



FACT SHEET ON THE CORPORATE LEGAL EXPOSURE ARISING THROUGH EMPLOYEES MISUSING EMPLOYER IT SYSTEMS

- ➔ Corporations are being sued by Employees who have been **sexually harassed or bullied** both through exposure to IIM¹, and in respect of co-workers misusing corporate E-Mail² and Internet Access facilities in the workplace.

Title VII does not proscribe all conduct of a sexual nature in the workplace. Thus it is crucial to clearly define sexual harassment: only unwelcome sexual conduct that is a term or condition of employment constitutes a violation.³ The Equal Employment Opportunity Commission's Guidelines define two types of sexual harassment: "*quid pro quo*" and "*hostile environment*."

The Guidelines provide that "*unwelcome*" sexual conduct constitutes sexual harassment when "*submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment*,"⁴ "Quid pro quo harassment" occurs when "submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual,"⁵ The Supreme Court's decision in Vinson⁶ established that both types of sexual harassment are actionable under section 703 of Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e-2(a), as forms of sex discrimination.

- ➔ Corporations can avail themselves of **statutory defenses** when sued by an Employee who have been sexually or racially harassed through the use of IIM in the workplace by taking **all reasonably practical measures to** avoid the act complained of. Image Interdiction Technologies are a reasonably practical measure.

- ➔ Corporations are **Vicariously Liable** to an Employee who has been Harassed by another Employee.

In the Supreme Court cases *Burlington Industries, Inc. v. Ellerth*⁷ and *Faragher v. City of Boca Raton*,⁸ the Supreme Court made clear that employers are subject to vicarious liability for unlawful harassment by supervisors. The standard of liability set forth in these decisions is premised on two principles: (i) an employer is responsible for the acts of its supervisors, and (ii) employers should be encouraged to prevent harassment and employees should be encouraged to avoid or limit the harm from harassment.

In order to accommodate these principles, the Court held that an employer is always liable for a supervisor's harassment if it culminates in a tangible employment action. However, if it does not, the employer may be able to avoid liability or limit damages by establishing an affirmative defense that includes two necessary elements: (a) the employer exercised reasonable care to prevent and correct promptly any harassing behavior, and; (b) the employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer or to avoid harm otherwise.

¹ IIM means "Inappropriate Image Material". This ranges from soft pornography to hard pornography and on to indecent photographs of children.

² This Fact Sheet treats all form of Instant Messaging, Web Mail and E-Mail as being "E-Mail".

³ 29 C.F.R. § 1604.11(a).

⁴ 29 C.F.R § 1604.11 (a) (1).

⁵ 29 C.F.R § 1604.11(a)(2).1 29 C.F.R. § 1604.11(a)(3).

⁶ 106 S. Ct

⁷ 118 S. Ct. 2257 (1998)

⁸ 118 S. Ct. 2275 (1998)



FACT SHEET ON THE CORPORATE LEGAL EXPOSURE ARISING THROUGH EMPLOYEES MISUSING EMPLOYER IT SYSTEMS

- ➔ Corporations are ***Vicariously Liable*** to a Third Party for an Employee holding of Pedophilic Pornography on the Employer's IT Infrastructure.

The New Jersey Appellate Division, in *Doe v. XYZ Corp.*⁹ ruled that an employer may be held liable in tort to the victim of pornography when it has actual or implied knowledge that its employee is using his workplace computer to access pornography, including child pornography, but does not investigate or stop the employee's conduct. Interpreted broadly, the decision stands for the proposition that New Jersey employers have **a legal duty**, not simply a right, to monitor employees' e-mail and internet use.

- ➔ Corporations are being sued by Employees who have been exposed to ***Pornographic Internet Content*** being accessed by their co-workers.¹⁰

- ➔ Credibility in the market-place is being ***seriously lost*** when it becomes public that Employees engage in Inappropriate Internet Use which involve IIM.

- ➔ Individuals and Corporations may suffer ***Criminal Prosecution*** when employees disseminate Pornography using the employer IT infrastructure.¹¹

- ➔ Corporations may suffer ***Criminal Prosecution*** if they neglect to prevent Employees from downloading Child Pornography into the workplace from the Internet using the employer IT infrastructure. With regard to pedophilic material, considered as "**contraband**" by the Supreme Court¹², the Risks are High and the potential for damage is Substantial. Investigations into this scenario are exclusively handled by the FBI.

