CHAPTER 10

WORKPLACE PRIVACY

Moderator: Mark Thompson, NAA member, Vancouver, British Columbia

Panelists: Terry Bethel, NAA member, Bloomington, Indiana
Matthew Finkin, NAA member, Champaign, Illinois
Paul Gerhart, NAA member, Cleveland, Ohio

Mark Thompson: This session may have begun at the Fall 2003 Education Meetings of the NAA. The day that meeting began, the local newspaper reported that the City Manager was having an affair with a city employee who had been promoted rather quickly. A subsequent sexual harassment investigation turned up 622 e-mails between the two parties, of which 577 were sexually explicit. So the issue was whether these e-mails should be available in their entirety for the investigation. Previous sessions in the Academy that have touched on this issue in discussions of employee surveillance and monitoring technology. We found then that there were not many cases involving these exotic technologies.

This session, therefore, will focus on the issue of employee privacy rights as they intersect with: (1) the rights of management to oversee the actions of its employees; and (2) the arbitration process. The discussion will be built around several cases developed for this symposium. The first cases discussed will examine more traditional privacy concerns and the latter ones will deal with problems associated with the newer technologies.

An Overview

Matthew Finkin: We think that the subject matter, i.e., privacy rights at the workplace, is still evolving. To provide an overview, employers tend to ground their right to monitor employee behavior on concepts of property rights or management prerogatives and the employees tend to protest such surveillance as an invasion of privacy rights. We will build our discussion around several real-

life incidents. All of these cases have been decided either in arbitration or before another tribunal. This is an especially intriguing area because seldom is there any contractual language that deals with issues of employee privacy. A 1992 study conducted by the Bureau of Labor Statistics found that only 17 of 640 collective bargaining agreements had any provision on employee privacy, and most of those 17 cases came from agreements with the Communications Workers over telephone monitoring of operators.

With the growth of e-mail and electronic interception, the continued absence of contractual treatment is rather surprising. Here are some of the questions that arise in this arena. Why are American unions not concerned with privacy issues? And, if they are not, are they adequately representing their constituencies? And, why aren't unionized American workers more concerned about potential invasions or infringements of their privacy? Is it because this is seen as a white collar problem, where the extent of organization (except in government) is far less? Is there some time lag between the newness of the issue and the response?

It is also possible that the doctrine of preemption under section 301 of the Labor Management Relations Act has had an impact on the issue. If an employee covered by a collective bargaining agreement claims a right to privacy as a defense against an employer action (e.g., discipline as a result of electronic monitoring), any court case contesting the employer's action might be dismissed on grounds of preemption, i.e., there is a collective bargaining agreement that contains both a management's rights clause and an agreement to arbitrate disputes that arise under the contract. The right to privacy is disposable under American law by the agreement of the employee. Under section 301, such cases may be deferred to an arbitrator. Can it be argued that the employee has waived his or her rights, and the case, therefore, belongs in arbitration rather than the courts?

There is at least one decision involving video monitoring where Chief Judge Posner of the Seventh Circuit suggests that the case should go to arbitration. If the arbitrator holds that the collective bargaining agreement did not speak to the issue, however, this form of monitoring is neither a reserved right of management nor an infringement of an employee right to privacy. If the contract is silent, therefore, the common law action can proceed. This decision leads me to believe that while this doctrine may have spread, it has not yet taken very deep root

Thompson: The first case does not deal with the new monitoring technologies. It deals with a more general problem concerning the admissibility of evidence.

The Mountain Casino Case

The Grievant is a cocktail waitress at a casino. On two successive days, customers have complained to management that she was extremely rude. Management took written statements from the customers. Both asked not to be named on the statement, but acknowledged the statements' accuracy orally after having read them through. The Grievant has been discharged and the union has taken up the grievance under the "just cause" provision of the collective agreement. The Union has demanded the names, addresses, and telephone numbers of the complaining customers; the Company has declined, stating that the customers did not wish to "be involved."

a. The Union asks the arbitrator to sign a subpoena for the Company to produce that information. How should the arbitrator rule?

b. The arbitration proceeds without that information, but the Union argues that in view of its inability to speak to the complaining persons, the written statements should not be considered—and thus there is no evidence of any misconduct. How should the arbitrator rule?

