

OCTLA

THE GAVEL

A QUARTERLY PUBLICATION OF THE
ORANGE COUNTY TRIAL
LAWYERS ASSOCIATION



Nuts & Bolts

**MILD TRAUMATIC
BRAIN INJURY**

**PHYSICIANS' DUTY
TO ADVOCATE**

**PROTECTING SSI
AND MEDI-CAL
BENEFITS**

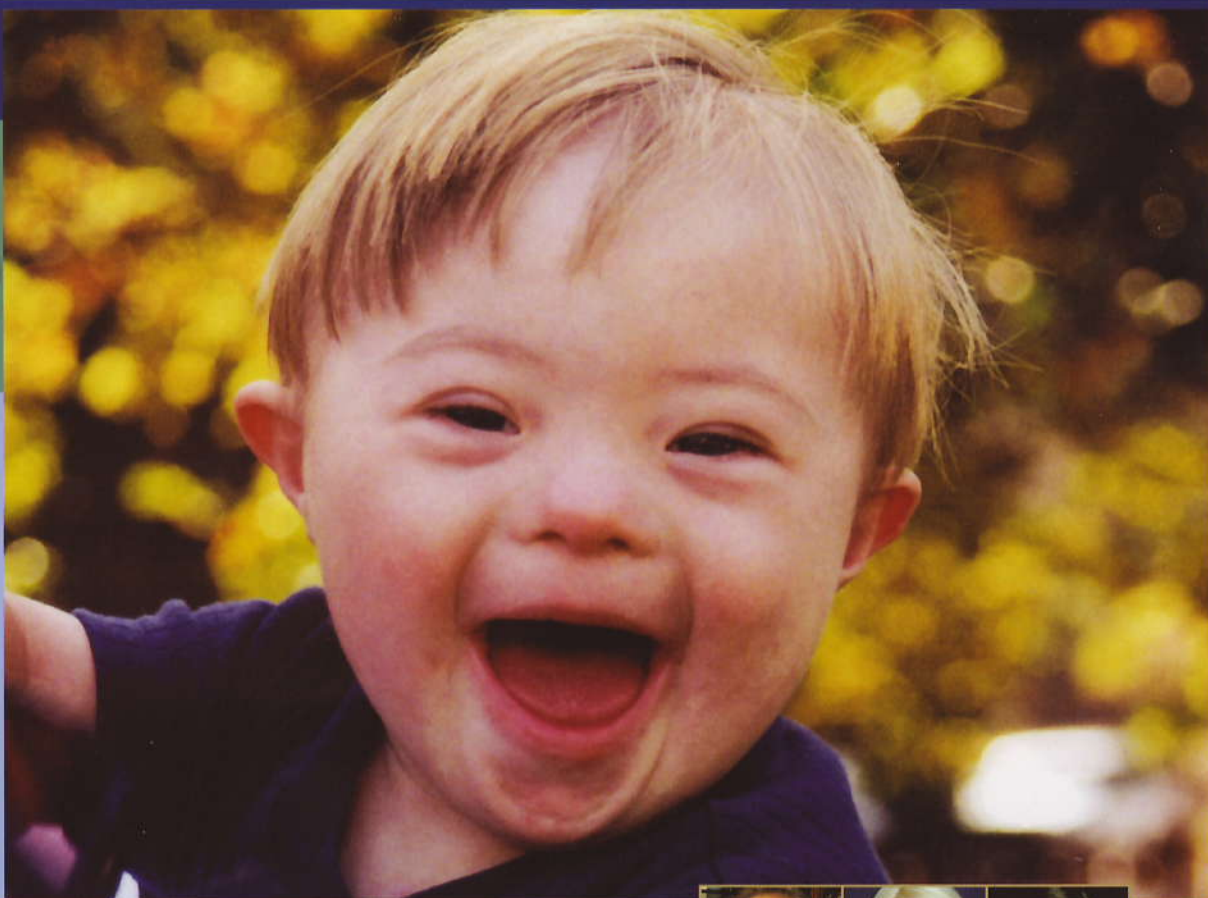
**TECHNOLOGY IN
THE COURTROOM**

***In-Depth Analysis*
PORNOGRAPHY IN
THE WORKPLACE**

**WORKPLACE
VIOLENCE**

WWW.OCTLA.ORG

VOLUME 9, NUMBER 4



OCTLA's Silent Auction

OCTLA'S TOP GUN DINNER & SILENT AUCTION—

***THIS YEAR WE LEND OUR SUPPORT TO BENEFIT THE
DOWN SYNDROME ASSOCIATION OF ORANGE COUNTY,
SEE PAGE 27...***



***OCTLA'S 2006 TOP GUNS—
OUR WINNERS, PAGE 22...***

FALL 2006

Porn on the Office Computer: Employee Privacy or Employer Liability?

A recent appellate court decision has created quite a stir among employment law experts. The case arose in New Jersey, but will likely have nationwide implications: In *Jane Doe vs. XYZ Corp.*, 382 N.J. Super. 122; 887 A.2d 1156; 205 N.J. Super. LEXIS 377; 23 I.E.R. Cas. BNA 1549, the court held that when an employer has actual or imputed knowledge that an employee is using a computer at work to "access pornography, possibly child pornography, [the employer] has a duty to investigate...and to take prompt and effective action to stop the unauthorized activity." While law professors protest that the case is a huge infringement on employees' privacy rights, the decision creates yet another basis for "hostile environment" claims on behalf of co-workers of the Internet porn surfer.

The New Jersey Case

When the 42-year-old accountant was hunching over at his computer concealing the monitor from his coworkers passing behind his chair, at first some thought the proximity between man and machine was due to his weakening eyesight. Not so! Instead of devoting his workday to his regular duties, this employee was using the company computer regularly and

Nicholas J. Toghia has a JD from the USC School of Law, and an MBA from USC's Marshall School of Business. He is an adjunct professor at UCLA Extension, Chapman University, and Loyola Marymount University where he teaches Employment Law for Business. He is a founder of OPUS GROUP LLC, a firm providing consultation, on-site education, training and investigation services for clients regarding a variety of workplace environment issues including wrongful termination, discrimination, and sexual harassment. He can be reached through his website at <http://www.opusgroupedu.com/>.



