quality of social network information: While social networks may be a rich source, the possibility of irregular and variable information increases the need for information users to make judgments about its quality. This is part of a larger emerging trend requiring users to demonstrate “information self-sufficiency,” or being responsible for making determinations of quality on unmediated information.

and in total accumulated 378 ratings. The results revealed that the judges were consistent in their ratings of the subjects and were able to differentiate between the top and low performers based on their Facebook profiles. The study suggested that social networking sites might be more reliable than other forms of personality assessments, such as interviews or resumes, because the candidate is more truly themselves on their Facebook profile than in these professional settings. Facebook reveals enough interaction with others and personal information to offer a fairly accurate illustration of the individual’s personality.

Kluemper et al., *supra* note 39, at 1.

The cost of recruiting and training replacements alone ranges from 25% to 500% of an employee’s salary. Hiring professionals attempting to identify the best candidate for a position are faced with a complex information problem. See Pike et al., *supra* note 19, at 56.
Although recently in the literature there has been a growing awareness of the importance of social network information in employment contexts, it has largely been limited to anecdotal accounts and speculative discussions of how social networks might be used.\textsuperscript{42}

Pike, Bateman and Butler, while not challenging the data gathering by employers at all, declared their concern regarding the quality that arises when social network information is used by hiring professionals, pointing out that a lack of quality information inherent in hiring decisions based on social network data makes it impossible to discover the true ability of candidates prior to employment.\textsuperscript{43}

While risks in using social network data exist, Donald H. Kluemper found that it is widely established that many hiring managers view websites such as LinkedIn and Facebook in the employment selection process, leading to the acceptance or rejection of job applicants. As an emerging employment selection tool, screening via social networking sites demonstrates potential as a rich source of applicant information, but, due to the rapid evolution of social media, scientific study of social networking sites has been substantially outpaced by organizational practice. Therefore, Kluemper offers human resources practitioners a wide range of considerations toward development of an effective social network screening policy while also making the case for academics to pursue further research in this nascent area.\textsuperscript{44}

\textsuperscript{42} See Slovensky & Ross, supra note 33.
\textsuperscript{43} Pike et al., supra note 19 (They suggested to consider the tension within several dimensions of information quality: accessibility (open-restricted), contextual (relevant-unsuitable), and intrinsic (reliable-questionable)).
\textsuperscript{44} Donald H. Kluemper, Social Network Screening: Pitfalls, Possibilities, and Parallels in Employment Selection, in Social Media in Human Resources Management (Advanced Series in Management, Volume 12) 1, 2 (Tanya Bondarouk, Miguel R. Olivas-luján, eds., 2013).
To conclude, undoubtedly, the hiring process has changed dramatically since the advent of social networks. The position that courts would, of course, be very important. However, since the process of social network mining for insights to job applicants remains unknown and therefore non-examinable, there can hardly be cases on point to this issue. However, tracking data posted in social networks doesn't end with the hiring process: employers are looking at data posted by and about employees throughout the employment period. This phase will be the focus of the next subsection.

C. Tracing Employee Data on Social Networks During Employment

The practice of tracking information posted by employees in their own private social network accounts gives rise to even more legal questions vis-à-vis screening, as it affects working conditions and may lead to dismissals and loss of positions. Many cases were recently brought, in addition to those described in the first part of this article, over dismissals of employees or denials of employment benefits due to data posted in social networks. For example: a nurse employed at a California hospital was fired after posting a Facebook status from her home to various friends, virulently complaining about work on her birthday and other days (“Instead of spending my birthday celebrating, I will be working all night cleaning up feces…Thanks to the …, not only am I working Mother's 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”).  

45 Guevarra v. Seton Medical Center, No. C 13-2267 CW (N.D. Cal. Dec. 2, 2013) (She also threatened her supervisors) [available at
Facebook “friend” shared this content with the employer. The nurse (Guevarra) was put immediately on administrative leave. She had received no prior warnings or reprimands. The next day, Guevarra was told that, upon review of her case, she was terminated, effective immediately. Not only was she discarded but she was also denied unemployment benefits, all because of her Facebook statement. The posts were found by an appellate board to be a breach of her obligations to the employer, so as to constitute misconduct connected with employment. Guevarra had violated the employer’s policy because her posting was visible to persons including co-workers and the claimant’s manager and was not analogous to a private communication conducted outside of work, such as one made in confidence to a family member. Consequently, the court granted the employer’s motion to dismiss with prejudice.46

The decision, while discussing various legal questions including freedom of speech, did not mention any privacy issue.47

Other court rulings also avoid discussion of privacy rights, validating actions against employees based on Facebook posts, even those believed to be semi-private (thought to be exclusively available to “friends” or private groups). For example, a 7th Circuit Appellate decision issued by Justice Richard Posner upheld the lower court’s judgment in favor of a daycare center which had dismissed an employee on the basis of hostile and profane Facebook posts. Justice Posner did not challenge the tracking of

---

46 Id.
47 On the other hand, an employee fired for using Facebook on company computers – in violation of company policy, which prohibited employees’ use of company property, including the computers, for personal business – was allowed to receive unemployment benefits in Missouri. 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 not the content of the post itself. Edmonds Dental Co., Inc. v. Keener, MLW No. 65026/No. WD75545 (Mo. Ct. App., 2013) (This appellate court remanded the employer’s appeal due to a question of fact regarding the employers) [available at http://scholar.google.com/scholar_case?case=14095840654512450945&hl=en&as_sdt=6,33).
data on social networks. He stated that, even if the center's reason for checking the online profile was not a good one, that is irrelevant if the center honestly believed that the plaintiff wrote the post.\(^{48}\)

The same result was held in the 11\(^{th}\) Circuit at the same period of time. A police department employee sued, claiming that she was not promoted in retaliation for Facebook postings, in which the plaintiff had criticized her colleague for interfering in an unethical manner with the investigation of a person the plaintiff had arrested for fraud and financial identity theft. The Facebook page was “set to private” but was available for viewing by an unknown number of plaintiff's “friends,” who, of course, could potentially distribute the comment more broadly. The Facebook comment launched an investigation of violation of the department's work rule requiring that any criticism of a fellow officer be directed only through official department channels. Summary judgment was granted to the employer and upheld on appeal: the police department’s legitimate interests in requiring that any employee grievances be addressed internally and privately were deemed to outweigh any first amendment interests of the employee.\(^{49}\)

To conclude, the court noted that “[p]rivacy in social networking is an emerging, but underdeveloped, area of case law” with consistency in case law at two extremes, one which allows Internet users NO expectation of privacy, and the other which says “there is a reasonable expectation of privacy for individual, password-protected


online communications.”"\(^50\) The claim of this article about the option of protecting, up to certain level, privacy in social network publications is not even mentioned.

III. 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, both with respect to control of the screening process and in courts hearing legal challenges, there is a basic set of legal concerns generated by the clash between privacy and the internet. 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.

