Fall 2011

Workplace Consequences of Electronic Exhibitionism and Voyeurism

William A. Herbert

© ISTOCK

Workplace Consequences of Electronic Exhibitionism and Voyeurism

WILLIAM A. HERBERT

Digital Object Identifier 10.1109/MTS.2011.942310
Date of publication: 13 September 2011

 1932-4529/11/$26.00©2011IEEE

The proliferation of computer-based communication technologies has substantially enabled the worldwide exchange of important ideas and information. Research and scholarly collaboration have been substantially enhanced as the direct result of these technological tools, fulfilling the dreams of early Internet proponents who fashioned it as an information superhighway.

At the same time, these communication technologies are having substantial negative consequences, unforeseen when they were introduced into the marketplace. There are some adverse consequences in the workplace emanating from the use of both employer and employee owned computer-based equipment for electronic communications. Many of these consequences are affecting societies and cultures generally. Here we focus on how, in the workplace, intentional or negligent electronic communicative irresponsibility can cause substantial problems for employers and employees.

Workplace problems resulting from new communication technologies include: a) increased distribution and availability of personal information and photographs, gossip, trivia and banalities; b) acceleration in the speed of communications, especially through email, instant messaging (IM), and social networking, resulting in an abridgement of the period of discernment, a decrease in attention span, and a suspension of the distinction between private and public information; and c) the ability of employers to monitor the personal and associational communications and activities of employees.

There are many other workplace issues that can arise from the use of new communicative technologies including the potential decline in productivity. Another developing problem is the use of electronic workplace communications as a substitute for direct personal contact resulting in miscommunications [1]. However, those types of workplace problems are not a direct outgrowth of the two primary issues discussed in this article: electronic exhibitionism and voyeurism.

Electronic Exhibitionism

Electronic exhibitionism describes the increasing worldwide phenomenon of individuals eviscerating their own privacy by affirmatively or inadvertently posting and distributing private and intimate information, thoughts, activities and photographs via email, text messaging, blogs, and social networking pages. Electronic voyeurism is descriptive of the related phenomenon of individuals and employers, who are members of what Daniel J. Solove has described as Generation Google, searching, indexing, and distributing electronic data about others [2].

It is clear that both electronic exhibitionism and voyeurism are on the rise. A study by the Pew Internet & American Life Project found that close to 20% of all Internet users utilize social networking pages as a means of providing updates about their personal lives and to obtain updates about the lives of others [3]. The rapid movement away from email and toward social networking as the electronic communication means of choice will have a consequential increase in electronic exhibitionism and voyeurism. As an article in the *Wall Street Journal* noted [4]:

> The combination of more public messages and tagging has cool search and discovery implications. In the old days, people shared photos over email. Now, they post them to Flickr and tag them with their location.

The Toilet Assumption

If offered the opportunity, most reasonable people would decline an opportunity for the expansive and wholesale disclosure of information about their personal lives and activities, or the display of intimate pictures in a periodical or on a billboard. To varying degrees, such disclosures are usually limited to select individuals with the means of disclosure subjectively modulated for each intended recipient. With the exception of letters, notes, and diary entries, a written record of intimate experiences and impressions is not left behind. Inherent in such limitations is a desire to retain a protected zone of individual privacy.

Despite the general reluctance to bare all through old media, new communicative technologies are leading, if not encouraging, individuals to engage in an unprecedented degree of exhibitionism about their personal lives, thoughts, and activities to a virtual worldwide audience. Frequently, such communications relate directly or indirectly to work or co-workers and have the potential for causing negative employment consequences. Despite the potential for adverse consequences, millions if not billions of people are unmasking themselves electronically through email, text messaging, blogs, and social networking pages, leaving a digital trail of information thereby eliminating plausible deniability. Many engage in such exhibitionism during working hours utilizing employer computers and equipment.

According to a December 2009 study commissioned by Microsoft, 36% of those surveyed worldwide expressed a concern about the impact of their online presence on future job prospects. The respondents who expressed the least concern about the impact of their electronic footprints on their professional lives were from the United States (U.S.) and the United Kingdom (U.K.) [5].

The growth in electronic exhibitionism may be caused, in part, by what Clifford Nass and Youngme Moon have labeled "reciprocal self-disclosure" where "people who receive intimate disclosure feel obligated to respond with a personal disclosure of equal intimacy" [6]. This tendency may also be due to the amorphous nature of virtual social networks that extend well beyond family and friends to workplace colleagues, acquaintances, and strangers [7]. Finally, in some circumstances, the exhibitionism may be a consequence of errors in judgment tied with cognitive lapses caused by chronic multitasking [8].