- ➔ Individual Executives may ***personally*** suffer ***Criminal Prosecution*** if they neglect to prevent Employees from downloading Child Pornography into the workplace from the Internet using the employer IT infrastructure. Investigations into this scenario are exclusively handled by the FBI.

The Company can be held liable by what is known as the doctrine of identification, also known in Criminal Law as the *alter ego* doctrine.¹³ What this means is that in each Company a Court of Law will recognize certain senior individuals as being the Company itself and the acts of these individuals when acting in the company's business are treated as the acts of the Company.

⁹ N.J. Super., 2005 WL 3527015 (App. Div. Dec. 27, 2005),

¹⁰ See the Examples at the end of this Fact Sheet

¹¹ See the Examples at the end of this Fact Sheet – Disseminating Pornographic Material via E-Mail is a Criminal Offense in Utah punishable with a jail sentence between 30 days and 5 years.

¹² *United States v. Kimbrough*, 69 F. 3d 723, 731 (5th Cir. 1995).

¹³ See generally, C. Wells, "Corporations: Culture, Risk and Criminal Liability" [1993] Crim.L.R. 551. This new form of liability, distinct from vicarious liability, was based on the concept of the company itself being identified with the acts of senior officers, rather than being accountable for the transgressions of employees. See also A. Reed & P. Seago "Criminal Law".



FACT SHEET ON THE CORPORATE LEGAL EXPOSURE ARISING THROUGH EMPLOYEES MISUSING EMPLOYER IT SYSTEMS

REAL-LIFE EXAMPLES

Orlando Police Officer Viewed Pornography While On Duty¹⁴

An Orlando police investigation found that five officers -- including two lieutenants -- used city computers to look at pornography while they were on duty, authorities said Tuesday.

*

Investigators discovered a handful of e-mails sent among officers with pictures of naked women performing sex acts or in sexual positions, although investigators said the officers may have exchanged dozens of images, internal affairs Sgt. Joseph J. Windt said.

"For the workplace, it's inappropriate, clearly inappropriate. What you do on your own time is your own business," Windt said.

The involved officers will remain in their positions and may receive punishment ranging from a written reprimand to eight hours' suspension, he said. Their respective supervisors will decide their punishment, he said.

Lt. Shawn Fawbush, Lt. Brian Gilliam, Officer Shawn Hayden, Capt. Jeffrey O'Dell, and Lt. Victor Uvalle were found to have broken police rules. Hayden, Gilliam, O'Dell and Fawbush admitted to their violations. Uvalle said he could not recall the incidents. Attempts to reach them for comment were unsuccessful. While the e-mails were sent between two and four years ago, they only came to light in December 2005 during proceedings for a civil court case against the department filed by Officer Matthew Floeter, according to a 10-page internal-report summary released Tuesday. Floeter's suit says that he was sexually harassed.

Floeter said the porn incidents took place in the department's Drug Enforcement Division, located in a building separate from the main headquarters. He gave investigators names of officers involved in sending the images. City authorities removed those computers from the office immediately after the accusation was made and inspected them

Former UNLV Professor Charged with Keeping Child Pornography in the Workplace.¹⁵

A former University of Nevada, Las Vegas music professor has been charged with 25 counts of possessing child pornography after more than 26,000 explicit images were found at his home and office.

Some of the images, which were found on computers, portable hard drives and discs, dated back to 2002, said Conrad Hafen, chief deputy attorney general over the Criminal Division and Political Corruption Unit. UNLV police were alerted to the crimes in August after a technician located child pornography on a UNLV computer server.

The employee was able to trace it back to Soule's office computer and observed Soule in the act of downloading pictures, Hafen said. The attorney general's office filed a criminal complaint against Soule and expected to arrest him by Wednesday. Soule retired from UNLV on Oct. 13 after earning more than \$102,000 in 2005. He was scheduled to teach several flute classes this semester.

Port of Seattle Police Officers discovered sending Pornographic E-Mails¹⁶

Thirty-two current and former Port of Seattle police officers -- nearly a third of the department's sworn force -- have been caught exchanging or receiving racist, sexist and sexually explicit e-mails since the end of October 2004, department records obtained by the Seattle P-I show.

¹⁴ Reported in the "Orlando Sentinel" -- December 5th 2006

¹⁵ Reported in the "Las Vegas Review Journal" -- October 24th 2006

¹⁶ Reported in the "Seattle Post - Intelligencer" -- January 19th 2007



FACT SHEET ON THE CORPORATE LEGAL EXPOSURE ARISING THROUGH EMPLOYEES MISUSING EMPLOYER IT SYSTEMS

For 16 months, no one in the department reported the smut-laced e-mails to top-level managers or internal investigators, even though the field-level supervisors joined line officers spending hours on their shifts viewing the material. The behavior wasn't discovered until a woman accused one officer of harassment, and internal investigators looked at his computer.