\textit{A. Disregarding Antidiscrimination Norms – The Problem Of Irrelevant Data}

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.\(^51\) Many employer actions and measures are limited and even forbidden under Title VII and other antidiscrimination laws. The hiring process is no exception. Whereas employers cannot ask applicants, during interviews, questions about factors such as race, sex, or nationality, much of this protected information can

\(^50\) The emphasis is in the original. Deborah Ehling v. Monmouth-Ocean Hospital Service Corp., et al., 872 F. Supp.2d 369, 373 (D.N.J. 2012) (A New Jersey hospital employee prevailed in her suit alleging common law invasion of privacy, in a case where an employer demanded a co-worker with “Friend” privileges to the Plaintiff’s Facebook pages display the profile to management, which subsequently took disciplinary action against the employee on the basis of her Facebook commentary, which Plaintiff believed to be protected by high privacy settings.) (available at http://scholar.google.com/scholar_case?case=9859139938102599616&q=pietrylo+v.+hillstone+rest.+group&hl=en&as_sdt=6,33&as_vis=1).

be easily discerned from data posted on a social media website, including individual profile pictures.52

Typically, employers discriminate against job applicants who have Facebook pages that exhibit unacceptable or inappropriate behaviors or lifestyles. Fifty-three percent (53%) of employers are biased against candidates whose Facebook pages reveal provocative or inappropriate content, while forty-four (44%) discriminate against profiles exemplifying alcohol or drug abuse.53 When a hiring manager sees a profile photo, for instance, it may be very difficult to disassociate that image from the applicant’s name. While regulations for employment decisions exist, the use of social media in recruiting and applicant screening functions makes such regulations challenging to define and even more difficult to enforce.54

People use social networks for social purposes. According to Peluchette and Karl, students make a conscious effort to portray themselves with a certain image on Facebook. Those who portrayed an image of themselves that was sexually appealing, wild, or offensive were most likely to post “inappropriate” information. Approximately fifty percent (50%) of the students in the study have profiles that exemplify a party lifestyle, including profanity, comments, and photos involving alcohol.55 Students readily post suggestive content on Facebook because they believe that their postings will not be seen by anyone outside of their own friend groups.

52 Cook, supra note 4, at 8.
53 Lockhart, supra note 2, at 1.
54 Cook, supra note 4, at 9.
55 Joy Peluchette & Katherine Karl, Social Networking Profiles: An Examination of Student Attitudes Regarding Use and Appropriateness of Content, 11 CYBERPSYCHOLOGY & BEHAVIOR (2008) (a survey of 1,150 hiring managers on the intensive use social networking sites as a form of job screening); Lockhart, supra note 2, at 7.
Unfortunately, this is simply not the case. Studies reveal that sixty three percent (63%) of employers who declared using social networks in the hiring process said they decided to not hire a person based on what they found on the candidate’s social networking site.

To avoid legal problems, employers must keep adequate records and be mindful of particular electronic communication laws, many of which vary depending on one’s industry or geographic location. Ideally, companies should have solid selection processes with imbedded screening in place to minimize the need for social media use within those procedures.

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

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

The main question which this article addresses innovatively is the contradiction between, on one hand, social network users’ waiver of privacy by 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 for several reasons. The misleading and vague privacy policies of social network websites is mostly influenced by their business method, which is to commercialize the private information posted by users to other entities, either commercial or

---

56 Lockhart, supra note 2, at 7.
57 Id.
58 Cook, supra note 4, at p. 9.
To Read or Not To Read: Privacy Within Social Networks, The Entitlement Of Employees To A Virtual “Private Zone” And The Balloon/Magnet Field Theory,
Dr. Shlomit Yanisky Ravid, Prof. of Law. Yale Law School, ISP, Fellow

governmental ones.\textsuperscript{59} Certain social network corporations purposely post an unclear and flexible privacy policy, which frequently changes.\textsuperscript{60} The result gives great latitude to the company, enabling it to promote its own interest of gaining profit from users with unprotected privacy.\textsuperscript{61} A lack of transparency regarding commercialization of personal data by social network entities encourages user posting of personal data.\textsuperscript{62} The term “privacy policy” in itself creates a false illusion of privacy among users who believe they can protect personal data.

For example: the privacy policy of Facebook declares that if a user chooses to protect pictures under a privacy policy choice, unknowingly, the protection does not include “albums” of pictures.\textsuperscript{63} But 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 she 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 “album” that is not automatically protected in the same manner individual photos would be is that multiple pieces of information are combined together to paint a holistic picture of an

\textsuperscript{59} See Sharon Hannes & Lital Helman, Corporate Responsibility of Social Networking Platforms (TBP) (They propose a new approach to address this challenge of using personal data on social networks: to link executive compensation in social networking firms to users’ satisfaction from the firm’s data management practices). Avi Goldfarb & Catherine Tucker, Online Advertising, 81 ADVANCES IN COMPUTERS 289, 292-94 (2011) (data in the web shared by commercial and non-commercial entities, such as employers and the government).


\textsuperscript{61} Hannes & Helman, supra note 59.


individual. This tremendously harms privacy rights, where a poster setting a high privacy setting to a specific photo might expect that setting to apply to the “albums” she creates. Clearly, there can much more diverse information gleaned from an “album” of various photos than from a single picture, so exposure of these pieces, gathered all together, deserves special awareness and ought to require explicit user acceptance.

In general, users also assume that their data will be exposed only to the group they can think about while posting (especially if they are diligent in controlling privacy settings) and not to third parties as employers.64 However, as the previously cited cases and scholarship establish, employers can and do look at employee social media profiles, whether the employees realize it or not.

C. Unequal Bargaining Power

Imagine you are a job applicant hoping to get a job. The employer asks you whether you have social network accounts. You know the purpose of the inquiry. To protect private content from the general public, you have information password protected so only “friends” can see it. Even though the employer does not ask you for the password, you know that you had better become a “friend” with the employer.65 Due to the gap in bargaining power between an applicant and a hiring employer, the employer in this scenario places the applicant in a very difficult position.

That awkward moment might even evolve into something worse upon hiring, when the employer demands the password to all employee e-mail and social network accounts. There’s really not much difference between demanding the keys to your

---

64 But should social network corporations be responsible for maintaining user privacy, or should employers be accountable to their current and potential future employees? 65 Gerano, supra note 3, at 665.
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’re not at work or at school, your health concerns, religious activities and political affiliations, and much, much more.66

Being aware of this dilemma, states as well as Congress have begun passing laws to forbid employers from requesting personal passwords from employees.67 Will such laws adequately address the problem? I argue that, due to the unequal power of bargaining, the laws may help but do not cure the entire issue. Job applicants will still face the dilemma of either voluntarily becoming a friend and exposing their social lives out of a professional context or getting excluded from the hiring process.68

Mark B. Gerano examined the extent to which public employers may investigate the social media content of a job applicant, also discussing the new legislation about employers’ access to passwords. He concluded that in some cases, such as in criminal law, there should be no restrictions.69

Recent technological changes have made it easier, faster, and cheaper than ever for employers to engage in surveillance of their workers. Many employers efficiently make use of technologies to monitor and, more fundamentally, control their employees’ behavior at a granular level that was not previously possible.