Exhibitionism is endemic to social networking. These pages provide a connection to a virtual world that actively encourages reciprocal self-disclosure. Critics of the 2009 changes to Facebook's privacy options claimed that they were aimed at encouraging users to maximize the audience that can access personal content [9]. Since that time, privacy concerns related to Facebook have received substantial media attention and governmental inquiries [10], [62], [63]. Such concerns, however, have not slowed the growth in the number of Facebook users. Statistics from Facebook suggest that the number of users throughout the globe has grown from 300 to 500 million in the past two years; at the same time, however, there has been a noticeable decline in the number of users in the United States, Canada, the United Kingdom and other countries [11], [60]. This expansive embrace of social networking worldwide is inconsistent with an important adage from a well-known American performing artist: "After a while you learn that privacy is something you can sell, but you can't buy it back" [12].

Four decades ago, sociologist Philip Slater coined a metaphor for the cultural phenomenon of ignoring social problems by placing them out of view: the toilet assumption [13]. This sociological metaphor is equally applicable to the disconnection between the electronic communicator and his or her digital trail. There is a perception of privacy when an individual communicates electronically, along with an implicit assumption that the audience is limited to the named recipient or the group of social network friends [7]. Furthermore, the use of the delete function for email creates the illusion of permanent eradication, which lowers inhibitions, personal, sexual or otherwise, with respect to the content of the electronic communications.

The use of the delete function for email creates the illusion of permanent eradication, which lowers inhibitions.

Many erroneously assume that a sent electronic communication or a blog post is impermanent and that the scope of accessibility is limited. Furthermore, password requirements for websites and privacy limitations on social networking pages do not effectively restrict the release of the content to others. This vulnerability is particularly true in the workplace, where the disclosure of "private" electronic communications may form the basis for adverse employment actions, discrimination complaints, and potential litigation [14].

There is a frequent cognitive disconnect between the preparation of an electronic communication and the potential risk of adverse consequences. Ian Clark, an accused murderer of a two-year-old in Indiana, faced the consequences of his electronic exhibitionism when he testified in his own defense. After Clark placed his personal character into issue during his testimony, the prosecutor challenged him with an unflattering self-description from his social networking page that contradicted his statements before the jury [15].

The potential for adverse consequences resulting from electronic exhibitionism and the toilet assumption is particularly strong in the workplace. During the workday, there is little understanding that emails, text messages, url addresses, and images from websites visited on workplace equipment are accessible by the employer. Similarly, the potential for employer accessibility to off-duty blog posts, and social networking pages, is frequently underappreciated. Nevertheless, a new term has been coined to describe the termination of an employee over the content of a blog: dooced [16].[1]

The accelerating speed of electronic communicative exchanges, in conjunction with workplace multitasking, increases the likelihood of personal exhibitionism. Within the swirl associated with multitasking, few remember that electronic communications "should be considered permanent and searchable; it can be copied, pasted and emailed to a wide audience" [17].

A fictional character in Cédric Klapisch's 2008 film *Paris* exemplifies the combination of electronic exhibitionism and the toilet assumption. In the film, an inhibited and lonely professor utilizes anonymous text messages to communicate and seduce a young student, oblivious to the digital evidentiary trail of his professorial lechery. Although the evidence from his text messages may have resulted in the demise of his

[1]The term "dooced" originates from the blog name utilized by an employee who was terminated for her posts about work.

academic career, the professor's mindlessness about this vulnerability is emblematic of how many people approach electronic communications. In fact, digital footprints from text messages are becoming an increasingly common evidentiary element in proving dalliances [18].

Work-related examples of electronic exhibitionism are not limited to fiction. The first electronic workplace privacy case decided by the U.S. Supreme Court involved a municipal police department accessing the transcripts of text messages sent and received by a police sergeant on a city-owned pager. Some of the texts were sexual in nature, and included exchanges between the sergeant and his then wife, and between the sergeant and his girlfriend. The city's investigation found that in one month, the sergeant sent and received 456 text messages with only 57 being work-related [19].

There are many other examples demonstrating the workplace vulnerabilities caused by exhibitionism. A sociology professor was suspended as the result of posted comments on her Facebook page about her students, which were perceived as threatening [20]. The long-term disability leave of a Quebec employee with major depression was cancelled after an insurance company accessed posted photographs on her social networking page showing her at bars and on holiday in a sunny destination [21]. An arbitrator sustained the termination of an elementary school teacher in 2009 for posting nude photographs of herself on publicly accessible "swinger" websites [22]. Similarly, the angry and homicidal comments of a bus driver on his Facebook page became a part of an investigation into his actions leading to a pedestrian death [23].

The disclosures resulting from electronic exhibitionism are not limited to personal information. Employee electronic communications can include discriminatory, disparaging, or defamatory remarks about the employer, supervisors, co-workers, or students. Electronic exhibitionist behavior can also result in the intentional or negligent disclosure of employer proprietary information, secrets, and confidences.

> There is a frequent cognitive disconnect between the preparation of an electronic communication and the potential risk of adverse consequences.