Bethel: I understand why the employer doesn't want to reveal the names of the customers. I also understand why the customers don't want to be involved. If I complained about the service at dinner tonight, that doesn't mean I'm interested in participating in any disciplinary action against the waiter. It's hard for me to understand how an arbitrator could uphold a discharge on the basis of this kind of information without giving the union at least the opportunity to speak to the complaining customer.

We face these kinds of situations in different contexts from time to time, especially when we consider statements from physicians or other people who are absent from the hearing. There may be no practical way of getting these people to the hearing. If all the union wants is the opportunity to talk to the complaining customers, I suppose you could consider arranging a telephone call that protects the identity of the complainants. But if the employer intends to rely on the statements as the justification for discharging the employee, I would be inclined to allow the subpoena. Absent

compliance by the employer, I can't see that I would give the statements any significant weight.

Gerhart: I've never had a case where an employer claimed to have evidence but didn't produce it. These are written statements but there is no indication of notarization. Essentially, what we have here is that classic problem of the inability to cross-examine what's written on paper. In this case, it doesn't seem equitable to allow that kind of evidence into the record, but if it is allowed in, it shouldn't be given much weight and the case would fall.

Finkin: Why is this case here? Someone went to a casino, complained, and maybe doesn't want his or her significant other to know where they were that day. They were outraged enough to complain but they don't want to be involved, and they think it's an infringement of their right of confidentiality to be required to come forward. This hypothetical is actually based on an NLRB decision where the NLRB agonized over whether the promise of confidentiality is binding. For example, prostitution is legal in Nevada. Suppose it was a patron of a brothel who complained about the service and didn't want it known. Should it make a difference that the company had given such a promise of confidentiality? Must an arbitrator respect a customer's right of confidentiality or anonymity when doing so puts an individual's job at risk?

I've had one such case and the position I took was that if someone's job was at stake, he or she had the right to confront the people making the complaints. You can't fire someone on the basis of a written letter saying, "I was there, this happened, and you have to do something about this employee." I'm quite prepared to say that I was insufficiently protective of privacy interests and maintaining confidentiality.

Thompson: I understood the problem to mean that the union thought the statements could come in; that the complaining customer would not show up; and what the union wanted was the opportunity to talk to the customer before the hearing so that it could understand what happened or possibly get a statement contradicting the first statement. Suppose the union gets the name and telephone number of the customer, calls the customer, has some discussion and then when the employer introduces a statement at the hearing, the union doesn't object except to point out that there's no ability to cross-examine. Can you uphold a discharge on the basis of that kind of evidence? Further, this case, being set in a casino, the likelihood is that the customer is from some place distant and is not going to return to testify, especially

if he lost all his money at the casino. And suppose I change the hypothetical and say that we have two complaints in two days or 20 complaints in two days. Does this change your thinking?

From the Floor: I've had cases concerning rudeness of customer service employees in a public electrical utility. Some of these complaints were anonymous, some were signed, and some were called in. The union consistently objected on the basis of hearsay. I do accept hearsay and I have upheld discipline for employees where there are multiple, but not single, complaints against the same employee for similar kinds of behavior.

From the Floor: One of the purposes of that grievance process is to allow both parties to hear each other's case, refine their position, and for the union to make a decision about whether to use its resources to take a case forward. Are any of you troubled by the fact that in this scenario, the union has not had an opportunity to see the other side's case, talk to the witnesses beforehand, and make an evaluation prior to taking the case over to arbitration?