---

67 Gerano, supra note 3, at 665. See National Conference of State Legislatures, Employer Access to Social Media Usernames and Passwords at http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx (last visited Mar. 21, 2014). 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 §§49.44.1-.2 (2013).
68 Gerano, supra note 3, at 665.
69 Id.
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. As a society, we must direct thought to the idea that full-grown adults are subjected to routine surveillance of their activities, to which they passively submit just to hold the jobs the need to pay their bills and provide for their families.70

Eventually, information asymmetries might cause a market inefficiency failure.71 Applicants and employees as social networks users are poorly positioned against employers as well as the social network corporations to take a stand on their rights because of bargaining power asymmetry and lack of information.72 Applicants and employees neither know nor have ways to find out what personal information has been gathered by the employers, or when and how often the information will be used.

**D. Cognitive Biases – The False Perception of Privacy**

What perceptions and expectations do people, especially young people, hold regarding privacy on the world wide web? Cognitive biases may serve as the basis of irrational behavior by users who expect privacy in personal data on social networks. Optimism bias, for example, can explain trust in third parties to avoid using personal data of the users against the users’ interest.73 Other biases, such as regarding short term and long term risk, loss aversion or crowd bias, all lead users to fallaciously trust

---

70 Catherine Crump, Your Boss Shouldn’t Read Your Email, FREE FUTURE (Jul, 16, 2013), https://www.aclu.org/blog/technology-and-liberty/your-boss-shouldnt-read-your-email.
71 ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 41 (2d ed. 1997).
policy makers, social networks fairness and the law, especially since most imagination are restricted to current known risks.\textsuperscript{74}

\textbf{E. The Right To Be Forgotten}

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.\textsuperscript{75}

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 the social network services. The case of data posted by third parties is even worse, as the user cannot, in many cases, delete it, even if aware of the data’s presence at all.\textsuperscript{76}

\textbf{F. Data Posted By Third Parties}

Users of social networks might control their own posts. However, a lot of data – written or pictured – is posted by third parties. Thus employees (or future employees) lose control, which he could never have had, of private details about themselves. Here, even changing the setting to one of anonymity is not an option.\textsuperscript{77}


\textsuperscript{76} Laura Lagone, \textit{supra} note 25.

\textsuperscript{77} The Facebook privacy policy describes the ripple effect of third party posts, tags, “likes” and other interactive tools at https://www.facebook.com/about/privacy/your-info-on-fb (last visited Mar. 24, 2014).
G. Dignity and Psychological Reasoning

Among other risks and harms caused by invasion to someone’s privacy lie the detriment to personal traits, such as autonomy, freedom, and dignity. People whose privacy has been invaded and have had personal information used against them have experienced mental injury and helplessness. There is significant research that, in the workplace, employees who feel a breach of trust may experience emotional distress, feelings of betrayal, anger and other emotions that affect the employee’s overall behavior and sense of loyalty to the organization.

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.

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

A. Introduction

“I felt total incomprehension, I was stunned,” said Ms. Paulin, a 12-year employee of the Swedish home furnishings group IKEA, after she was forced out of her job after the company was said to have provided a private detective with her Social Security number, private cell-phone number, bank account details and other personal data, accusing her of having false claimed to be ill. She left the
To Read or Not To Read: Privacy Within Social Networks, The Entitlement Of Employees To A Virtual “Private Zone” And The Balloon/Magnet Field Theory,
Dr. Shlomit Yanisky Ravid, Prof. of Law. Yale Law School, ISP, Fellow

dismissal meeting confused and distraught, feeling “robbed of myself and my reputation.” A few days later, Ms. Paulin attempted suicide.80

Ikea’s investigations were conducted for various reasons, including the vetting of job applicants, efforts to build cases against employees accused of wrongdoing, and even attempts to undermine the arguments of consumers bringing complaints against the company. The case has caused public outrage in France because the spying cases 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. 81

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

---

80 Nicola Clark, Revelations That Ikea Spied on Its Employees Stir Outrage in France, N.Y. TIMES, December 15, 2013, at B3 (One of the emails from Mr. Paris, 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. 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, the finance department of Ikea France approved more than €475,000 in invoices from investigators). available at: http://www.nytimes.com/2013/12/16/business/international/ikea-employee-spying-case-casts-spotlight-on-privacy-issues-in-france.html?smid=fb-nytimes&WT.z_sma=BU_RTI_20131216&bicmp=AD&bicmlkp=WT.mc_id&bicmst=1385874000000&bicmet=1388638800000&fblinkge0&_r=0 (last visited Mar. 24, 2014).
81 id. (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, the finance department of Ikea France approved more than €475,000 in invoices from investigators).
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, yet 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. In other words, despite granting employers access to information about their private lives by exposing themselves online, respondents expect that work life and private life should be generally segregated—and that actions in one domain should not affect the other.  

Furthermore, portable electronic devices are now pervasive and increasingly dominate everyone’s life. Thus, some people who are aware of the potential outcomes of a possible violation of their privacy pay a price, avoiding any kind of Internet expression, becoming virtual cripples, choosing to stay behind as current popular means of communication advance.

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

---

82 Abril et al., supra note 15, at 65-66 (empirical data reveals that new employees’ stated expectations of privacy appear to be somewhat paradoxical: employee respondents generally want privacy from unintended employer eyes, and yet they share a significant amount of personal information online, fully knowing it could become available to employers and others.).

83 Michael Z. Green, Against Employer Dumpster-Diving for E-Mail, 64 S.C. L. Rev. 323 (2012) (argues that the rise to ubiquity of portable electronic devices (Blackberries, i-phones, i-pads, Androids, etc.) that blur the workspace with private spaces and blend work-time and private-time, calls for a rethinking of traditional distinctions and a new emphasis, not on employees’ reasonable expectations, but, rather, employers’ reasonableness in monitoring workers). See also United States v. Ziegler, 456 F.3d 1138, 1144 (9th Cir. 2006) (withdrawn on rehearing).
B. The Psychological Importance of Privacy

Virtual tools play an essential role in the definition of the person “identity,” “self,” “self-expression,” and “self-identification.” 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. The virtual spheres influence this consciousness, as related to privacy, because they do not depend on or stem from tangible assets or physical reality. In other words, privacy actually exists within our minds and souls. Privacy is the way we perceive privacy. This insight leads to the conclusion that differentiating between tangible and virtual spheres in their legitimate influence on privacy rights discourse or an expectation of privacy may be misleading.

Perceiving the consciousness as the intermediary between the cause of violated privacy and the psychological outcomes thereof justifies the interconnection, as has been made in the legal literature, between the right to privacy (including within a virtual sphere) and important values embedded in psychological concepts such as freedom, dignity, autonomy of the persona, selfhood and human relation.