In summary, the mindlessness implicit in electronic exhibitionism has led to the expansive disclosure of data accessible to a potential worldwide audience or, at minimum, the employer who owns the computer equipment. The architecture of electronic forums, such as blogs and social networking, entice the unwary into making unguarded disclosures and comments that they would be unlikely to make in personal interactions or would want to publicize in traditional media. Similarly, the use of password protections can have the unintended consequence of creating the false sense that an electronic communication will not be shared with anyone outside the select group with access.

We next turn to the reciprocal topic of electronic voyeurism, the growing tendency to utilize the Internet as a tool for picking the ripe fruit of exhibitionism.

Voyeurism, Cybervetting and Too Much Information

Seven years ago, feminist writer Katha Pollitt publicly confessed to an Internet-based activity that few others acknowledge: she used search engines to pry into someone else's private life [24]. In Pollitt's case, her electronic voyeuristic adventure was motivated from feelings of abandonment and betrayal by her former boyfriend. According to her published account, the searches resulted in her gaining access to relatively mundane information about her former boyfriend, his new girlfriend, and others in his social world. Apparently, none of Pollitt's targets, at the time, had left extensive electronic footprints.

However, things have changed. Another writer with a broken heart published an article describing how he learned of his former girlfriend's new boyfriend from photographs on her Facebook page. This information inspired him to gather information about the boyfriend through a Google search, and then, to his horror, he also discovered that his own grandfather had become a Facebook friend of his former flame [25].[2]

The growing temptation to engage in electronic voyeurism is not limited to former paramours or to efforts to obtain salacious information. As Daniel Solove has written: "Everybody's googling. People google friends, dates, potential employees, long-lost relatives, and anybody else who happens to arouse their curiosity" [2]. A 2007 study by the Pew Internet & American Life Project found that 53% of adult Internet users surveyed acknowledged using search engines to obtain information about others including 19% who admitted

[2]More recently, novelist Helen Schulman published a candid description of her conflicts and compulsions in following the blog entries of a former lover. See [65].

searching for details about their co-workers and colleagues [26].

Voyeuristic activities can lead to a multitude of problems. The subtleties of persona and reputation can be severely tarnished from a simple Google search or an erroneous social network befriending. The results can form the basis for gossip and misunderstandings between friends, family, and co-workers. Without contextualization, personal information or comments from the Internet can present false images and mistaken impressions. The target of the voyeurism may feel victimized, although personally responsible for the availability of the information. Such feelings of victimization are fully understandable when a social networking page is hacked and personal and erroneous content is then spewed to others [27].

The adverse workplace consequences of electronic voyeurism can be pronounced. Job applicants, employees, and employers can be harmed in different ways based upon the accessibility of too much information to employers and co-workers.

The use of the Internet to obtain information about current employees and job applicants is referred to as cybervetting [28]. In many ways, cybervetting is an electronic extension of traditional employer investigatory methods. Increasingly, employers embrace cyber-investigations because, thanks to electronic exhibitionism, such investigations are likely to reveal more relevant information reflecting upon an individual's trustworthiness, maturity, prudence, sense of responsibility, and work ethic. As a practical matter, the most revealing source for personal information may be an individual's blog, social networking page, electronic comments at websites, and his or her tweets.

According to Microsoft's December 2009 study, 74% of the recruiters surveyed worldwide admit to evaluating candidates based upon information obtained online. In the U.S., 75% of the recruiters admitted to a corporate policy of examining online information about applicants and 70% admitted to rejecting an applicant based upon information from the Internet [5].

Another 2009 study found that 45% of human resource professionals surveyed actively screen candidates for employment by visiting social networking pages. In addition, 35% of those surveyed acknowledged declining to hire applicants based upon the exhibitionist content found on social networking pages: inappropriate photographs; references to drug and alcohol use; negative comments about prior employers and co-workers; and discriminatory remarks [29], [30]. Although the 2009 study focused on accessing social networking pages, cybervetting frequently includes Internet searches of websites and personal blogs for information on prospective and current employees.

In the absence of unlawful motivation or the improper use of information about an individual's protected class status or activities, there are few legal restraints on employers and recruiters accessing public online information about an employee or applicant. The decision to engage in cybervetting can stem from legitimate business concerns. A third party harmed by an employee's use of the Internet may commence litigation against the employer claiming negligent hiring, training, or supervision [31]. A simple Internet search can uncover derogatory, defamatory, inappropriate comments and confidential information about the employee, co-workers, the employer, the employer's products, or the workplace [32]. Intemperate posts on a website or a blog about supervisors and co-workers can form the basis for disciplinary action [33]. One American company had to amend its employee blogging policy after discovering that an employee had anonymously blogged about company policy and legal issues that he was directly involved with [34].

