NONPROFIT RISK MANAGEMENT CENTER
www.nonprofitrisk.org

Workplace Privacy:
Steering Clear of Danger While Protecting Your Nonprofit

A Risk Management Webinar

August 9, 2006
2:00-3:00 pm, EST

Presented by:
Jennifer Chandler Hauge, Esq., Volunteer

Nonprofit Risk Management Center
1130 17th Street, NW - Suite 210
Washington, DC 20036
(202) 785-3891 - FAX: (202) 833-5747
Web site: www.nonprofitrisk.org

Handout developed by:
Jennifer Chandler Hauge, Esq.
jchandlerhauge@gmail.com

Generous funding to support this Web Seminar was provided by the Public Entity Risk Institute. For more information, visit www.riskinstitute.org.

Workplace Privacy

Is "Big Brother" present in your workplace? To some extent, "he" should be! Unfortunately some workers are not always engaged in the nonprofit's business while they are "at work." There may come a day when your nonprofit has to review criminal history records, or inspect an employee's work station or e-mail account, or request an employee to undergo a drug test. When that day comes, what right does the employee have to claim that his or her privacy is invaded by the nonprofit's search or request?

In this Webinar we will explore the limits of privacy at the workplace:

> What right does an employer have to learn information about an employee or prospective employee that is "private"?
>
> Once the employee is hired, can the employer inspect an employee's work space or is the work space "private"?
>
> What rights do employees have to review their personnel file?
>
> What other workplace issues might be impacted by laws protecting privacy rights?

There are countless issues that are addressed by a host of state laws protecting privacy rights, from laws about keeping social security numbers confidential, to laws about wiretapping and eavesdropping on phone conversations. Each state has its own privacy laws. Additionally, there are a quite a few federal privacy laws that apply in all states.

Here is a link to a good summary of the topics that are addressed by state privacy laws: http://www.epic.org/privacy/consumer/states.html.

Here is a link to a 14-page booklet that summarizes the primary federal and state privacy laws: http://www.bbbonline.org/UnderstandingPrivacy/library/fed_statePrivLaws.pdf.

First: What is the Right to Privacy?

The right to privacy is a "Constitutional right" that is not based on one single law but instead is implied from the Constitutional right not to be subjected to unreasonable searches and seizures. As this body of law has grown and as society has both found more reasons to inquire about personal confidential information, and more ways to probe into dark corners with technology, many different laws have been passed at the federal and state levels that attempt to protect an individual's right to privacy.

The Constitutional Right to Privacy

The Fourth Amendment of the United States Constitution creates a right for an individual's person and property not to be subjected to an "unreasonable search or seizure." Though not explicit in the Constitution, case law has conferred a constitutional right to privacy on all individuals.

Searching a staff member's desk, videotaping staff in action with clients, listening to an employee's voice mail, accessing computer files or requiring an employee to take a drug test

each raises *potential* privacy law issues because all these actions divulge personal confidential information about the employee, perhaps without the employee's consent.

However, court cases have consistently held that in the right conditions, an employee of a private employer (as opposed to the government) *does **not** have a constitutional right to privacy at the workplace.*

Therefore, nonprofits can conduct monitoring activities with a staff member's consent, or even without consent when warranted, especially if the right to inspect or monitor is supported by a *clear written policy*.

STEP ONE: Manage your employees' expectations about their privacy rights.

An employee might have the impression that his computer files, telephone messages, work area, and desk drawers are "private." Consequently, nonprofits should reduce any expectation of privacy at the workplace through a written policy that reminds staff that work areas, including desks, computers, software, and the contents of filing cabinets or storage closets, do not belong to the employee, but are the property of the nonprofit.

1. Have a written policy that gives the nonprofit the right to inspect work areas, electronic and other files, desks, telephone messages, and e-mail messages at the nonprofit's discretion.

Another way to reduce expectations of privacy and maintain the nonprofit's option to search employee work areas is to gain all employees' written consent to searches. If employees have provided written consent, and have been warned not to expect that their desks, work areas, computer files or voice mail are "private," the employer will prevail if the employee raises a legal challenge.

2. Use a form for employees to read and sign, providing their consent to any potentially invasive activity such as: conducting background checks, workplace "audits" of employees' work stations or equipment, (computer and otherwise) and their consent to random drug tests, if applicable.