“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,

---

84 Green, supra note 83, at 326-330.
85 Mihaly Csikszentmihalyi, Introduction, in OPTIMAL EXPERIENCE: PSYCHOLOGICAL STUDIES OF FLOW IN CONSCIOUSNESS 10, 17 (Mihaly Csikszentmihalyi, Isabella Selega Csikszentmihalyi, eds., Cambridge University Press, 1998). (Consciousness is the information system that could differentiate among variety of stimuli that could choose certain stimuli and focus selectively on them and that could store and retrieve the information is a usable way).
the kind of religious and political beliefs we hold, or the information we wish to divulge about ourselves.” 87

Scholars and jurists have suggested many definitions of privacy without having settled on any one as the right one. 88 I hold the notion that, 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. 89 The levels, boundaries or content of what is considered private differ among situations, cultures and individuals, but share basic common themes. One of them is the wish to remain unnoticed or unidentified in the public realm (anonymity). 90

C. The Balloon / Magnet Field Theory

This sphere of privacy consists of our perception about information and emotions can be analogized to the concept of an intangible “balloon” (or magnetic field) that always accompanies a person wherever she or he goes within the public domain and when perceiving an encounter with other people or actually interacting

88 The most famous one is “the right to be left alone.” Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890).
89 Solove et al., supra note 2386, at 39-42 (different definitions of privacy).
To Read or Not To Read: Privacy Within Social Networks, The Entitlement Of Employees To A Virtual “Private Zone” And The Balloon/Magnet Field Theory, 
Dr. Shlomit Yanisky Ravid, Prof. of Law. Yale Law School, ISP, Fellow 

with other people. The size of the “balloon” differs according to the interaction. When we are with family and friends we consciously shrink “the balloon” and share part of it with them. When we are with foreigners or employers we need to save “the balloon” in order to preserve our personal sovereignty. The person may choose the time, place and the level of disclosures of personal information, experience and emotions as well as the company before whom such disclosures are made. The state of privacy is related to the act of concealment. 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. The persons differ from one situation to the other. Different sets of social norms control distinct social settings. 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 subject to sanction for visible deviation from patterned role behavior. Drinking with friends or at a festive celebration is welcome, unlike drinking at the workplace or while driving. Today, the Internet has blurred the borders between social contexts and mixed the different situations, creating a blend, and sometimes a clash, of rights and wrongs. It is ok to take pictures with friends at a costume party, but the same picture, once posted on the web, can cause a person’s dismissal. A person should have adequate freedom to build the “self” and choose

91 Id.  
92 Shlomit Yanisky Ravid, Will the Wolf Dwell with the Lamb? Psychological Relationships in the Workplace, in LIBER AMICORUM ELISHEVA BARAK-UPPICKIN (Guy Davidov and Guy Mundlak, eds., 2012).  
93 Sidney M. Jourard, Some Psychological Aspects of Privacy, DUKE L. & CONTEMP. PROBS. 307, 308 (1966) (physical sickness and mental disease may be the outcome of role-conformity).
how that self will be represented. Likewise, the concept of privacy as limited accessibility enables us to identify when loss of privacy occurs to one self.94

In contrast, one of Professor Jed Rubenfeld’s main claims is that privacy exists within a private sphere.95 This idea is based on the traditional distinction that led to the famous Supreme Court statement in Katz: “What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”96 I suggest that the real meaning of privacy does not exist when there are no others around, as the meaning of privacy and the need to privacy is established when other people may be perceived as invading into this conceptual privacy sphere. It can occur by physical invasion, such as seizure, scrutiny or rape, but most of the time it happens by others finding personal information (surveillance) or asking personal questions (investigation). Privacy, then, is the outcome of a person’s wish to withhold from others certain knowledge as to his past, present or future. The wish for privacy is the desire to be an enigma to others or, more generally, the desire to control others’ perceptions and beliefs by monitoring the exposed information about one’s self.97 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.98 Therefore, I recommend that the classic traditional

94 Solove et al., supra note 23, at 40.
95 Rubenfeld, supra note 90.
97 Jourard, supra note 93.
98 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. As elucidated in the Restatement Second of Torts §§ 652A-652E, the common law protects privacy interests in four distinct contexts: (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. The great majority of jurisdictions have made these four privacy torts part of their common law.) These four categories are based on William L. Prosser, Privacy, 48 Cal. L. Rev. 383, 389 (1960). Tort law is different from employment law as employees are
definition of privacy as “the right to be left alone” should be adjusted to recognize a protected sphere (against disclosure of certain facts) within any public realm. This shift from the state of merely alone to protection of one’s personality explains and justifies privacy at the virtual spheres. Whereas the 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 an employee’s mail. Although the home is the quintessential “private” space in the American legal lexicon, employees have important privacy interests in their private information outside the home, too.

D. Personal Health and Welfare

The experience of psychotherapists has shown that people maintain themselves in physical health as well as psychological and spiritual well-being when they have private space – some locus that is inviolable by others, except by the person’s express invitation. People disclose themselves to those whom they trust and it is reasonable to expect trust to be built before the disclosure. Nevertheless, electronic communication is different than traditional communication. Writing to a computer or keypad tends to seem impersonal. Consequently, messages are depersonalized, often resulting in stronger or more uninhibited text and more

---

100 Restatement (Third) of Employment Law ch. 7, introductory note (Tentative Draft No. 5, 2012) (explaining the right to be left alone as the right to keep certain areas and activities free from intrusion by others as well and protected against outside interference as some activities are considered so much part of individual’s personality).
102 Jourard, supra note 93, at 310.
assertiveness in return.103 In other words, today’s electronically transmitted communications are more likely than more traditional forms to be even more personal and, as perceived by the creator, private in nature. Yet, despite documented adverse effects from psychological and business perspectives, employee monitoring and surveillance remain pervasive in the business world.104

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 employees taking initiative and even better worker health.105 Advantages would be not only to the employer, but to society as a whole.106

VI. ALTERNATIVE LEGAL TOOLS

Given an understanding of the right of privacy as framed by the above-mentioned justifications, policymakers, and scholars ought to rethink the current legal regime regarding employee privacy within the digital sphere in general and with

---

105 Id. See also Jourard, supra note 97, at 308. See also Ethan S. Bernstein, The Transparency Paradox: A Role for Privacy in Organizational Learning and Operational Control, 57 ADMIN. SCI. Q. 181 (2012) (creating zones of privacy may increase performance).
106 See, e.g., Pauline T. Kim, Electronic Privacy and Employee Speech, 87 CHI.-KENT L. REV. 901, 931 (2012), available at http://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=3859&context=cklawreview (asserting that “[b]ecause 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.”).
respect to data posted on social networks in particular, using modern principles to replace or at least reshaping 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 section describes the traditional approach that led to the new reality of an almost total loss of privacy related to information posted in social networks about applicants or employees, both in the public and private sectors. This is followed by a description of suggested legal principles that according 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 unwelcome reading of private mails or text messages in mobile phones and other devices, tracking of employee location, tracking their internet activities and more specifically surveillance of social network postings (i.e. on Facebook), which is the focus of this article. Indeed, courts and lawmakers around the world are having trouble conceptualizing privacy in new technologies. 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.