An Internet search of a current employee can be part of an investigation into an employee's workplace conduct, or part of an employer's policy and practice of cybervetting. The fruit of such searches can uncover facts directly related to the conduct under investigation or can form the basis for the commencement of an investigation. In one case, during an investigation into alleged fraud and theft by a government employee, the employer conducted a Google search resulting in information about the employee's prior employment history. As part of the legal challenge to his termination, the employee claimed that the Google search violated fundamental fairness. A reviewing court, however, rejected this argument on the grounds that the information obtained had no impact on the employer's decision to terminate [35].

Cybervetting is not, however, a risk-free activity for employers. It can result in false or incorrect information that might lead to overreactions and adverse employment decisions harmful to both the individual and the employer.

> Digital footprints from text messages are becoming an increasingly common evidentiary element in proving dalliances.

Cybervetting frequently includes Internet searches of websites and personal blogs for information on prospective and current employees.

Concerns over problems resulting from cybervetting led the Defense Personnel Security Research Center (DPSRC), in association with the International Association of Chiefs of Police (IACP), to issue a 2010 report providing suggested employment policies, guidelines, and practices for cybervetting [28]. The report encourages the creation and implementation of a written agency policy articulating the purpose and scope of the cybervetting. It also encourages transparency by providing notice to, and seeking consent from, employees and applicants before accessing information from a website, blog, or social networking page that is password protected. Finally, it recommends the use of departmental social media policies setting forth applicable rules for work-related Internet activity and off-duty social networking. IACP has posted a model social media policy for police departments [36]

Unlike the European Union (EU), and its member States, there are few legal restrictions limiting U.S. employers from engaging in workplace computer surveillance [1], [37]. With certain notable exceptions, American law permits employer monitoring of workplace computers. The mere issuance of a workplace computer use policy, conditioning such use on the right of the employer to monitor, can defeat a claim of a reasonable expectation to electronic workplace privacy. However, an employer can be held liable for accessing workplace electronic communications if it failed to implement an appropriate computer use policy or it permitted employees to use personal passwords to restrict accessibility to personal email or computer files [1].

While workplace computer use policies and monitoring are relatively common, employer written policies on employee social media activities and cybervetting are not [1], [38]. There are multiple reasons for implementing and circulating both types of policies. However, federal and state collective bargaining laws may restrict the ability of an employer to unilaterally implement such policies [1]. These legal limitations on employer unilateral actions are particularly relevant when a policy applies to protected union-related activities and other legally protected activities and conduct.

A computer use policy can annunciate limitations on employee use of workplace computers and networks, and place employees on notice that such electronic workplace activities will be monitored [1]. Monitoring can be accomplished through the application of software and periodic audits. Electronic monitoring can track the content of email, websites visited, and images from those websites. It can lead to the discovery of personal and confidential information that is maintained on the employer's mail server or hard drive. There are legitimate purposes for such monitoring, including: protecting intellectual property and trade secrets; complying with regulatory obligations; avoiding liability based upon conduct of employees; conducting discrimination and disciplinary investigations; and responding to discovery demands from regulatory agencies and litigants.

Computer-use policies can substantially aid in an employer's defense against claims of unlawful monitoring. However, policies are not particularly effective in curbing electronic exhibitionism, without related workplace training. For example, the police sergeant who sent multiple sexually explicit texts to his wife and girlfriend on a city-owned pager had been given a copy of the city's computer use policy, had signed and acknowledged he understood the policy, but believed that the text messages on the pager were not subject to the policy [19].

In order to be effective, computer use policies and training must be periodically updated to keep pace with technological change. A New Jersey judicial decision regarding an employee's alleged waiver of the attorney-client privilege illustrates this point. In general, the attorney-client privilege can be waived by an employee sending a communication on a workplace email system knowing that the employer has a policy and practice of monitoring such communications. However, in the New Jersey case, the employer's computer use policy did not specify that it was applicable to password-protected webmail, and therefore the court concluded that the employee's use of the employer's laptop to communicate with her attorney by webmail did not waive the attorney-client privilege [39]

Like other computer use policies, policies regarding social media and cybervetting may affect employer liability. For example, an employer may be found liable for cybervetting if it fails to obtain voluntary individual consent before accessing a password-protected page. A lawsuit stemming from a New Jersey restaurant management's access of an employee social networking page exemplifies the dangers of an employer accessing a password-protected website or social networking page [40]. In that case, two restaurant employees created a private and password-protected MySpace page

for the purpose of venting about work. They invited current and former co-workers to join. Each participant was granted password-protected access. After one participant showed the page to a restaurant manager, she received an order to provide her password to two other managers. Utilizing her password, the managers repeatedly accessed the page to read and print posts deemed inappropriate. Based upon the posts' content, the two employees who had created the page were fired. They sued the restaurant under laws prohibiting the access of stored electronic communications without authorization or in excess of authorization. Following a jury trial, the restaurant was found liable for obtaining the password in a coercive manner and repeatedly accessing the page despite being aware that the page was intended to be private.