Bethel: Yes, I am troubled. I assume that the union has the customers' statements, but one of the most troubling things for arbitrators is to have a discharge case presented on the basis of hearsay, especially when the principal accuser is not present in the hearing. I wouldn't be inclined to give the statements any weight, if I let them in at all. Some collective bargaining agreements that I work under require the parties to disclose information and the identity of witnesses prior to the hearing, and if they don't, the evidence doesn't come in. In other situations when new evidence or a surprise witness appears on the day of the hearing, I will give an adjournment in order for them to have an opportunity to interview the witness or prepare a defense. In this case, the company did not simply find a witness that it didn't know it had. It refused all along to give information and then at the hearing, it wants to put the information in. I'm not going to let them put the information in over the objection of the union. Depending on what the history of the parties is with respect to these kinds of problems and what the contract says, I may give them an adjournment but if the company's been refusing to furnish information that it had available, I don't think I'd be inclined to let the witness testify that day over union objection.

From the Floor: What do you do in the case when the complaining witness is a child? Where the parents don't want the child to testify because he or she might be traumatized? These cases can range from rudeness, to foul language, to mistreatment.

Gerhart: I think the situation is the same. No matter what the circumstances or how heinous the crime might have been, there still has to be proof and there still has to be the opportunity to confront that proof in a reasonable way.

From the Floor: Would you accept a deposition?

Gerhart: It depends on the circumstances, but if the union had not had a chance to examine the person giving the deposition, I don't believe so. What I suggest is that where a child is making a complaint, special procedures or arrangements can be made and I think as arbitrators we have the power to permit those arrangements. For example, suppose you had an eight- or nine-year-old child complaining about some kind of behavior by a teacher or by a nurse in a hospital, there's no reason why the child couldn't be brought into a private setting and the story told in a way that everyone could see the demeanor of the child and form some impression about the validity and the value of the evidence being given. I think we have to be creative in these kinds of circumstances.

Bethel: Aren't there circumstances in which young children are interviewed by social workers or psychologists and then the interviewer testifies about what the child said? Obviously these cases are much harder than cases involving rudeness to a casino guest.

From the Floor: Is there any rule, law, or regulation that protects this customer's privacy or is this simply a policy of the company? The customer voluntarily stepped forward, voluntarily gave their name, address, and telephone number. Is there anything that would give this customer a privacy right?

Finkin: That's why the NLRB asked whether a promise of confidentiality had been given. In which case it would be a claim of breach of contract. The only possible tort claim would be what's called the public disclosure of an embarrassing or offensive fact and this requires two elements: (1) that there be publicity, i.e., simply a disclosure to any third party; and (2) is the fact so publicized one that would offend a reasonable person? The fact that you made a complaint about a rude cocktail waitress is not in and of itself embarrassing although that one might claim that there is a potential of embarrassment. I think the tort action would fail for want of adequate publicity. Most of the courts are pretty zealous in saying that there has to be a fairly wide distribution in order for this tort to be available.

Finkin: Problem two is listed as *Central States Trucking*. This problem is based on *Cramer v. Consolidated Freightways, Inc.*, 255 F. 3d 683 (9th Cir. 2001), a panel decision that was later reversed.

Central States Trucking—Teamsters

The employer, an interstate trucking company, concealed videocameras and microphones behind two-way mirrors in the restrooms at one of its terminals. The purpose was to detect drug use among its drivers. Employees at the terminal discovered the surveillance equipment when a mirror fell off the men's restroom wall, exposing a camera. A similar hole in the wall was later discovered in the women's restroom. The company's collective agreement with the Teamsters addresses privacy as follows:

> The employer may not use video cameras to discipline or discharge an employee for reasons other than theft of property or dishonesty. If the information on the videotape is to be used to discipline or discharge an employee, the Employer must provide the Local Union, prior to the hearing, an opportunity to review the videotape used by the Employer to support the discipline or discharge. Where a Supplement imposes more restrictive conditions upon use of videocameras for discipline or discharge, such restrictions shall prevail.

