Workplace Consequences of Electronic Exhibitionism and Voyeurism

William A. Herbert
Deputy Chair and Counsel
New York State Public Employment Relations Board
wherbert@nycap.rr.com

Abstract

The popularity of email, blogging and social networking raises important issues for employers, employees and labor unions. This article will explore contemporary workplace issues resulting from the related social phenomena of electronic exhibitionism and voyeurism. It will begin with a discussion of the international social phenomenon of individuals electronically distributing their personal thoughts, opinions, and activities to a potential worldwide audience while at the same time retaining a subjective sense of privacy. The temptation toward such exhibitionism has been substantially enhanced by the advent of Web 2.0. The article then turns to the legal implications of electronic voyeurism including employer surveillance of employee workplace computer use and employee off-duty blogs and social networking pages. It will also examine the issues associated with employers and recruiters conducting internet searches for information about job applicants. In the conclusion, the article will discuss various means for responding to the workplace issues resulting from electronic exhibitionism and voyeurism on and off the job.¹

1. Introduction

The proliferation of computer-based communication technologies has substantially enhanced the worldwide exchange of important ideas and information. Research and scholarly collaboration has 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. This article will examine some adverse consequences in the workplace emanating from the use of both employer and employee owned computer-based equipment for electronic communications. While many of these consequences are affecting societies and cultures generally, the focus of this article is on the workplace where intentional or negligent electronic communicative irresponsibility can cause substantial problems for employers and employees.

Among the problems that have developed in the workplace stemming from new communication technologies include: a) the distribution and availability of personal information and photographs, gossip, trivia and banalities; b) the acceleration in the speed of communications, especially through email, 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, based upon permanent employee electronic trails.

It should be noted there are many other workplace issues that can stem 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 electronic voyeurism.

Electronic exhibitionism describes the increasing worldwide phenomenon of individuals eviscerating their own privacy by affirmatively 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 exhibitionist material of others. [2]

¹ The opinions expressed in this article are the personal views of Mr. Herbert and do not reflect the views of the New York State Public Employment Relations Board. ©William A. Herbert
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:

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. [4]

2. Electronic Exhibitionism and 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 aperture and 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 life were from the United States (US) and the United Kingdom (UK).[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] The 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 assert that they were aimed at encouraging users to maximize the audience that can access personal content. [9] This criticism is supported by Facebook’s recommendation that users chose the “everyone” option. Under this option, all publicly available content on an individual’s Facebook page becomes accessible through a simple Google search. The choice by Facebook’s CEO to publicly adopt this option is a strong indication that his company sees a competitive marketplace benefit in encouraging electronic exhibitionism. [10] However, this type of expansive social networking behavior is inconsistent with an important adage from a well-known American artist: “After a while you learn that privacy is something you can sell, but you can’t buy it back.”[11]

Three 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. [12] The toilet assumption is also applicable to the disconnection between the electronic communicator and his or her digital trail. There is a perception of privacy when an individual electronically communicates, along with an implicit assumption that the audience is limited to the named recipient or the group of social network friends. [7] Moreover, the use of the delete button creates the illusion of permanency, which lowers inhibitions, personal, sexual or otherwise, with respect to the content of the electronic communications.

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
intended recipient from forwarding the content to others. This vulnerability is particularly true in the workplace, where emails, text messages and social networking posts can form the basis for discrimination complaints and potential litigation. [13]

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. 2

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 easily accessible by the employer. 3 Similarly, the potential for employer accessibility to off-duty blog posts, and social networking pages, is frequently under appreciated. Nevertheless, a new term has been coined to describe being terminated over the content of a blog: dooced. [14]

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 e-mailed to a wide audience.” [15]

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 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. [16]

Work-related examples of electronic exhibitionism are not limited to fiction. The US Supreme Court upheld the termination of a police officer for the on-line sale of pornographic videos of himself in uniform. 4 A sociology professor was suspended as the result of posted comments on her Facebook page about her students, which were perceived as threatening. [17] 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. [18] An American high school teacher was forced to resign after administrators learned of the posting of photographs on her Facebook page that showed her drinking alcohol while on vacation. [19] Finally, the angry and homicidal comments of a bus driver on his Facebook page have become a part of an investigation into his actions leading to a pedestrian death. [20]

The disclosures resulting from electronic exhibitionism is 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.