In another case, an airline pilot sued his employer after it gained repeated access to his secure website under false pretenses and read posts criticizing the employer and his union [41]. Access to the website was limited to invited co-workers who received a password. The website's terms and conditions expressly prohibited access by airline management. Each time access was sought, the user had to affirmatively accept the terms and conditions including a commitment to keep the posted information confidential. After obtaining permission from one of the invited co-workers to use his name, an airline vice-president gained access to the website, and distributed the posted material. Based upon those facts, an appellate court ordered a trial on the pilot's claims.

There are other potential legal problems for employers who engage in electronic voyeurism and cybervetting. It can create the appearance of surveillance toward protected collective worker activities and can be used to prove employer animus toward such activities [1]. For example, the cybervetting of employees in British Columbia following the filing of a union representation petition, was alleged to have been unlawfully motivated by employer animus toward the union activity [42].[3]

An employer's knowledge or possession of cyber-based information may constitute material evidence for a claim of unlawful discrimination, violations of privacy, or infringements upon legal rights to engage in certain protected activities. The timing of an employer's discovery of personal information can form the evidentiary foundation for a claim that a subsequent adverse employment action was motivated by the employer's knowledge. With the probable increase in the use of social networking as part of labor organizing campaigns [43], employer electronic surveillance may lead to liability because some employers forget that voyeurism, like exhibitionism, leaves a digital trail [44]. By implementing a cybervetting policy, and contracting with a third party company to conduct the electronic search, an employer can limit its exposure to liability [45].

Any discussion about workplace related electronic voyeurism would not be complete without mentioning its role in litigation. Increasingly, attorneys are accessing or seeking access to the contents of social networking pages of adverse parties and witnesses. The rationale for such access is that a social networking page can be a rich source of relevant information [46]. A page with unrestricted public access can provide an attorney with a quick and simple means of gathering probative information about a party or witness.

Even when privacy protections are in place, an attorney can question witnesses about their electronic communicative habits during pre-trial depositions as a means of establishing a legitimate basis for peering into the private content on a social networking page. Increasingly, courts are mandating litigants to provide adverse parties with access to restricted social networking pages for the purpose of obtaining information relevant to issues in the litigation [47]. Finally, it must be emphasized that electronic voyeurism in litigation is not limited to social networking pages. In the U.S., e-discovery demands for communications stored in an employer's computer network are common, resulting in release of employee electronic communications deemed relevant to the issues in a case.

> Voyeurism, like exhibitionism, leaves a digital trail.

Exhibitionism and Voyeurism Issues in the Workplace

The developing problems caused by electronic exhibitionism and voyeurism warrant a careful reexamination of current self-regulatory and regulatory regimes [48].

Despite the ubiquity of electronic communications, it is not common for employers to offer training about email and Internet use or the workplace implications of social media. Most employers rely upon unilaterally imposed policies, which are issued for litigation avoidance, without any related training [49]. Practical training, developed with union and employee participation,

[3]The United States Chamber of Commerce has published a report describing legal developments at the National Labor Relations Board with respect to social networking issues in the workplace. See [64].

can help limit the temptation toward electronic exhibitionism and encourage more responsible electronic communications. Training can also help eliminate the toilet assumption and improve what Malcolm Gladwell has described as an individual's adaptive unconscious [50]. Furthermore, labor-management cooperation can assist in establishing prudent limits on electronic voyeurism by placing negotiated checks on employer cybervetting of employee electronic activities.

Although IBM has issued social computing guidelines that include practical information and suggestions for responsible electronic communications, most other employers have not followed IBM's lead [38], [52], [53], [66]. It is far more common for employers to simply ban social networking or block access to social networking pages in the workplace, a strategy that can alienate younger workers [53], [54]. Overly restrictive social media policies can run afoul of contemporary employee expectations, as well as laws protecting the right of employees to engage in protected concerted activities [55].

The most promising means for solving the problems of electronic exhibitionism and voyeurism may be technological innovation. As Jeffrey Rosen has described, new companies are beginning to market services that will minimize the consequences of electronic exhibitionism by scrubbing the Internet of reputation-impairing electronic material [48]. The research aimed at creating self-destructing electronic communications offers another important future technologically based solution [47], [56]. Architectural modifications to current communicative technologies also have the potential for discouraging electronic exhibitionism and voyeurism in the workplace. Such modifications can include a presend email review function, the establishment of a privacy option for workplace email, or periodic workplace privacy reminders of the employer's monitoring policy.

Finally, governments can play an important role by seeking to compel telecommunications and social networking companies to encourage responsible electronic communications. In the U.S., legislators, administrative agencies, and computers scientists are exploring regulatory and architectural means for enhancing online privacy notification [57]. In addition, the unanticipated consequences of new communicative technologies may stir remedial legislative action. In Germany and the U.K., laws have been proposed to prohibit employers from cybervetting applicants [58], [59]. It is probable that similar legislative proposals will be made on the state level in the U.S. [47]. These legislative proposals are indicative of the growing societal concerns over the consequences of electronic exhibitionism and voyeurism.