repeatedly to access pornography on line, with website names such as "Sextracker," "Sleazy Dream Main Page," "Teennflirts.org," "Incest Taboo," and "Young Girls Nude 13-17 Years Old." Each time he logged on, the computer recorded the visit as a historical "cookie" leaving a telltale digital record of the websites accessed by this employee. He was not just an occasional browser. Beginning in 1998 or early 1999 and stretching over a period of several months, these website visits recurred many times a day during business hours.

The company's Internet Services Manager assigned to service workstations routinely reviewed computer log reports as part of his normal duties. He discovered the employee's activities and informed his superior, the Senior Network Administrator, as well as the employee's immediate supervisor. All three managers told the employee to stop these activities, but did not inform their own supervisors of what happened. Instead, a limited investigation was con-

ducted for a day or two and the server logs revealed that notwithstanding the "cease and desist" directive, the employee was still visiting pornographic web sites on his employers office computer, including "bestiality" and "necrophilia" sites. Notwithstanding these odious activities, the network administrator was instructed to stop tracking the employees Internet usage because of a company policy on employee privacy that prohibited monitoring or reporting the Internet activities of employees. Violation of this "no snooping on other employees" policy carried a penalty from reprimand to termination.

Several coworkers in his department noticed that while in his cubicle, which had no doors and was open to view, the employee was acting strangely by shielding his computer screen and quickly minimizing the images on the monitor whenever someone was in the vicinity so that others could not see what he was viewing. Coworkers reported these incidents to their supervisor and they correctly surmised that the employee was viewing pornography, which made the rest of the workers in employee's unit feel distinctly uncomfortable. Nevertheless nothing resulted from their complaints. Several more discussions and meetings among company supervisors and upper managers did not result in any discipline or other action against the employee, although they actually knew of the employee's proclivities and activities for many months.