By applying an “incorrect” or “incomplete” traditional legal interpretation to the virtual era, the U.S. regime has caused American employees to have almost entirely lost their right to privacy within the workplace. The reasonable expectation of privacy test implemented by the public sector, when applied within a modern virtual

---

107 Abril et al, supra note 3, at 64 (the shared unease among lawmakers around the world suggests that they need more information to gauge privacy and behavioral norms for new technologies).
workplace realm, virtually eliminates employees’ privacy rights. The same result of drained privacy rights has been diagnosed in the private sector by Professor 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.\textsuperscript{109} Therefore, moving toward “opt-in” employee “consent” policies would not change this result. Even in cases where the court respects the employee’s privacy in a private sector job, it does not mean that employers cannot monitor or regulate the use of workplace computers: companies can adopt and enforce lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies; employers may discipline employees and, when appropriate, terminate them, for violating proper workplace rules that are not inconsistent with a clear mandate of public policy.\textsuperscript{110} The outcome is that employees have almost totally lost their privacy rights within the virtual spheres of workplaces.

This article argues that the current U.S. legal posture, stemming mainly from court decisions which eventually 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 Supreme Court in its 1987 \textit{O’Connor v. Ortega} decision (recognizing that employees’ tangible workspaces, such as a desk, cubicle, or office, in a public workplace may be deemed as private space)\textsuperscript{111} should be applied to today’s virtual workspaces,


\textsuperscript{111} 480 U.S. 709 (1987).
To Read or Not To Read: Privacy Within Social Networks, The Entitlement Of Employees To A Virtual “Private Zone” And The Balloon/Magnet Field Theory.

Dr. Shlomit Yanisky Ravid, Prof. of Law. Yale Law School, ISP, Fellow

extending the law so as to integrate it with the realities of the digital era. The employee expectation of privacy test as well as other contract and tort theories likewise should be either replaced or adjusted to this notion of virtual workplace privacy zones.

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 its capacity as an employer. Public sector employer 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, whereas private sector workers are governed mainly by explicit or implicit contracts. The prevailing attitude in the U.S. workplace and courts is that e-mail privacy (and, less explicitly, Internet usage in general) as well as tracking of private information on employee Internet posts is not protected, whether originating in the physical workplace or from the virtual sphere, especially when employees use

112 That distinction notwithstanding, the practice of permitting employer intrusion upon employee electronic communication and digital tool usage is prevalent within both sectors. See Paul M. Secunda, Privatizing Workplace Privacy, 88 NOTRE DAME L. REV. 277 (2012) (offers a clear delineation of the differences between the private and the public employment sectors, 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 it is evolving).

113 Famously articulated by Justice Harlan (“there 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.’”), concurring in Katz v. U.S., 389 U.S. 347, 360 (1967). But the Court later 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’)” was not repudiated by Katz, but rather supplemented by the ruling. U.S. v. Jones, 132 S. Ct. 945, 950 (2012).

114 Jolls, supra note 109.
employer computers and networks. Courts have held that employees cannot have a reasonable expectation of privacy related to e-mail or other electronic communications, and federal law is very limited and generally leans away from affording employee privacy, especially when it comes to the specific issue of e-mail. Courts have held that employees cannot have a reasonable expectation of privacy related to e-mail or other electronic communications.  

Physical instruments and spaces have traditionally defined privacy law in the United States. The reasonable expectation of privacy analysis, endemic to privacy jurisprudence, is firmly rooted in the experience of physical space and its surrounding normative circumstances. Policy makers have thus far failed to adjust privacy norms to the new reality that most workers function within a virtual sphere in a way that individual privacy will be at least partially protected.

2. The Private Sector

The reasonable expectation of privacy test developed by the public sector, when applied within a modern virtual workplace realm, nearly eradicates employees’ privacy rights. 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. “Consent” policies,
clearly, are not the answer to safeguarding employee privacy rights within virtual workplaces.

Chapter 7 of Restatement (Third) of Employment Law, on Employee Privacy and Autonomy, summarizes the legal rules relevant to employee privacy in the private sector. The legal rules are based mainly on two fields. One is the law of contracts, in which the most relevant legal tool is the employer policy. The contracts law regime views company policy (often expressed in the form of an employee handbook) as a valid contract, subject to the conditions which validate contracts in general. Employees give implied or explicit consent to surveillance by their employer or prospective employers, although screening might not meet the condition of a contract, as applicants usually don’t know that their data is under scrutiny at this stage. The other realm upon which employment law draws heavily, in terms of privacy issues, is the law of torts, from which the expectation of privacy test is drawn. This brings the test which was developed at the public sector to the private one.118

The ultimate result in both employment sectors is thus the same: employees remain with no actual protection of their privacy in regard to track 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 at 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, but not limited to, social networks.

---

118 Restatement (Third) of Employment Law, ch. 7 (Tentative Draft No. 5, 2012).
An extremely important point is the fact that the mere existence of technical surveillance tools, capable of tracing, and tracking of personal data, does not mean that using them to violate privacy is a permissible norm. There is a gap between what technically can be done 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.

Under the main principle of this study – that employees have the right to a secured “private zone” that protects data about them posted on social networks – policy makers should re-think specifically the existing legal tests and consider replacing them with alternative tools that balance their legitimate interests with employee rights.

1. The Least Invasive Means – Proportionality

Without excluding other alternatives, consider the “Least Restrictive Means” test, usually considered as part of proportionality analysis, as an example for an alternative legal tool. Proportionality analysis has evolved over the past fifty years and is today an overarching principle of constitutional adjudication and preferred for managing certain disputes as a multi-purpose, best-practice standard.

The core of necessity analysis is the deployment of a least restrictive means test, ensuring that the measure does not curtail the right any more than is necessary to


120 Alec Stone Sweet & Jud Mathews, Proportionality Balancing and Global Constitutionalism 47 COLUM. J. TRANSNAT’L L. 73-74 (2008) (In the authors’ view, proportionality-based rights adjudication now constitutes one of the defining features of global constitutionalism, if global constitutionalism can be said to exist at all).
achieve its stated legitimate goals. The idea behind this principle is simple. When there are two or more ways to safeguard a legitimate 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 “right” one.