An employee might have the impression that what s/he does outside of work is no business of the nonprofit and therefore the employee cannot be disciplined or terminated because of conduct outside of work. In fact, certain conduct, such as substance abuse and intimate relationships with co-workers, can have a direct impact on the employee's performance at work, or on the safety of others, or the environment co-workers experience while at work. Consequently, the nonprofit should also retain the right to discipline the employee or terminate the employee based on conduct outside work—EXCEPT where such a step would be contrary to law: e.g., California. (See Webinar materials from July 2006.) This can be done with a general Code of Conduct statement that employees sign, or a Code of Ethics that applies to the entire organization. When conduct outside work impacts the employee's performance at work, the employee must be sure to hold a performance counseling session and reprimand or discipline the employee for the performance failing, as applicable.

3. Have a written policy addressing conduct outside of work. Manage employees' expectations about the fact that their conduct must be consistent with the nonprofit's

values. Consider drafting a "code of conduct" or a Code of Ethics. Counsel and discipline employees appropriately for failing to meet expectations at the workplace.

Some workplaces, such as child care and elder care centers, may use video surveillance for security purposes. Photo images of employees will inevitably be included in the images captured on film. Employees should know about the cameras and their locations, which should not be placed in any location, such as a restroom or locker room, where there is a generally accepted expectation of privacy. A nonprofit's right to videotape staff is strengthened if the cameras are in plain sight and if the taping occurs in areas at the workplace where the staff have no reasonable expectation of privacy. If employees are aware of the cameras, and the nonprofit can validate that their employees were shown the cameras and had their use for security purposes explained to them, there should be no grounds for an employee to later claim that it was an invasion of the employee's privacy rights to be captured on firm.

4. Include a review of surveillance cameras during the orientation for new employees, as applicable.

The constant evolution of technology creates its own challenges relating to violation of privacy. Given the nature of the Internet and e-mail, and how easy it is to access, download, print and transmit information using a variety of electronic and wireless devices, employees are constantly able to view, send and receive nonwork-related communications. Many do so while at work, at times resulting in abusive situations where employees spend more time e-mailing friends and surfing the Internet than drafting a funding proposal. The widespread use of social networking Web sites and the prevalence of blogging will only grow in the future, making it crucial for nonprofits to clarify that personal use of the nonprofit's computers, e-mail and the Internet should be limited.

There may be a time when the nonprofit will have to investigate an employee's use (or abuse) of technology. When that time comes, it will be important for the nonprofit to have the unquestioned right to inspect the employee's computer files.[1] Consequently, employees need to be informed from Day #1 that the nonprofit has the right to monitor employees' computer use. Written policies are the most efficient way to manage employees' expectations in this regard.

Policies on the use of technology should address:

appropriate use of technology, including e-mail and the Internet

the fact that e-mail and computer hard drives are subject to search at any time

[1] Some workplaces have allowed employees to bring in their own computers to use at work, which raises the issue of ownership. Who owns the computer? Has the employee donated it to the nonprofit? Or retained ownership? Unless this question is answered, there can be a real conundrum: is the computer that is used for the work of the nonprofit and used at the worksite of the nonprofit subject to the nonprofit's computer technology policies? (If it is networked with other nonprofit computers it should be.) Regardless, the employee probably has a heightened sense of privacy expectation in a computer that s/he brought to the workplace. This issue is only raised as a red flag. It is up to the nonprofit to resolve the ownership issue before the nonprofit can determine whether its computer use policies apply to that computer.

that employees must provide their passwords to appropriate personnel, such as their supervisor

that posting, accessing, downloading, printing, or transmitting inappropriate, unprofessional, pornographic or obscene information is contrary to the nonprofit's values

that employees are expected to respect copyright and trademark laws, and

that a violation of policy that will subject the employee to discipline, up to and including discharge.

Risks Relating to E-mail and Internet Use

The use of e-mail at work also raises the possibility that an employee will send or receive e-mail tainted with bias, discriminatory or defamatory language, obscene or pornographic material. For this reason it is essential that e-mail policies define inappropriate communications as anything which is not work-related and/or which violates copyright laws or infringes on a trademark.

Personal communications sent internally to another employee via e-mail can result in liability for the employer. In one instance an e-mail communication that was presumably deleted came back to haunt the employer. In that case, one employee sent another a crude, racially biased joke about a co-worker via e-mail, which was deleted by the recipient. However, the employee who was the subject of their humor heard about the joke, and used this fact as evidence of a hostile environment at the workplace in a sexual harassment trial. The plaintiff was able to enter a hard copy of the "deleted" message into evidence at trial, since the employer's computer system had backed it up. The employer was ultimately held responsible for the employee's biased e-mail message. Consequently, although this e-mail was a "private" conversation between two employees, its tone and content was imputed to the employer and resulted in significant liability to the nonprofit. The lesson: employees need to be forewarned that even their private conversations are the business of the nonprofit.