Author Information

The author is Deputy Chair and Counsel of the New York State Public Employment Relations Board. Email: wherbert@nycap.rr.com.

Acknowledgment

This article is an updated version of a paper presented at the 2010 IEEE International Symposium on Technology and Society, Wollongong, Australia. The opinions expressed are the personal views of Mr. Herbert and do not reflect the opinions of the State of New York or the New York State Public Employment Relations Board. Mr. Herbert would like to acknowledge his daughters Beth Lee-Herbert and Lisa Lee-Herbert who have patiently tutored him with respect to computer-based technologies for over a decade. Without their bemused assistance, this article would not have been possible.

References

[1] W.A. Herbert, "The electronic workplace: To live outside the law you must be honest," *Employee Rights & Employment Policy J.,* vol. 12, no. 49, pp. 52, 73, 102–103, 2008.

[2] D.J. Solove, *The Future of Reputation: Gossip, Rumor and Privacy on the Internet*. New Haven, CT, and London, U.K.: Yale Univ. Press, 2007, pp. 9–12.

[3] S. Fox, K. Zickuhr, and A. Smith, "Twitter and status updating" Oct. 2009; http://www.pewInternet.org/~/media//Files/Reports/2009/PIP_Twitter_Fall_2009_web.pdf.

[4] J.E. Vascellard, "Why email no longer rules … and what that means for the way we communicate," *WSJ*, Oct. 12, 2009; http://online.wsj.com/article/SB10001424052970203803904574431151489408372.html.

[5]Microsoft Data Privacy Day, Reputation Research; http://www.microsoft.com/privacy/dpd/research.aspx.

[6] C. Nass and Y. Moon, "Machines and mindlessness: Social responses to computers," *J. Social Issues*, vol. 56, no. 1, pp. 89–90, 2000.

[7] L. Gelman, "Privacy, free speech, and 'blurry edged' social networks," *B.C.L. Rev.* vol. 50, no. 5, pp. 1315-1344, 2009.

[8] E. Ophira, C. Nass, and A. Wagner, "Cognitive control in media multitaskers," in *Proc. National Academy of Sciences*, vol. 106, no. 37, Sept. 25, 2009.

[9] K. Bankston, "Facebook's New Privacy Changes: The Good, The Bad and The Ugly;" http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly.

[10] B. Cohen, "Facebook brings back an old-fashioned approach to privacy," *Guardian*, Feb. 1, 2011; http://www.guardian.co.uk/commentisfree/2011/feb/01/facebook-privacy-old-fashioned.

[11] M. Zuckerberg, "300 Million and On," Sept 15, 2009; http://www.facebook.com/blog.php?post=136782277130; Facebook Press Room, http://www.facebook.com/press/info.php?statistics (last accessed Feb 5, 2011).

[12] B. Dylan, *Chronicles, Volume 1*. New York, NY: Simon & Schuster, 2004, pp. 117–118.

[13] P. Slater, *The Pursuit of Loneliness: American Culture at the Breaking Point*. Boston, MA: Beacon, 1970, pp. 15–19.

[14] S.C. Bennett, "Look who's talking: Legal implications of Twitter social networking technology," *NYSBA.,* May 2009, pp. 10–14.

[15] *Clark v. State,* 915 N.E.2d 126, 129–131 (Ind. 2009).

[16] K. Maxwell, *Macmillan English Dictionary*, Word of the Week Archive; http://www.macmillandictionaries.com/wordoftheweek/archive/050131-dooced.htm.

[17] M.E. Getnick, "Social media: The good, the bad and the ugly," *NYSBA J.,* Oct. 2009, p. 5.

[18] L. M. Holson, "Text messages: Digital lipstick on the collar," *New York Times*, Dec. 8, 2009; http://www.nytimes.com/2009/12/09/us/09text.html?_r=1&hp.

[19] *City of Ontario v. Quon*, 130 S.Ct. 2619 (2010)

[20] "Not so private professors," *Inside Higher Ed.* Mar. 2, 2010; http://www.insidehighered.com/news/2010/03/02/facebook.

[21] "Depressed woman loses benefits over Facebook photos," *CBC News*, Nov 19, 2009; http://www.cbc.ca/canada/montreal/story/2009/11/19/quebec-facebook-sick-leave-benefits.html.

[22]*Phenix City Bd of Educ and Alabama Educ Assoc*, 125 Lab. Arb. Rep 1473 (BNA, 2009).

[23] Pete Donohue, "Bus driver who mowed down student had 'wrote' rage episode on Facebook: Sources," *Daily News*, Nov. 11, 2009; http://www.nydailynews.com/news/2009/11/11/2009-11-11_bus_driver_who_mowed_down_student_had_wrote_rage_episode_on_facebook__sources_th.html.