Records obtained by the P-I show such behavior has been going on in the department for years, including a case in 1997 that involved a prominent sergeant who is now a lieutenant and SeaTac city councilman.

Though some in the department recommended tougher punishment for those caught up in the current case, few of the officers involved were disciplined. Nine got written reprimands, and others who received e-mails, but didn't store or forward them, were let go without punishment. The accused harasser, Sgt. Jon Schorsch, 39, also was found to have misused the Internet, but he resigned under threat of termination after a judge issued a protection order in the harassment case. No one, including lieutenants and sergeants, was punished for failure to report the Internet abuse, though failure to do that is a department rule violation.

The department-wide investigation conducted between March and September uncovered dozens of inappropriate e-mails, including derogatory and stereotyping comments, photographs and video images aimed at blacks, Asians, Arabs and Hispanics.

Other e-mails showed sexually graphic and demeaning pictures of women, including images of them defecating on each other, having sex and performing oral sex. Still others contained images of a woman kicking a naked and bound man in the crotch, and a video of a woman whose tube-top is yanked down by a stranger on the street.

Maryland Employees View Pornography at Work¹⁷

A legislative audit of computer records released yesterday found that 22 maintenance workers, police officers and other employees at the Maryland Transportation Authority and the Maryland Aviation Administration pulled up hundreds of porn Web sites at work last fall.

Officials at both agencies said disciplinary action has been taken against the employees, but wouldn't say whether anyone had been fired.

"(I was) shocked to hear about the violations," said Ronald L. Freeland, executive secretary of the MdTA. "Disappointed that they would use their employer's work time to do it."

Both agencies already use Internet monitoring software that restricts access to explicit Web sites, but they'll hire outside contractors to install more rigorous software.

The Office of Legislative Audits checked computer records over a 31-day period after being alerted to the pornography by a call to the state's fraud hotline. Bruce Myers, who led the audit of both agencies, said MAA employees used state-owned computers to view sexually oriented Web sites up to 600 times in an eight-day period. The MdTA employees accessed similar sites up to 2,200 times in a seven-day period.

Auditors disregarded violations if they couldn't be tied to an individual employee or appeared to be a mistake.

Sixteen of the employees worked at the MdTA, which oversees the state's toll facilities and the MdTA Police, and the other six worked at the MAA, which runs BWI Thurgood Marshall Airport.

"This behavior is unacceptable and it will not be tolerated," said MAA spokesman Jonathan Dean.

In their responses to the audit findings, included with the report to the General Assembly, the agencies said they'll have contractors conduct a more expansive review of Web sites accessed by their employees. Both reviews are expected to be completed by July 2007.

¹⁷ Reported in the Maryland Legislative Audit of March 12th 2007



FACT SHEET ON THE CORPORATE LEGAL EXPOSURE ARISING THROUGH EMPLOYEES MISUSING EMPLOYER IT SYSTEMS

Though pornographic Web sites often attempt to spread computer viruses or spyware, Mr. Freeland and Mr. Dean said no such harmful software appears to have been installed on state computers. Sen. Ed DeGrange, D-Glen Burnie, whose district includes BWI, said the violations bothered him but proved that the audit process works.

"That's why we have legislative audits, to find these kinds of abuses," he said. "Now the agencies are aware of it. They're looking into it, and if they find it necessary, heads will roll." Mr. Myers doesn't consider the problem widespread.

A survey conducted by Websense, an Internet security company, found that 12 percent of employees surveyed have visited pornographic Web sites on the job. About 95 percent of those employees said their visits were accidental.

"I think this is isolated to a few employees and this shouldn't make a black mark on the whole state of Maryland," Mr. Myers said.

The legislative audit is available at www.ola.state.md.us/Reports/Hotline/MAA-MdTACompMisuse2007.pdf.

Salt Lake City Police Union Sent Pornographic Attachments to E-Mails¹⁸

Salt Lake City - The head of the Salt Lake City police union is under investigation for sending sexually explicit photographs from his work computer.

Tom Gallegos, president of the 300-plus-member Salt Lake Police Association, sent photographs depicting sexual acts and nudity over a work e-mail account "several times" between February 2005 and October 2006, according to police records and members of the city's Police Civilian Review Board.