Applying this constitutional principle to the context of workplaces, whether public or private sector, I suggest using such a least *invasive* means analysis as the applicable test for maintaining virtual privacy of data posted in social networks. If the CV or an interview, or any other data provided voluntarily by the applicant, is available as a means for ascertaining candidate qualifications, then violating privacy in order to gather such information (even from public spheres) would be impermissible. Such a rule of proportionality could be implemented with respect to the issue of employee privacy quite efficiently. Employers should limit incursion of employee “private zones” to extreme legitimate circumstances in which severe, immediate damage may be caused to the employer’s legitimate interests (such as criminal harmful activity by the employee) and 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 other, less invasive alternatives to achieve the same result and if it is 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

---

121 Id. at 75.
invasive than human monitoring of information posted on social networks.¹²³

2. Obeying Other Laws – Antidiscrimination Laws

Any employer action, including cases of legitimate surveillance, is subject to existing laws, including antidiscrimination laws as applicable to workplaces. The fact that certain information is accessible and can be read easily and rapidly does not justify per se the violation of antidiscrimination laws. Therefore, discriminative data should not been looked for by employers; if seen, it should not be taken into consideration in the hiring, promoting or firing of employees or in any other context relating to workplaces. For example, information about gender, age, sexual preference, or religion should be irrelevant to the hiring process in most of the case (unless it meets the demands for permissible distinction).¹²⁴

The same rule which prevents employers from asking applicants questions about their sexual habits¹²⁵ 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” which limit the tracking and the usage of social network information should be established.


¹²⁴ Civil Rights Act of 1964, supra note 51.

3. Transparency And Informed Consent

Current employees as well as applicants should not only be aware of employer policy and its effects, they should explicitly agree to it. Therefore, as a first step, employers should adopt a transparency policy regarding privacy at the workplace, conforming to all other conditions described in this subsection. This policy ought to be in a written form, clear and containing details, inter alia, about the different aspects of privacy incursion by the employer, including internet surveillance on social networks, e-mail surveillance, and computer usage policy. It should be published and accessible to all applicants and employees at the workplace. If the company has an employee handbook, the policy should be included in it. However, all these measures, which represent today’s norm relating to privacy policy at workplaces, are necessary but not sufficient to create a valid agreement with workers. Applicants and employees should explicitly agree to data tracking (under any of the different conditions) and should have a right to refuse these actions.126

One of the most important components to a reasonable privacy policy is employee consent. There are several levels of consent. The first is implied consent, derived from the mere fact of the employee–employer relationship. The second is informed consent, created by potential or actual prior knowledge about the privacy policy. The third is an express consent, in which employers obtain employees’ informed, willing, written and signed consent to any invasion to employees’ 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 the employee, with his signature. The fourth type of consent is one in which policy-makers and lawmakers impose their consent, otherwise the consent (of the weak side usually) is invalid.\footnote{127}

There are two types of employee consent with regard to the details of the violation of privacy: (i) general consent to a policy; and (ii) specific consent to each instance of monitoring.\footnote{128} Is implied consent sufficient for authorizing monitoring data from social networks by employers? Courts have stated that to be sure, under the private party consent to surveillance provision of the Electronic Privacy Communications Act,\footnote{129} consent need not be explicit, but may also be implied.\footnote{130} In a case involving a claim of implied consent under this subject court explains: “[I]mplied [consent] is ‘consent in fact’ which is inferred ‘from surrounding circumstances indicating that the [party] knowingly agreed to the surveillance.’” \footnote{131} Thus, implied consent – or the absence thereof – may be deduced from the prevailing circumstances of a given situation. The circumstances relevant to an implication of consent will vary from case

\footnote{127} But see Yoan Hermstrüwer & Stephen Dickert, Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten 3 (Max Planck Institute for Research on Collective Goods, Working Paper No. 2013/15, 2014) (arguing that consent to disclosure of personal information creates a risk of a chilling effect that increases propensity to comply with social norms, inducing them to forego benefits that norm deviations, such as the exercise of civil liberties).

\footnote{128} Jolls, supra note 126; Levinson, supra note 123.


\footnote{130} Williams v. Poulos, 11 F.3d 271, 281 (1st Cir.1993) (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.” Lazette v. Kulmatycki, supra note 8.).

\footnote{131} Griggs-Ryan v. Smith, 904 F.2d 112, 117 (1st Cir. 1990), quoting US v. Amen, 831 F. 2d 373, 378 (2d Cir. 1978).
to case, relying on language or acts which tend to prove (or disprove) a party’s awareness of, or assent to, encroachments on the routine expectation that conversations are private.\textsuperscript{132} Indeed, to secure the necessary “private zone” as justified by psychological reasoning presented in this study, the adoption of the more restrictive levels of consent on the scale would be preferable.

Relying on a policy of consent bears risks, as employees are likely to sign any agreement in order to be employed.\textsuperscript{133} Therefore, employers should consider informed and express consent when the broader policy includes more components for securing a minimum of privacy which will not be subject to contractual waiver. This is a significant change from the prevailing legal reality in which implied consent is, in many cases, sufficient.

In fact, even knowledge of the capability of monitoring alone cannot be considered implied consent. In \textit{Deal v. Spears}, the court 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.\textsuperscript{134} In the case where plaintiff believed she had eliminated her g-mail account from the blackberry, she was unaware of the possibility that others might access her future e-mails from that account; random monitoring is one thing; reading everything is another.\textsuperscript{135}

Furthermore, employees should not be penalized for refusals of employer requests to monitor data in social networks, analogous to the recent laws prohibiting employers from asking for employees’ private passwords.\textsuperscript{136}

\textsuperscript{132} \textit{Griggs-Ryan}, 904 F. 2d at 117.
\textsuperscript{133} Jolls, \textit{supra} note 126.
\textsuperscript{134} 980 F.2d 1153, 1157 (8th Cir.1992).
\textsuperscript{135} Lazette v. Kulmatycki, \textit{supra} note 8.
\textsuperscript{136} \textit{See supra} note 67 and discussion thereto.
4. Inspection, The Right To Be Heard and The Right To Appeal

All data gathered legitimately should be reported to the applicant and employees, followed by the right of employees to explain, give comments and even appeal.

5. Specific Legitimate Purpose

Tracking of any data on employees or applicants beyond the business context should be considered an invasion to privacy. Information must be tracked for specific, clear and legitimate purposes only. Employer should not use information gathered from monitoring for a purpose other than the purpose for which the monitoring was performed.\(^\text{137}\)

6. The European Approach To Privacy At The Workplace.

This final subsection discusses global trends, which have contributed to a recent shift in U.S. legal norms that support the notion of securing more private zones within virtual spheres to employees and applicants.

Europe enjoys one of the most protective systems in this sphere, which is based on the European Convention on Human Rights,\(^\text{138}\) the Council of Europe Convention 108,\(^\text{139}\) various European Union instruments, and case law of the European Court of Human Rights and of the Court of Justice of the European Union.\(^\text{140}\) There is no specific legal framework in the EU governing data processing

---

\(^{137}\) See Levinson, supra note 123.

\(^{138}\) Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950 (right to respect for private and family life, home and correspondence).

\(^{139}\) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981.