[24] K. Pollitt, "Webstalker," *New Yorker*, Jan 19, 2004, p. 38.

[25] C.H. Antin, The boundaries of a breakup, *New York Times*, Nov 20, 2009; http://www.nytimes.com/2009/11/22/fashion/22love.html?scp=10&sq=&st=nyt.

[26] M. Madden, S. Fox, A. Smith, and J. Vitak, Digital Footprints: "Online Identity Management and Search in the Age of Transparency," Dec. 2007, pp. 23–29; http://www.pewInternet.org/~/media//Files/Reports/2007/PIP_Digital_Footprints.pdf.

[27] B. Stone, "Crooks hijack Facebook accounts, injuring dignity," *New York Times*, Dec 14, 2009; http://www.nytimes.com/2009/12/14/technology/Internet/14virus.html?_r=1.

[28] A.Rose, H. Timm, C. Pogson, J. Gonzalez, E. Appel, and N. Kolb, "Developing a Cybervetting Strategy for Law Enforcement: Special Report," Dec., 2010; http://www.iacpsocialmedia.org/Portals/1/documents/CybervettingReport.pdf.

[29] J. Wortham, More employers use social networking to check out applicants", *New York Times*, Aug. 20, 2009; http://bits.blogs.nytimes.com/2009/08/20/more-employers-use-social-networks-to-check-out-applicants/.

[30] "Forty-Five Percent of Employer Use Social Networking Sites to Research Job Candidates," *CareerBuilder Study Finds;* http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr519&sd=8/19/2009&ed=12/31/2009&siteid=cbpr&sc_cmp1=cb_pr519_&cbRecursionCnt=1&cbsid=8412d5b32ef54ce6854a035cf3a59d12-303995843-x3-6.

[31] *Maypark v. Securitas Security Services USA, Inc.*, 775 N.W.2d 270 (Wis. App, 2009); *Doe v. XYC Corp*, 887 A.2d 1156 (N.J. Super. Ct. App. Div. 2005).

[32] J. S. Klein and N. J. Pappas, "Legal issues arising out of employees' use of Social Networking Web Sites," *N.Y.L.J*, Oct. 5, 2009, p. 3, col. 1.

[33] *Curran v. Cousins*, 509 F.3d 36 (1st Cir, 2007) (critical comments by employees on their union's website about supervisors and workplace policies on a union's website resulted in adverse employment actions.); *Richerson v. Beckon,* 337 Fed.Appx. 637, (9th Cir 2009) (criticism by a public employee of unnamed co-workers posted on a blog found to be unprotected speech under the First Amendment to the U.S. Constitution).

[34] Cisco, "Lessons Learned … Cisco Updates Policy on Employee Blogging," *The Platform: Opinions and Insights from Cisco*, Mar 24, 2008, http://blogs.cisco.com/news/comments/lessons_learnedcisco_updates_policy_on_employee_blogging/.

[35] *Mullins v. U.S. Department of Commerce,* 244 Fed.Appx.322 (Fed. Cir. 2007).

[36] IACP Social Media Model Policy, Aug 2010; available at http://www.iacpsocialmedia.org/Portals/1/documents/Social%20Media%20Policy.pdf.

[37] W.A. Herbert, "Workplace electronic privacy protections abroad: The whole wide world is watching," *U. Fla. J.L. & Pub Pol'y,* vol. 19, pp. 379–420, 2008.

[38] American Management Assn, *2007 Electronic Monitoring & Surveillance Survey: Over Half of All Employers Combined Fire Workers for E-Mail & Internet Abuse,* 2008; http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/.

[39] *Steingart v. Loving Care Agency*, 973 A.2d 390 (N.J. 2009).

[40] *Pietrylo and Marino v. Hillstone Restaurant Group d/b/a Houston's*, 2009 WL 3128420 (D.N.J.), 29 IER Cases 1438 (D. NJ, FSH).

[41] *Konop v. Hawaiian Airlines, Inc*. 302 F.3d 868 (9th Cir. 2002), *cert den*., 537 U.S. 1193 (2003).

[42] *Lougheed Imports Ltd*, BCLRB No. B190/2010; http://www.fasken.com/files/upload/BC%20Labour%20Relations%20Board%20-%20West%20Coast%20Mazda.pdf.

[43] *New Approaches to Organizing Women and Young Workers: Social Media & Work Family Issues,* Jul. 2010; http://www.working-families.org/learnmore/pdf/NewApproachestoOrganizingWomenand YoungWorkers.pdf.

[44] R. Jackson, "New Facebook privacy settings are both a goldmine and a minefield for employers," *Employment Law Alert,* Dec. 11, 2009; http://www.nixonpeabody.com/publications_detail3.asp?ID=3065&NLID=11.