In summary, the mindlessness implicit in electronic exhibitionism has led to the expansive disclosure of personal and business information that is accessible to a potential worldwide audience. 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 publicized in traditional media. Finally, the use of password protections can have the unintended consequence of creating the false sense that an

---

3 In Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir 2008), rehearing en banc den., 554 F.3d 769 (9th Cir 2009), cert granted, Ontario, Ca. v. Quon, 130 S.Ct. 1011, (2009) the United States Supreme Court is scheduled to decide an appeal by a California municipality to a ruling finding that it violated the constitutionally protected privacy rights of one of its police officers when it obtained the content of personal text messages sent and received from the municipality’s pagers. A decision on the appeal is expected by the end of June 2010.

4 City of San Diego, Cal v. Roe, 543 U.S. 77 (2004). In light of the subject of this article it is fair to admit to an early morning post about this decision, which remains available online six years later. See, W. A. Herbert, The Decline in Protected Worker Free Speech Needs to Be Challenged, ACSblog, American Constitution Society, available at http://www.acs.law.org/node/9043
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.

3. Electronic Voyeurism and the Problem of Too Much Information

Six 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. [21] 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, six years ago, none of Pollitt’s targets had 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. [22]

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 searching for details about their co-workers and colleagues. [23]

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 are fully understandable when a social networking page is hacked and personal and erroneous content is then spewed to others. [24]

The growth and popularity of social networking have inspired requests for electronic friendships fraught with potential danger. For example, a state court judge was reprimanded for communicating with an attorney through Facebook during litigation. [3] Another judge was reassigned after attorneys complained that he had requested becoming Facebook friends. [25] A Florida judicial ethics opinion has warned against judges seeking to befriend attorneys on Facebook because it may convey the impression of a special relationship. [6]

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. For example, a potential legal mine field is created when a manager and subordinate befriend each other through social networking. Such communications can lead to claims of harassment and/or proof of employee misconduct. [26]

It is common for US employers to monitor workplace computers for the content of employee email, web wandering and downloads. [1][27] The monitoring is accomplished through the application of software and periodic audits. Through this monitoring, employers can track the content of email, websites visited and images from those websites. Such monitoring can lead to the discovery of personal and confidential information that is maintained on the employer’s mail server or hard drive. In some jurisdictions, the attorney-client privilege can be waived when an employee utilizes his or her employer’s computer to communicate with a personal attorney.

There are a number of nondiscriminatory business reasons for an employer to monitor and access employee workplace electronic activities. These reasons include: protecting intellectual property and trade secrets; complying with regulatory obligations; seeking to avoid liability based upon conduct of its employees; conducting discrimination and disciplinary investigations; and

5 In Re B. Carlton Terry, Jr., Inquiry No. 08-234 (April 1, 2009) available at http://www.aoc.state.nc.us/www/public/coa/jsc/publicreprimands/jsc08-234.pdf

responding to discovery demands from regulatory agencies and litigants.

Unlike the European Union (EU), and its member States, there are few legal restrictions limiting US employers from engaging in workplace computer surveillance. [1][28] 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 workplace computer use policy or it permitted the use of individual employee passwords to restrict accessibility to email or computer files. [1]

In contrast, the provisions and principles of the Convention for the Protection of Human Rights, the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data and the 1995 Privacy Directive place greater restrictions on employer accessibility to employee workplace electronic communications. [28]

There are few legal restraints on employers and recruiters accessing public online information about an employee or applicant. According to Microsoft’s December 2009 study, 74% of the recruiters surveyed worldwide admit to evaluating candidates based upon information obtained online. In the US, 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]

An applicant’s electronic exhibitionism can shed light on his or her maturity, prudence and responsibility. Although the study focused on accessing social networking pages, it is probable that the same employers conduct internet searches of websites and personal blogs for information on prospective and current employees.

Employer internet searches of current employees are frequently motivated by 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.7 In addition, a simple internet search can uncover derogatory, defamatory or inappropriate comments and information about the employee, co-workers the employer, or the workplace. [31] Intemperate posts on a website or blog about supervisors and co-workers can lead to termination and other unwanted employment actions.8

An employer may also discover that an employee has posted proprietary or confidential information. 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. [32]

A Google search of a current employee can be part of an investigation into an employee’s workplace conduct. The fruit of the search can uncover facts directly related to the conduct under investigation. In one case, during an investigation into alleged fraud and theft by a government employee, the employer conducted a Google search of the employee’s name. The search resulted in information about his prior employment history. As part of the legal challenge to his termination, the employee claimed that the employer’s 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.9

As a practical matter, the best source for obtaining personal information is from an individual’s blog or social networking page. By their very nature, blogging and social networking encourage electronic exhibitionism. However, there are legal limitations on the means that an employer can utilize to gain access to a privacy protected social networking page or blog.