\(^{140}\) See Handbook on European Data Protection, European Union Agency for Fundamental Rights and Council of Europe 3 (2013) (This handbook on European data protection law is jointly prepared by the European Union Agency for Fundamental Rights and the Council of Europe, for the purpose of serving as the main point of reference in this field). (With the entry into force of the Treaty of Lisbon in December 2009, the Charter of Fundamental Rights of the European Union became legally binding,
in the context of employment. In the Data Protection Directive, employment relations are specifically referred to only in Article 8 (2) of the directive, which concerns the processing of sensitive data.\footnote{141} With regard to the Council of Europe, the Employment Data Recommendation was issued in 1989 and is currently being updated.\footnote{142}

A few of the above recommendations serve as core principles in the European law. First, according to the Council of Europe Employment Recommendation, personal data collected for employment purposes should be obtained from the individual employee directly. Second, personal data collected for recruitment must be limited to the information necessary to evaluate the suitability of candidates and their career potential. Third, the recommendation also specifically mentions judgmental data relating to the performance or potential of individual employees. Judgmental data must be based on fair and honest evaluations and must not be insulting in the way they are formulated. This is required by the principles of fair data processing and accuracy of data. Even an employee’s representative may receive the personal data of that employee only in so far as this is necessary to allow him to represent the interests of that employee.

Fourth, under the Employment Recommendation, employees should be informed about the purpose of the processing of their personal data, the type of personal data stored, the entities to which the data are regularly communicated and the purpose and legal basis of such communications. Employers should also inform their

---

and with this the right to the protection of personal data was elevated to the status of a separate fundamental right.)

\footnote{141} Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281.

\footnote{142} Council of Europe, Committee of Ministers (1989), Rec.(89)2 to Member States on the Protection of Personal Data used for Employment Purposes, Jan. 18, 1989. See also Consultative Committee to Convention 108, Study on Recommendation No. R (89) 2, on the protection of personal data used for employment purposes and to suggest proposals for the revision of the above-mentioned Recommendation, Sept. 9, 2011.
employees in advance about the introduction or adaptation of automated systems for
the processing of personal data of employees or for monitoring the movements or the
productivity of employees. Fifth, employees must have a right of access to their
employment data as well as a right to rectification or erasure. If judgmental data is
processed, employees must, further, have a right to contest the judgment. These rights
may, however, be temporarily limited for the purpose of internal investigations. If an
employee is denied access, rectification or erasure of personal employment data,
national law must provide appropriate procedures to contest such denial.

Sixth, the European approach recognizes the significance of consent as a legal
basis for processing employment data. However, there is awareness of the economic
imbalance between the employer asking for consent and the employee giving consent,
and Europeans often raise doubts about whether consent was given freely or not.
Therefore, the circumstances under which consent is requested should be carefully
considered when assessing the validity of consent in the employment context.\textsuperscript{143}

Seventh, even when data is relevant, there are limitation on collecting data.
For example: employers may ask employees or job applicants about their state of
health or may examine them medically only if necessary to: determine their suitability
for the employment; fulfill the requirements of preventative medicine, or allow social
benefits to be granted. Health data may not be collected from sources other than the
employee concerned except when express and informed consent was obtained or
when national law provides for it.\textsuperscript{144}

\textsuperscript{143} Article 29 Working Party (2005), Working document on a common interpretation of Article 26(1) of
\textsuperscript{144} See Working Party, supra note 143, at 180-182.
The next section addresses the recent shift in U.S. legal norm toward the European approach, supporting the notion of securing more private zones within virtual spheres to employees and applicants.

VI. A SHIFT TO A DIFFERENT ATTITUDE: SECURING A VIRTUAL “PRIVATE ZONE”

A. Legislation Forbidding Employer Access to Employee Social Media

Following the increasing numbers of people in the U.S. alone who use social media both at and away from their workplaces, employers seeking information about employees or applicants started asking them to turn over their usernames or passwords for their personal social networks or e-mail accounts.\(^{145}\) Arguably, employers could justify this request 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 liabilities.\(^{146}\) However, some policy-makers throughout the U.S., in accordance with the position expressed in this article, consider requiring access to personal accounts an invasion of employee privacy. State lawmakers introduced legislation beginning mainly in 2012 to prevent employers from requesting passwords to personal Internet accounts in order to get or keep a job. Some states have similar legislation to protect students in public colleges and universities from having to grant access to their social networking accounts. Legislation has been introduced or is pending in at least twentyeight (28) states, whereas, ten (10) states: Arkansas, Colorado, Illinois, Nevada, New

---

\(^{145}\) See National Conference of State Legislatures, supra note 67.  
\(^{146}\) Restatement (Third) of Employment Law, supra note 118.
To Read or Not To Read: Privacy Within Social Networks, The Entitlement Of Employees To A Virtual “Private Zone” And The Balloon/Magnet Field Theory.

Dr. Shlomit Yanisky Ravid, Prof. of Law. Yale Law School, ISP, Fellow

Jersey, New Mexico, Oregon, Utah, Vermont and Washington, have enacted legislation as of March 21, 2014.\footnote{See National Conference of State Legislatures, supra note 67.}

For example: Washington’s bill Concerning Personal Social Networking Accounts relates to employment practice, passed unanimously by both branches of the state legislature and signed into law, bans an employer from 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.\footnote{WASH. REV. CODE § 49.44 (2013).} The pending legislation in New York prohibits an employer or educational institution from requesting that an employee or applicant disclose any means for accessing an electronic personal account or service, protects the privacy of employees' and prospective employees' social media accounts, and prohibits an employer from requesting or requiring that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through specified electronic communications devices.\footnote{A.B. 443C, S.B. 2434C, 2013-2014 Reg. Sess. (N.Y. 2013).}

In California, existing 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, and 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. A current bill...
would apply these provisions to public employers. However, in states such as Texas, North Dakota, West Virginia as well as others, similar legislation has failed. Nonetheless, the legislative initiatives in so many states represent significant progress and recognition of the complexity of relations within workplaces in general and the right of employees to privacy within virtual spheres in particular. The recent state laws have the potential to substantially increase privacy protections of employees concerning social networking.

However, the amendments were subject to criticism by scholars who claimed public employees, who are both governed by the Constitution and protected by unions, laws and other structures not always applicable the private sector, must be held to the a regulatory structure necessary to check powers of the state. On the other hand, the new laws might be difficult to implement in workplaces where employees agree to implied (as well as any other) demands. The main problem remains when the new laws do not limit an employer from accessing social media content from a page with low or no privacy settings or receiving it from individuals with lawful access to the page.

Moreover, even the most progressive legislation does not adopt any different rules from the common law, but, rather, relies on the traditional Expectation of Privacy test (which may not be fulfilled, even in a “closed” social networking group that does not include the employer’s representatives). Therefore, we cannot apply

---

151 See National Conference of State Legislatures, supra note 67.
153 Id. at 433.
these tools to a social network profile which was not limited to a very specific group or to data posted by third parties.

On the one hand, it is well recognized that the right to privacy is not an absolute right, but rather is a set of privacy interests that the common law protects against wrongful intrusion by others. The basic claim of wrongful invasion of an employees’ right of privacy by employers requires not only (a) an intrusion upon the employee’s protected privacy interest, but also that (b) the employer’s intrusion upon that interest is highly offensive in scope or manner.\textsuperscript{154} 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.