The Teamsters grieved the installation of the surveillance equipment as an invasion of employees' privacy. The employer argued that the collective agreement placed only one restriction on its use of videocameras and that the inclusion of the provision in the collective agreement implied consent by employees to be videotaped.

Thompson: Although the original case took place in California, and was contested in court, we have changed the geographic setting of the case to eliminate the impact of California's rather unusual law on privacy, and have moved the case from the court to an arbitration tribunal.

Finkin: As you can see, there is a detailed provision in the collective agreement governing evidence from the use of videocameras for discharge purposes. The company argument in this case is that the union's agreement to the surveillance provision signifies its tacit agreement that the employer could install hidden cameras behind the mirrors in the men's and women's restrooms. How many of you would read this provision to have that effect? {About 4 out of 100 participants answered that they would read the provision that way.} In the actual court case, the Ninth Circuit panel decided that the contract could be read that way and the case should have gone to an arbitrator. This decision was reversed en banc by the full Ninth Circuit.

From the Floor: I thought that you could read the provision to authorize the use of cameras in places where theft of property was likely, perhaps in the warehouse or in the shipping department. It's hard for me to understand how that would justify using cameras in the restroom. I think if the employer has the ability to discharge people with videocamera evidence of theft, you can read this to mean that the employer has some leeway in terms of the kinds of places it can install cameras.

From the Floor: I'm not sure I would disagree with the decision. If an arbitrator found that the contract could be read that way, I would suspect that no court would have overturned that decision. I would ask myself if it was possible that an arbitrator could rule that way and if it is possible, I'm not at all sure that the en banc decision was wrong.

From the Floor: Clearly, this is a problem of contract interpretation. In interpreting the contract, the first question I'd ask myself is "What was the mutual goal of the parties in agreeing to allow the employer to do some taping?" Obviously, the focus of their concern is deterrence of theft. But hidden cameras don't deter theft, exposed cameras do, and there are many situations in which employers put up cameras that don't work. It reduces the amount of theft from customers as well as employees. It seems to me that in agreeing to allow the employer to install cameras and use the film as evidence of theft, the parties are revealing what their goal is. That goal has nothing to do with hidden cameras and hence there has not been any kind of waiver, assuming that the collective bargaining agent even could waive that very personal right of privacy.

From the Floor: The issue in the Ninth Circuit was one of preemption. In order to get by the preemption argument, the legal standard is whether or not there is a clear and unmistakable waiver of the privacy right in the body of the collective bargaining agreement. Because there was no such clear and unmistakable waiver, the court got to the issue and concluded that it was not preempted.

Finkin: The question the court addressed is not whether there was a clear and unmistakable waiver in the contract. The question was whether the union had the power to waive the employees' related privacy rights, and the court en banc said that California law provided a floor of minimum protection below which the union could not agree. So it's irrelevant whether or not the contract had

that effect because the court held that it was without power to have that effect.

Mount Olive Church

The church congregation runs a youth counseling service, funded in part by the United Way. Employees are represented by an independent union. The director of the service suspected, on good evidence, that a counselor was engaging in multiple homosexual relationships. The director was concerned about the impact that the counselor's personal life might have on his work, especially in a faith-based organization. With the assistance of the local police department, the agency hired a computer expert to help it gain access to the employee's personal Hotmail account, which the counselor sometimes accessed using the employer's computer. The hired expert quickly found the counselor's password and gained access to the account. The counselor's e-mails did include references to homosexual encounters, and the employer terminated him.

The union grieved the dismissal on the grounds that the employer's action of gaining access to its member's private e-mail account violated his privacy, and the evidence could not be introduced into a disciplinary proceeding. The employer maintained that it was entitled to review the contents of the mail account, which was used through its computer system.

What ruling on the evidentiary question would you make?