Gallegos' actions earned him a written reprimand from police administrators in January. But Mayor Rocky Anderson, who caught wind of the photos this week, said Gallegos would be investigated further. He declined to say which agency was investigating. "This matter is being handled as any other matter involving potential criminal misconduct," Anderson said.

Asked how graphic the photographs were, Anderson said he began looking at them but stopped. "Two was enough," he said. Antje Curry, a former review board member who reviewed the Gallegos case, said the photos were "in horribly bad taste." "I don't think there's any question that the e-mail that was passed around was pornographic," said Scott McCoy, the new acting chairman of the board, a citizens panel that investigates complaints of officer misconduct.

Gallegos did not return several phone calls seeking comment Friday.

Sending pornographic material over e-mail is a third-degree felony that carries a prison term of 30 days to five years, according to Utah law.

Assistant Attorney General Paul Amann said he expected any police department that suspected an officer of committing a felony to turn the investigation to an outside agency for review. "If there is a crime there, that's something for law enforcement agency - presumably a separate law enforcement agency - to examine," Amann said. That apparently did not happen in the Gallegos case. Salt Lake City Police Chief Chris Burbank did not return phone calls this week. Police spokesman Jeff Bedard refused to say whether other officers exchanged the e-mails. "We're really not going to say anything else except what's in there," Bedard said, referring to portions of Gallegos' disciplinary record, which were released this week by order of the city's Records Appeals Board. The written reprimand in January was the third such discipline Gallegos has received in two years for inappropriate conduct with co-workers, according to the disciplinary records.

¹⁸ Reported in the "Salt Lake Tribune" - May 26th 2007



FACT SHEET ON THE CORPORATE LEGAL EXPOSURE ARISING THROUGH EMPLOYEES MISUSING EMPLOYER IT SYSTEMS

Sexual Harassment is Not a Joke to Employers¹⁹

Anita Hill ... the Lewinsky-Clinton affair ... the crude e-mail you received (and forwarded) last week ...

It would be nearly impossible to be a member of American society and not have at least some familiarity with the concept of sexual harassment. Perhaps it is these images of Senate hearings, seemingly endless media dissection and “good-natured” e-mail banter that cause the mere mention of the phrase “sexual harassment” to be met with chuckles, eye rolls and a general flippancy. For employers, however, claims of sexual harassment, and the lawsuits that sometimes ensue, are no laughing matter.

In fact, the cost of successfully defending a single harassment suit routinely exceeds \$100,000. Even worse, according to the Equal Employment Opportunity Commission (EEOC), the average sexual harassment verdict against an employer is more than \$250,000, with some verdicts reaching into the millions and even tens of millions of dollars.

What's more, these lawsuits are far from uncommon. In 2006, employees filed more than 15,000 claims of sexual harassment against their employers with the EEOC. This figure does not even include the tens of thousands of complaints that employees made to their state human resource commissions. Significantly, the number of sexual harassment complaints filed with state and federal employment commissions has risen steadily every year since the first sexual harassment lawsuit was filed in 1976. Nevertheless, even three decades after these lawsuits first appeared on the business horizon, many employers are still ill-equipped to prevent this type of illegal behavior from occurring within their workplaces and to defend against these cases once they are filed.

That's the bad news.

The good news is that employers can take preventive steps to minimize the risk that they will be sued for sexual harassment. Critically, these same steps go a long way toward shielding the business from liability in the event the company is sued.

Before an employer can work to prevent sexual harassment from occurring, the employer must have a clear and accurate understanding of the two distinct types of sexual harassment that can plague a workplace. The first and least common form of harassment is quid pro quo harassment. This occurs when a supervisor uses his or her control over a term or condition of an employee's job for romantic or sexual gain. Examples include requiring sexual favors of an employee to maintain employment and hinging salary increases on an employee's response to sexual advances.

The far more common type of harassment, occurring in the strong majority of all sexual harassment cases, is what is known as hostile work environment. This form of harassment can occur at the hands of supervisors and coworkers alike. A hostile work environment is created where an employee experiences workplace harassment and fears going to work because of the offensive, intimidating or oppressive atmosphere generated by the harasser. Whether a harasser has created a hostile work environment is determined by a review of all of the circumstances, including the frequency of the allegedly harassing conduct, its severity, whether it is physically threatening or humiliating and whether it unreasonably interferes with an employee's work performance

¹⁹ Reported in the “The Democrat” – May 13th 2007. An Article by Bill Krizner. Bold highlighting of text by Dr. Bandey.