\textbf{B. Court Decisions In Favor Of Employee Privacy}

Recent U.S. court decisions have deviated from the traditional legal inclination toward validating firms’ policies and against upholding employees’ expectations of privacy in data posted within the virtual spheres. Even though the following court decisions do not always refer to tracking data on social networks they refer to other “realms” within the virtual world used by employees (such as private e-mails), which share the same logic and therefore are applicable to the study.

In Ehling v. Monmouth-Ocean Hospital Service Corp., the plaintiff asserted a claim for common law invasion of privacy, premised on Defendants' alleged unauthorized “accessing of her private Facebook postings” regarding the occasion of Holocaust Museum shooter, where she expressed a personal view. One of the questions discussed was whether plaintiff did not have a reasonable expectation of

\textsuperscript{154} Restatement (Third) of Employment Law, § 7.01 cmt. a (Tentative Draft No. 5, 2012).
privacy in her Facebook posting. In this case, 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 whom she had individually invited to view a restricted access webpage. Defendants argued that there cannot be a reasonable expectation of privacy in a comment disclosed to dozens, if not hundreds, of people. The Court stated that plaintiff may have had a reasonable expectation that her Facebook posting would remain private, considering that she actively took steps to protect her Facebook page from public viewing.  

In 2012, the New Jersey Supreme Court adopted another pro-employee privacy decision, while opposing the employer’s explicit policy. The company provided the employee with a laptop computer to conduct company business. From that laptop, the employee could send e-mails using her company e-mail address; she could also access the Internet and visit websites through the company’s server. Unbeknownst to the employee, software on the laptop automatically made a copy of each web page she viewed, which was then saved on the computer’s hard drive in a “cache” folder of temporary Internet files. Unless deleted and overwritten with new data, those temporary Internet files remained on the hard drive. The employee used her laptop to access a personal, password-protected e-mail account on Yahoo’s website, through which she communicated with her attorney about her situation at work. Not long after, she left her employment and returned the laptop, soon to file a complaint, among other issues, about harassment.

157 Id., at 655-656.
This case presented novel questions about the extent to which an employee can expect privacy and confidentiality in personal e-mails accessed on a computer belonging to her employer. Marina Stengart used her company-issued laptop to exchange e-mails with her lawyer through her personal, password-protected, web-based e-mail account, believing that her communications would remain private.  

In anticipation of discovery, the defendant employer hired a computer forensic expert to recover all files stored on the laptop, including the e-mails, which had been automatically saved on the hard drive. Attorneys reviewed the e-mails and used information culled from them in the course of discovery. The company argued that it had the right to review the information in light of the company's written policy on electronic communications, claiming that Stengart had waived the attorney-client privilege by sending e-mails from a company computer.  

The New Jersey Supreme Court ruled that Stengart had a reasonable expectation of privacy regarding the correspondence, affirming the Appellate Division's ruling stating that the employer had violated the employee’s privacy by reading and using the documents.  

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.  

---

158 *Id.*  
159 *Id.* at 656-657 (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).  

160 *Id.*, at 654-655 (The Court noted 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 Stengart opened private emails on her private account.)
After Lazette stopped working in Verizon, her supervisor read over 48,000 personal emails via the phone Verizon had given to her. The court ruled in favor of the employee’s right to privacy, ruling that the employer had no right or authority to read the plaintiff’s personal emails. The fact that Lazette had used a company phone to access her personal email, did not give the employer “automatic” authority to access and read the employee’s private emails.161

Such cases, like the legislative initiatives described earlier, represent significant progress in the public discourse about employee privacy in the workplace with respect to electronic media. Nonetheless, the status of protection for employee and prospective employees’ personal data as published within social networks and other sources is far from being ideal.

VII SUMMARY AND CONCLUSIONS

Social networks are public digital environments where people can gather via mediating technologies. They support social interaction162 by allowing users to create personal profiles, identify lists of associates, send messages, and participate in discussion forums.163

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 people’s communication with one another. Nowadays, other alternatives are not viable and therefore, cannot be considered as a “real” alternative.

161 Lazette v. Kulmatycki, supra note 8 (the mere fact that the employee used a company-owned blackberry to access plaintiff’s e-mails does not mean that he acted with authorization when he did so. In other words, court did not recognize implied consent).
163 boyd & Ellison, supra note 37.
Privacy in social networking is an emerging, but underdeveloped, area of case law.\textsuperscript{164} There appears to be some consistency in the case law on the two ends of the privacy spectrum. On one end of the spectrum, there are cases holding that there is \textit{no} reasonable expectation of privacy for material posted to an unprotected website that anyone can view.\textsuperscript{165} On the other end of the spectrum, there are cases holding that there \textit{is} a reasonable expectation of privacy for individual, password-protected online communications.\textsuperscript{166} U.S. Courts, however, still use traditional tests, relying on either 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 about or coherent approach to data posted with restrictive measures (i.e. defined as private or aimed to 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 in how far they think 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.\textsuperscript{167}

\textsuperscript{164} See Robert Sprague, \textit{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).

\textsuperscript{165} See United States v. Gines-Perez, 214 F.Supp.2d 205, 225 (D.P.R.2002), rev’d on other grounds, 90 Fed. Appx. 3 (1st Cir. 2004) (“It strikes the Court as obvious that a claim to privacy is unavailable to someone who places information on an indisputably, public medium, such as the Internet, 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 restricted”).

\textsuperscript{166} See, e.g., Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 587 F.Supp.2d 548 (S.D.N.Y.2008) (employee had a reasonable expectation of privacy in personal, password-protected e-mail messages stored on a third party's server, although the employee had accessed that outside server while at work).

\textsuperscript{167} Lior Jacob Strahilevitz, \textit{A Social Networks Theory of Privacy}, 72 U. Chi. L. Rev. 919, 939, 973 (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.”);
A different perspective on the issue of employee privacy discusses 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, for how long, which data can be stored, who has access to the data, should employees be aware of this data and so on and so forth.

The answers for questions about the right of employees to private virtual zones emerge also from multinational firms, and the new era of international commerce gives rise to new considerations. American corporations working abroad and with foreign firms located in different countries, might wrongfully assume that American policy prevails. The result might be a breach of the 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 less relevant. 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 can justify using personal information in social networks per se. It is time, then 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, enjoy privacy within their social networks, without compare Multimedia WMAZ v. Kubach, 212 Ga. App. 707, 709 & n. 1, 443 S.E.2d 491 (Ga. Ct. App.1994) (plaintiff's disclosure of facts to sixty people did not render them public) with Fletcher v. Price Chopper Foods of Trumann, Inc., 220 F.3d 871, 878 (8th Cir.2000) (plaintiff's disclosure of facts to two coworkers deprived her of a reasonable expectation of privacy).

Restatement (Third) of Employment Law, § 7.01 cmt. b (Tentative Draft No. 5, 2012).
fear of intrusion or professional reprimand over private matters, as discussed in this study.