Gerhart: Let me provide some technical background. Hotmail is a free e-mail account service maintained by Microsoft. A Hotmail account may be accessed through any computer that is connected to the Internet. Thus, the grievant could access his account at home, in an Internet café, or at work. To gain access, however, one must provide a password. Thus, the grievant had a reasonable expectation of privacy. The grievant admitted that he did access his Hotmail account through the employer's computers. It is not clear from the facts, however, whether it was on the employer's computer that he generated these e-mails for homosexual liaisons. I have assumed that the employer has no rules restricting the use of its computers for personal purposes at work. This is quite typical, especially for smaller employers.

A fundamental question in the employer-employee privacy area is whether the employee has a reasonable expectation of privacy. For example, if the employer provides the employee with a locker,

does not provide the lock, and permits the employee to use his own lock, there is an expectation of privacy. On the other hand, if the employer provides the lock and the key, presumably there is no expectation of privacy on the part of the employee. This provides a general principle that may be applicable in this case.

I also considered the homosexual aspect of the case was a red herring, or whether it might be relevant. It has relevance if we put it in the context of youth counseling, with related notions of psychological dependency or perhaps drug use.

The bottom line is the extent to which the employer has a right to invade an employee's privacy. The case law essentially says that the employer owns its computer system and has the right to investigate whatever is stored on that system. But in this case the employer broke into the employee's personal Hotmail account, where the messages are stored on a Microsoft server, far away from the employer's premises, and the account is password protected. I think the employee does have an expectation of privacy in this case and I would have some serious problems allowing that evidence into the record if it were obtained as described in this case. Under those assumptions, I would not allow the evidence.

Finkin: I thought the only relevance of the homosexual conduct tied into the nature of the employer—a church, a faith-based organization—and not with the fact that the employee was involved in a youth counseling service. Further, I see no evidence that the employee accessed his Hotmail account at the employer's workplace and, even if he did, that wouldn't necessarily mean that he was doing it on paid time. Otherwise, I agree that you have a password-protected account and no reason to believe that the employee was abusing his computer privileges. I also would not be inclined to let this in, especially because the employer had to hire an outside consultant to break the password.

From the Floor: I was interested in this particular issue three or four years ago and I've lost track of it. There's something called the Electronic Communications Privacy Act that specifically states that computer equipment and electronic mail or data that goes over the line does not have the same protections as a phone call, for example. Let's say, using these same facts, this employee made a liaison over the telephone. I believe that in such a case, the employer could listen in to the phone call, determine that it was of a personal nature, hang up, and then discipline the employee. But the employer couldn't continue to listen in once the employer made that determination.

Furthermore, my employer deposits my paycheck electronically into my bank, I go onto my computer at work, type in my password into my bank account, make sure that my check was deposited, and verify the account information. If my employer suspects me of theft, does it have the right to go into my bank account? And how about employer access to my medical information?

Finkin: This is an ECPA case and quite a confusing one because the grievant claimed that there was no homosexual material to be viewed on his computer. Therefore, according to his account, there was no violation because nothing was viewed. The employer says that they did view it and the nature of the material disabled him from serving because it was a faith-based organization. To answer your question though, as a question of law, under the Stored Communications Act (SCA), an employer has access to any material stored in its own system. So if you e-mail your doctor and ask about your test results for HIV and the doctor, foolishly or otherwise, e-mails back and says, "I have terrible news for you," that now becomes stored in the employer's system. Under the SCA, the employer and owner of the system has free and unfettered access to any material stored in its system even though it knows the communication to be a personal one.

The French have gone in the opposite direction. In France, once an employer identifies an e-mail as being personal, it may not read and may make no use of any personal information stored in its own system because that is viewed as an invasion of privacy. If our grievant were to rely on the law to protest his dismissal, the arbitrator could draw no sustenance from private law. We are still left with the question of what to do with a lawful retrieval of personal, very sensitive information as evidence in a discharge case?