In October 2000, the employee married a woman with a ten-year-old daughter, and during the next five months he secretly videotaped and photographed the child at

OCTLA GAVEL

their home in nude and semi-nude positions. He then transmitted the clandestinely taken photos of his young stepdaughter over the Internet from his workplace computer to a child porn site in order to gain access to the site. In June 2001, the employee was arrested on child pornography charges. His arrest followed the discovery of nude photographs of the stepdaughter in the company's trash dumpster. He acknowledged that he

mother of the minor child against the employer. The company defended on the ground that the employee's privacy rights trumped the employer's right to monitor his computer use at work.

The Appellate Court, in reversing the trial court, noted the following issues had to be addressed: (1) whether the employer had the ability to monitor the employee's use of the Internet on his office computer; (2) if

In the published opinion, the Court found that (A) the employer admitted it had the capability to run software to monitor employees' activities on the Internet; (B) the employer's own e-mail policy recited that "all messages composed, sent or received on the e-mail system are the property of employer" along with the "right to review, audit, access and disclose all messages." Concerning the Internet, employees

were permitted to "access sites, which are of a business nature only"; and (C) the employer actually

"The existence of a duty for the employer to act is a matter of law."

stored child pornography, including nude photos of his stepdaughter, in his workplace computer. He also admitted downloading over 1000 pornographic images while at work. A search of his computer showed e-mails being sent to porn websites and interactions with others regarding child pornography.

Although the employer took no immediate disciplinary action, suit was filed by the

the employer had the ability to do so, whether it had the right to monitor the employee's activities; (3) whether the employer knew, or should have known, that the employee was using the office computer to access child pornography; (4) whether the employer had a duty to prevent the employee from pursuing his activities; and (5) whether employer's failure to act caused harm to the child.

knew from the computer logs, reports from supervisors, and complaints by coworker employees, that employee was using the office computer during work hours frequently and repeatedly to visit Internet porn sites. The most important ruling was issued in response to the following question: did the employer have a duty to prevent employee

(Continued, see Office Porn, page 10)

Office Porn

(continued from page 9)

from continuing with his activities once it became known what he was doing? In other words, was the employer under a duty to act, either by (1) terminating the employee or (2) reporting his activities to law enforcement authorities, or both. The court unequivocally answered these questions with a resounding "Yes."

The opinion then explained that the existence of a duty for the employer to act is a matter of law deriving from considerations of both public policy and fairness. the court noted that it is a crime, under both state and federal laws, to possess or view child pornography. The federal law is the Protection of Children from Sexual Predators Act of 1998 (PCFSPA). Another federal statute is the Child Online Protection Act (COPA). These laws are expressions of public policy against child pornography and reflect the legislative intent that public policy

favors the exposure of crime.

This appellate decision plowed new ground in the fertile lands of employment law. It created a form of employer liability. Viewed in isolation it may be dismissed as a case of aberrant behavior by a pervert. But academic literature based on credible research maintains that sexual predators are more prevalent today not only as misfits on the periphery of society, but also insinuated into the workplace. While the pervert who peddles pornographic digital photos of underage stepdaughters may be rarity, it is not uncommon to have an "office lecher" who likes to access pornographic websites that distress his fellow employees and create a hostile work environment for his coworkers.

Some startling economic statistics support the academic research. According to an industry survey of the entertainment industry announced on Fox TV network on March 26, 2006, in 2005 the industry

produced 13,600 new porn movies. there were 93 million DVD rentals of pornographic movies euphemistically referred to as "adult entertainment." Pornographic movie production is a \$13 billion industry, and its products and distribution websites receive 70% of hits during working hours, between 9-4 in every time zone. There is a 70% probability that those who visit porn websites will eventually lose their jobs as their non-business related use of company equipment is discovered by management, leading to further damage to their marriage and family relationships.

The case is a stark and ominous illustration of the dark side of technology, and this decision imposed a new form of liability on employers. Even before this case employers had the right to monitor company computer use by employees if the terms of employment and the employee handbook spelled out such procedures. But such right was

OCTLA GAVEL

permissive, not mandatory. More than an absolute right, it was viewed as a combination of employer business policy and a limited waiver of privacy by the employee. It is a huge leap from saying that an employer can, if it wants to, monitor and control employees' e-mail and Internet access, to saying that an employer is liable if it doesn't supervise an employee's use of the office computer equipment.