[45] G.W. Schultz, "Is your boss spying off the clock," *Huffington Post,* Nov. 11, 2010; http://www.huffingtonpost.com/gw-schulz/is-your-boss-spying-off-t_b_782312.html.

[46] R. Kelner, G. Kelner, "Social networking sites and personal injury litigation," *N.Y.L.J.*, Sept 23. 2009, p. 3, col. 1.

[47] *E.E.O.C. v. Simply Storage Management, LLC*, 270 F.R.D. 430 (S.D.Ind., 2010). *Romano v. Steelcase* Inc, 30 Misc.3d 426 (Sup Ct, Suffolk Co, 2010); *Leduc v. Roman*, (Ont. Superior Ct, 06-CV-3054666PD3 (2009) available at http://www.canlii.org/en/on/onsc/doc/2009/2009canlii6838/2009canlii6838.pdf.

[48] J. Rosen, "The end of forgetting," *NY Times*, July 10, 2010; Twitter tapping, *NY Times*, Dec. 12, 2009; http://www.nytimes.com/2009/12/13/opinion/13sun2.html?_r=1&scp=1&sq=social%20networking&st=Search.

[49] P.M. Berkowitz, "Adjusting to new norms as social networking pervades the workplace," *N.Y.L.J.*, Nov 12, 2009, p.5, col. 1.

[50] M. Gladwell, *Blink: The Power of Thinking Without Thinking.* New York, NY, and Boston, MA: Little Brown, 2005, pp. 11–16.

[51] *IBM Social Networking Guidelines;* http://www.ibm.com/blogs/zz/en/guidelines.html.

[52] R. King, "Companies want to monitor workers on social networks," *BusinessWeek*, May 17, 2009; http://www.businessweek.com/technology/technology_at_work/archives/2009/05/workers_social.html?chan=top+news_top+news+index++temp_technology.

[53] T. Baldas, "Companies say no to friending or tweeting," *LTN Law Technology News*, Oct. 08, 2009; http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202434373430.

[54] M. Irvine, "Young workers push employers for wider web access," *USAToday*, July 17, 2009; http://www.usatoday.com/tech/webguide/Internetlife/2009-07-13-blocked-Internet_N.htm.

[55] *Sears Holdings (Roebucks)*, Case 18-CA-19081, NLRB General Counsel Advice Memorandum (Dec. 4, 2009).

[56] R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, "Vanish: Increasing data privacy with self-destructing data," in *Proc. USENIX Security Symp*. Aug. 2009; http://vanish.cs.washington.edu/pubs/usenixsec09-geambasu.pdf.

[57] S. Lohr, "Redrawing the route to online privacy," *NY Times,* Feb 28, 2010; http://www.nytimes.com/2010/02/28/technology/Internet/28unbox.html.

[58] P.L.Gordon, "As Germany considers restrictions on use of social media for recruiting, multi-national employers need to start thinking about social media policy," *Littler Privacy Blog*, vol. 2.0, Sept 10, 2010; http://privacyblog.littler.com/2010/09/articles/social-networking-1/as-germany-considers-restrictions-on-use-of-social-media-for-recruiting-multinational-employers-need-to-start-thinking-about-social-media-policy-20.

[59] "Employers should be banned from searching Facebook profiles of job applicants, say children's groups," *Mail Online*, Mar. 25, 2008; http://www.dailymail.co.uk/news/article-544389/Employers-banned-searching-Facebook-profiles-job-applicants-say-childrens-groups.html.

[60] F. Manjoo "Has Facebook peaked?," *Slate*, Jun. 14, 2011; http://www.slate.com/id/2296932/.

[61] L. Belkin, "Queen of the mommy bloggers," *New York Times,* Feb. 23, 2011; http://www.nytimes.com/2011/02/27/magazine/27armstrong-t.html?pagewanted=all.

[62] E. Steel and G. A. Fowler, "Facebook in privacy breach," *WSJ,* Oct. 18, 2010; http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html.

[63] T. Claburn, "Facebook faces Congressional privacy interrogation," *InformationWeek*, Feb. 5, 2011; http://www.informationweek.com/news/Internet/social_network/show-Article.jhtml?articleID=229201226&cid=RSSfeed_IWK_All.

[64] M.J. Eastman, "A survey of social media issues before the NLRB," Aug 5, 2011; http://www.uschamber.com/sites/default/files/reports/NLRB%20Social%20Media%20Survey.pdf.

[65] H. Schulman, "An Ex blogs. Is it O.K. to watch?" *New York Times*, Aug 5, 2011; http://www.nytimes.com/2011/08/07/fashion/modern-love-when-an-ex-blogs-is-it-ok-to-watch.html?_r=1&ref=modernlove.

[66] K. Mikkelson, "Cybervetting and monitoring employees' online activities: Assessing the legal risks for employers," *The Public Lawyer*, Sum. 2010; http://abalel.omnibooksonline.com/2010/data/papers/161.pdf.