From the Floor: A key in this case is the rule regarding the use of the employer's computer and e-mail. Recently I had a case involving discipline for use of the e-mail and the contents thereof. However, this employer had an explicit rule for the use of the company e-mail system and its rules prohibited employees from accessing their personal accounts from the company e-mail system. The nature of the rules here would be very important.

Finkin: It is very common for employers today to create rules that restrict the use of the company's computers to company business. The state of Illinois has such a rule. I got a routine message from our electronic resource center reminding us of that

just minutes before our academic vice-president sent me a list of jokes that he thought he ought to bring to my attention. These rules are widely disregarded. E-mail has become the way you communicate and it is understood that no matter what the rules are, people are going to behave with the computer in the same way they do with the telephone. Is a simple violation of the rule enough or do the employer's efforts to enforce its rule matter?

Response: The evidence in the case I had showed that everyone in this work group used e-mail all the time and I sustained the grievance and returned the employee to work with full back pay. Interestingly enough, after the discharge and before the arbitration award, the employer revised its policy and then held an additional training program regarding the use of e-mail that I cited in the award. The employer clearly was uncomfortable with the employees' understanding of its work rules.

From the Floor: The issue in this case is just cause and, depending on how the collective bargaining agreement reads, the reasonableness of the rule. The question we have to ask is: Is it reasonable for an employer to intrude on the private communication of an employee and, if so, to what extent? It is not uncommon for other countries to take an approach to e-mail that mirrors our approach to telephone calls, that is, the employer can look at the e-mail to determine whether it is personal in nature, and that's all! If the employer prohibits the use of the e-mail for personal matters, that is evidence of the employee's wrongdoing. In most countries that have addressed the issue, the employer cannot look at the private communication itself. Because e-mail is an instrumentality that is global in nature, the perceptions of fairness that are beginning to become common throughout the work world should perhaps provide some guidance for us.

From the Floor: I disagree with the comments that it has anything to do with the employer's rule, at least as this question is posited. This case has nothing to do with using the employer's computer system. The question is: Can the employer use my Hotmail? I think the federal law answers that. The employer's right to look stops at the end of its server. If it is on Microsoft's server, they cannot look.

Gerhart: I would agree completely and that's essentially where I came out on the case. There is a possibility that these messages were generated using the employer's computer, and that's troublesome. However, essentially I came down exactly where you did on this case.

I want to say something about two issues that have been raised: first, the fact that the employer was a church and the international perspective. The differences between France and the United States have been mentioned. Some of us may recall that there was a celebrated case somewhere around Paris a few years ago. A Catholic girls elementary school employed a female teacher who had a child out of wedlock. The school decided that this was inappropriate behavior for one of its teachers and did not create the right kind of example for the young women in the school and terminated this woman. The court held differently. The court found that the behavior took place entirely off school grounds and that having the child was totally irrelevant to the teacher's ability to teach and to accomplish the job. Second, except for Australia, the rest of the world is pretty much to the left of the United States on this issue: They respect employee privacy rights to a much higher degree. The country that seems to be most sensitive to employee privacy rights, perhaps because of their experience with the Nazis, is Germany, where there's an intense protection of employee privacy rights vis à vis the employer.

Finkin: The United States, I think, continues to be an "outlyer." As the CEO of Sun Systems said, "right of privacy, get over it, you don't have any" and not just in the workplace. I think today you have to take Australia out of that column. The Australians are moving quite vigorously and in very creative ways. The state of New South Wales—which has the largest population in the country—has established a privacy protection commission and has passed a new law concerning video surveillance in the work place. In order to install a hidden camera in the workplace in New South Wales, the employer has to get a warrant from a magistrate, and has to specify the reason, circumstances, and limits. New South Wales views the power of the employer no differently than we would view the power of government to intrude on your privacy. It's a model that I think is interesting to think about.