The foregoing case is but one example of the abuse, misuse, and non-work-related exploitation of company-owned and company-maintained office equipment. However, there are other categories of misuse of office apparatus, information technology or telephone communications that create liability for employers. The following is a brief compendium of the major offenses and offenders.

Other areas of Liability Exposure

Workplace privacy issues have become a significant area of litigation between employees and employers. Here are some categories of liability for employer practices arising out of technology utilization that either expose companies to liability for invasion of privacy, or create a hostile work environment:

Monitoring Telephone Calls

Employers have always monitored employee job performance for productivity, efficiency, and work product quality, but traditionally they relied on managers and supervisors to do this. Today, employers are using technology to track employee work performance, sometimes by monitoring telephone calls. In some industries, such as airline reservations, telemarketing, and customer complaints, employees understand that they may be monitored. Recorded messages advise callers that their conversations may be monitored "for quality assurance purposes." if the caller continues there is an implied, if not express, consent to recording every word exchanged during the conversation. But what is the rule about outgoing calls made by the employee? The same rationale would not cover such eavesdropping. Indeed, the Electronic Communications Privacy Act (ECPA) enacted by Congress in 1986 specifically prohibits the intentional interception of "any wire, oral or electronic communication." 18 U.S.C. § 2510(4). Therefore unless the employee consents to the monitoring of private conversations, the interception, monitoring, or recording of such conversations may be illegal and support a claim for invasion of privacy.

Using Video Surveillance and Taping Conversations

As technological innovators create smaller, faster, less failure-prone devices and as the cost of such technology becomes cheaper than human observers, many companies are relying on video surveillance equipment

(Continued, see Office Porn, page 35)

Office Porn

(continued from page 11)

to observe what transpires on the factory floor, warehouse, storage room, lockers, hallways and other areas where employees are in transit or perform work. In response to being watched at all times, employees have brought claims against employers alleging constitutional and statutory violations for monitoring the workplace through the use of electronic devices such as hidden cameras and other types of motion-activated video surveillance recorders. The critical issue is whether the employees have an objectively reasonable expectation of privacy that they would not be videotaped by their employer. Under California law, employers may not video or audio tape employees in a restroom, locker room, or room designated by the employer for changing clothes. Cal. Labor Code § 435. But the expectation of privacy may also include situations that are not obviously private. For example, in a cubicle environment, where conversations can be overheard because there are no walls or doors, employees may still have a reasonable expectation that their conversations will not be intercepted, especially if they speak in *sotto voce* [ie, under one's breath] and stop talking whenever others appear.

Monitoring E-Mail

If there is one area where employees ignore prudence and caution, it is when they use e-mail and express themselves through the keyboard and the send button in ways they would rarely attempt to do in verbal communication. People do not use the same level of care when drafting electronic communications as they do when drafting written-on-paper communications. When employees send or receive crude or lewd e-mail, users believe a password guarantees privacy, speed creates a "click, click, click ...oops" moment because when it is gone, it is gone for good and cannot be recalled; when clicking on "send to all"

reaches destinations never imagined or intended—all of these acts create liability not only for themselves but for their employers. The proliferation of this technology has left heaps of liability in its wake. Sources of employer problems attributed to e-mail use include inadvertent disclosure of racial, ethnic, or gender insults, offensive graphics, and jokes which constitute harassment. The Federal Wiretapping Act as amended by ECPA controls employer liability for intercepting e-mail and the applicability of the ECPA to private employers monitoring their employee's e-mail is still unresolved by federal courts. California is more predictable. Calif. Penal Code § 631 makes it unlawful to intentionally tap or make an unauthorized connection with a telegraph or telephone wire, line, cable or instrument or willfully and without the consent of all parties to the communication, or in any unauthorized manner, reading or attempting to read or learn the contents of a communication while in transit or being sent from or received at any place within the state. Calif. Penal Code § 632 makes it unlawful to intentionally and without consent of all parties eavesdrop upon or record confidential communication.