---


8 See, Curran v. Cousins, 509 F.3d 36, 43 (2007) (employee made critical comments about supervisors and workplace policies on a union’s website that required a registration but was accessible to both members and non-members.); Richer son v. Beckon, 2009 WL 1975436 (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 US Constitution).

A lawsuit stemming from a New Jersey restaurant management’s access its employees’ social networking page sheds light on one of these legal limitations. 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. 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. An appellate court ordered a trial on the pilot’s claims.

There are other potential legal problems for employers who engage in electronic voyeurism. Voyeurism can create the appearance of surveillance toward protected collective worker activities and can be used to prove employer animus toward such activities. The timing of an employer’s discovery of certain personal information, such as a medical condition, off-duty activism or sexual orientation, can form the evidentiary foundation for a claim that a subsequent adverse employment action was motivated by the employer’s knowledge. With the possible increase in the use of social networking during labor organizing campaigns, employer electronic voyeurism may lead to liability because some employers forget that voyeurism, like exhibitionism, leaves an evidentiary digital trail.

A discussion about 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 parties and witnesses. The rationale for such access is that a social networking page can be a rich source of relevant information. For example, a claim for mental anguish resulting from a termination can be challenged or supported based upon the content of a plaintiff’s Facebook page. 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. In Canada, courts have ordered the production of publicly accessible Facebook content and have admitted such content into evidence.

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 posted on the social networking page. One Ontario judge ruled that because a litigant permitted public accessibility to extensive personal information on a Facebook page, additional personal information reserved only for friends must be disclosed.

Finally, it must be emphasized that electronic voyeurism in litigation is not limited to the accessing social networking content. In the U.S., demands for electronic discovery have become common. Under ediscovery rules, an employer can be required to release employee electronic communications deemed relevant to the issues in a case.

4. Conclusion

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

Despite the ubiquity of workplace email and internet access, it is not common for employers to offer training about email content and etiquette. In contrast, electronic communicative skill training is beginning to be

---

incorporated into legal education curricula and legal literature. [37][38] Another self-regulatory means for resolving certain workplace problems is to permit employees to use encryption or other means for self-identifying their personal and confidential communications. [1]

Workplace training about employer access to electronic activities is rare. Most employers rely upon unilateral imposition of computer use policies, which are issued for litigation avoidance without any related training. Practical training, developed with union and employee participation, 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. [39] Furthermore, labor-management cooperation can assist in establishing prudent limits on electronic voyeurism by placing negotiated checks on employer searches of electronic activities.

Policies and training with respect to employee blogging and social networking are equally important. [40] IBM has issued social computing guidelines that include practical information and suggestions for responsible electronic communications. [41] However, most companies have not followed IBM’s lead. [42] It is far more common for companies to simply ban social networking or block access to social networking pages, a strategy that can alienate younger workers. [43][44]

Another means for responding to electronic exhibitionism and voyeurism is to encourage architectural modifications to communicative technologies. These modifications may include: the development of self-destructing electronic communications [45]; establishing a pre-send email review function; the development and installation of periodic workplace privacy reminders; and encouraging the use of encryption, passwords and other privacy options.

Governments can play an important role by seeking to compel telecommunications and social networking companies to encourage responsible electronic communications. In the US, legislators, administrative agencies and computers scientists are exploring regulatory and architectural means for enhancing online privacy notification. [46] The Social Networking Task Force of the European Commission is working on obtaining self-regulatory declarations from social networking companies aimed at protecting children. Data protection agencies, such as the Article 29 Working Party, can play an important role by providing recommended solutions. [47]

Finally, some unanticipated consequences of new communicative technologies may require legislative action. This has already occurred in the EU, its member States and to a limited extent in the US. [1][26] In England, advocates want a ban on employers using social networking pages in selecting applicants. [46] There are proposals in the US for regulating surveillance of social networking pages. A bill in New Jersey would impose penalties for sexually or harassing communications through social networking. [13] Legislative and administrative initiatives at various levels of government are indicative of the growing regulatory patchwork quilt aimed at an integrated worldwide means of electronic communications.

Acknowledgements

Mr. Herbert would like to acknowledge his daughters Beth Lee-Herbert and Lisa Lee-Herbert. For over a decade, they have patiently tutored him with respect to computer-based technologies. Without their bemused assistance, this article would not have been possible.

References


13 Social Networking Safety Act A3757 available at http://www.njleg.state.nj.us/2008/Bills/A4000/3757_R1.HTM


[37] M. H. Weresh, More E-mail Tips, E-Tone, Anonymity, and Social Glue (FWIW), The Iowa Lawyer, Nov 2008, p. 22.