Illinois State Department of Motor Vehicles and AFSCME

In September 2000, an employee reported seeing a picture of a naked woman on a co-worker's computer. This led to an investigation and to the eventual discipline of 30 employees. Discipline ranged from a written warning to suspensions of various lengths, plus three discharges. The arbitrator received the appeal of one of the discharges, Mr. Paine. The stated cause for discharge was

accessing adult Web sites in violation of the employer's sexual harassment policy. The Department also had a zero tolerance policy regarding sexual material on its computer systems, which mentioned "discipline, including discharge" as penalties. Paine had attended Internet training and received instruction on the policy.

A second employee who was discharged was a supervisor who distributed sexually oriented material to 23 other employees, including three of her direct subordinates. The third discharged employee was found to have spent much of his working time looking at pornographic Web sites.

Paine neither spent much time looking at pornographic material, compared with others not terminated, nor did he distribute material to other employees. The decision to terminate him was based upon the material he viewed, which included torture and bondage sites. Other discipline involved more conventional pornography.

Bethel: Should a distinction in discipline be based on the kinds of Web sites you view? I have some difficulty understanding the mania that exists about looking at pornography. I understand that if somebody has a pornographic Web site where other employees can see it, it can create a hostile environment. But if you're sitting in your cubicle or in your office looking at a Web site and no one else can see it, I don't see how that matters any more than spending an hour and a half using the employer's computer system to look for the best mortgage rate. Drawing a distinction between the kinds of pornography someone views doesn't seem to me to be a legitimate basis for making a discharge decision. I must admit that personally I probably would be less sympathetic to this grievant if he was looking at child pornography. But child pornography is illegal, as I understand it, and it also involves an illegal act against a child.

However, generally I am not comfortable making a discharge decision or allowing an employer to make a discharge decision on this kind of distinction. This employer has already acknowledged that simply looking at pornographic material at work is not just cause for discharge because he caught 30 employees and only three were fired.

From the Floor: What if you happen to have a small office of three women and three men and a big man is sitting there looking at torture, bondage, rape, murder.

Bethel: And if you've got a computer screen on your forklift truck and go running through the plant, I can understand that. However, but I said if somebody's sitting in his office or his cubicle,

I don't understand why this makes so much difference. I don't mean to suggest that employers can't keep employees from wasting time at work looking at non–work related material on their computer, but if you're in an area where no one else can see what you're doing, I don't see how this is any worse than looking up a mortgage, and presumably this employer wouldn't fire somebody for that.

From the Floor: I would have agreed with you five years ago before I had a case involving output from a printer queue. The material in question was a special area of pornography that I didn't know existed—it was police officer torture snuff porn. After the experience of that case I am no longer willing to say that the nature of the offensive material doesn't make a difference. Maybe it's the degree of hazard—How hazardous is it to another employee to encounter this material?—but I'm no longer willing to embrace the notion that pornography is pornography is pornography.

Finkin: The justifications that employers give to monitor these kinds of communications range from taking time away from work, transmitting secrets or confidential business information, sexual harassment, and down the list. People who are obsessed with pornography don't want the employer to know that and take pains to conceal it. It is rather the advantageous disclosure, leaving the pornographic photograph in the Xerox or, as something that happens or, as in this case, from an investigation that had no particular person targeted at the outset. If you took the pornography out of this case, you would have a very traditional just cause case.

From the Floor: In the public sector we have very strict rules about what you can use your computer for at work but we have also had a case where a professor was training teachers, and was illustrating the output of a Web site mistake—demonstrating to the trainees that if they log on to whitehouse.gov, they get the government, but if they log on to whitehouse.com, they get pornography. One of the students had brought her 5-year-old to the class with her. When asked to access whitehouse.com, she got pornography. She then sued the university because the university: (1) did not tell her she could not bring her child to class; and (2) caused her to put the child in the situation where he had seen this material that she said traumatized him. So whatever you do, you can get sued.

Thompson: On behalf of the audience I first want to thank our three panelists for their stimulating discussion and on behalf of the panel, I would like to thank the members of the audience for your interventions.