Monitoring Internet Use

The Internet has become the defining technological innovation of our time. It has made access to information and conducting transactions fast and easy. However, many employees are using the Internet for a multitude of non work-related purposes, including downloading free computer games, checking stock quotes, reading the "sports page" and conducting on-line shopping transactions. Employee misuse of employer provided Internet access has gone beyond downloading games or checking sports scores. Open viewing of sexually explicit Web sites such as Penthouse, using Playboy screen savers, viewing photos of nude sex "bombshells" or streaming videos of pornographic performances have become

(Continued, see Office Porn, page 36)

Office Porn

(continued from page 35)

more than just a cause for loss of productivity. These and other inappropriate conduct may create a "hostile work environment" and provide the basis for sexual harassment claims. The Telecommunications Act of 1996 imposes criminal liability for transmitting or allowing to be transmitted "indecent" materials over online and computer networks to which minors have access. Although this law limits the liability of companies whose employees illegally spread obscene material without management knowledge, employers may nevertheless be held liable for the creation of a hostile work environment.

Blogs, Chat Rooms, Instant Messaging, Cell Phone Cameras

When they first appeared, Internet users created weblogs or "blogs" to share useful Internet sites with other net surfers. Since then, blogs have evolved into on-line diaries, chat rooms and instant messaging and thereby created personal public forum for discussing office politics, management misconduct, and disseminating discriminatory and slanderous comments targeting co-workers, supervisors or executives based on race, gender, sexual orientation,

disability, age and a host of other graphic and verbal comments that violate Title VII or FEHA. A recent abuse of technology is the use of cell phone camera features for "upskirting"-taking snapshots of unsuspecting female coworkers by bending over and pretending to pick up some object from the carpeted floor while clicking the shutter button, then disseminating the pictures over the company intranet accompanied by offensive commentary.

The Role of the Consulting Expert

The foregoing is a brief but representative sample of the many sources of employer-employee conflict in the workplace that could expose a company to liability for violations of federal and state statutes and case law. The challenge for both sides is how to present the claims and defenses in a cogent and admissible fashion to the trier of fact. The courts must balance an employee's right to privacy with an employer's interest in monitoring its employees' conduct, and

at the same time the legal system must also protect the rights of coworkers who are entitled to work in a safe, harassment free, and non-hostile environment.

Independent consultants with knowledge, understanding, and experience in investigating workplace incidents are an important resource to both employers and employees and their attorneys in advancing or defending claims arising out of workplace misconduct. They can gather and review employers' policy manuals, employee handbooks, complaint procedures and dispute resolution protocols and opine whether such are within or below the prevailing standard of care in human resources management.

Consulting experts can investigate and determine whether the employer has systems in place as opposed to no published policies but only an ad hoc approach to the following important subjects:

- Are the company's computers and other

OCTLA GAVEL

equipment (fax machines, photocopiers) to be used solely for company business

- Has the company reserved the right to monitor the employee's use of company computers, including but not limited to the employee's use of the Internet and e-mail
- Does the company keep copies of all computer passwords and inform employees that existence of such passwords does not guarantee the confidentiality of any electronic communications
- Is there a firm company policy that the transmission of any discriminatory, offensive or unprofessional messages is strictly prohibited.
- Are all workers aware that on-line access to any discriminatory, offensive or unprofessional messages is strictly prohibited
- Are employees prohibited from using company equipment to post personal opinion on the Internet, especially if the opinion

is discriminatory, political or offensive in nature

- Does the company have a clear, detailed but easy to understand policy against unlawful misconduct in the workplace
- Does the company have an effective employee complaint process without fear of retaliation
- Does the company conduct prompt and thorough investigations of all complaints
- Does the company impose discipline on violators while protecting the victims

The prudent employer and the vigilant employee should both be interested in creating, maintaining and monitoring a workplace environment that is free from misconduct and enables every employee to reach his or her maximum potential and permit the company to economically thrive in an increasingly more competitive environment. ■