This and other risks underscore how critical it is for nonprofits to use written policies that address expectations for employees when using technology. Other risks relating to the improper use of technology include:

copying software that is licensed to the nonprofit for the employee's personal use (theft or at the very least a violation of license agreements);

using the telephone, facsimile, or e-mail systems for the dissemination or solicitation of information about for-profit ventures, religious beliefs or political causes, or any non job-related business;

uploading or downloading any protected, copyrighted, or proprietary software that does not have a firewall or other security features, which can put the entire nonprofit's computer system at risk for computer viruses;

harassing or intimidating co-workers or third-parties, through the use of the nonprofit's computers.

(A full discussion of technology risks is beyond the scope of this Webinar. However, the Center for Nonprofit Risk Management's publication *Full Speed Ahead: Managing Technology Risk in the Nonprofit World* addresses a wide range of technology-related risks. To order a copy, call:

(202) 785-3891, or visit the Center's Web site to a detailed description of the book and use the online ordering process.)

Basic Risk Management Principles:

1. **Preparation**: Know in advance that the invasion of privacy rights can lead to sticky constitutional challenges to employees' privacy rights. Anticipate that employees will *not* always comport themselves consistently with the employee's values.

2. **Manage Employees' Expectations** about privacy in the workplace.

3. **Documentation:** Consider what written policies will assist the nonprofit if it is ever necessary to discipline or terminate an employee due to conduct outside work, or inappropriate conduct while at work.

4. **Policies:** Nonprofits should consider the value of written policies addressing:
   compliance with copyright laws
   prohibition against viewing and downloading pornographic material from the Internet
   prohibition of the use, sale, distribution or being under the influence of illegal drugs or alcohol while at work
   the obligation to inform the nonprofit about outside work
   permission of outside work as long as it does not conflict with the best interests of the nonprofit, in which case the employee will be asked to either cease the outside work, or resign from employment, or otherwise satisfactorily address the conflict.

5. **Consistency:** Apply the policies consistently, making sure that similar situations result in similar disciplinary actions.

6. **Investigate, don't assume**. Remain receptive to suggestions or shared concerns about the conduct of an employee outside of work, but do not jump to conclusions. Investigate thoroughly, especially allegations of drug or alcohol use, or anything that could be especially damaging to the reputation of the employee.

Big Brother Is Watching (or Listening)

An employee's right to privacy is also impacted when an employer seeks to monitor telephone conversations or voice messages, read e-mails sent or received, or conduct video surveillance.

The federal Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. 2510 et seq., extended traditional privacy principals to a new set of technologies: e-mail, cellular phone calls and paging devices. The ECPA prohibits the interception of electronic communications without the consent of one party to the communication. The majority of state laws also require consent of at least one party to a communication. *However, once a communication has been received and is*

stored (e.g., a voice message or e-mail that has been listened to/read and is still present in a phone or computer) the communication can no longer be "intercepted," so accessing voice messages and reading e-mails that have been received and read is not a violation of law.

In a Virginia case, *United States v. Simmons*, 92 F. Supp. 324 (E.D. Va. 1998), the federal court found that searching the hard drive of an employee's computer for an e-mail message is not an "interception" of an electronic communication that would violate federal law. On the other hand, it was clearly a violation of the Electronic Communications Privacy Act when an employer installed a "voice logger" that monitored telephone conversations of employees 24/7. *Sanders v. Robert Bausch Corp*., 38 F. 3rd 736 (4th Cir 1994).

An employee's (and client's) consent to monitoring will remove the federal and state law obstacles that regulate interception of electronic communications. Many nonprofits, such as child care centers and nonprofits offering telephone hotlines, routinely monitor employees' conduct with surveillance videotapes or by taping hotline conversations. These nonprofits in particular should obtain employees' (and clients') consent and have written policies to notify staff of monitoring activities. Nonprofits offering hotline services would be well advised to put a message on the telephone service such as: "for your protection and to enable [Name of Nonprofit] to monitor quality of service, this conversation may be recorded." The general rule is that if one party to the communication is aware of or has consented to the interception, then there is no invasion of privacy. However, several states have laws that completely *prohibit* an employer from "eavesdropping" on employee conversations or that require *all parties* to a conversation to provide consent.

Examples:
California: No person other than an authorized law enforcement officer may wiretap or eavesdrop on confidential communications. Cal. Penal Code Sections 631, 632 and 636.
Georgia: Requires consent of all parties prior to wiretapping or eavesdropping on conversations. O.C.G.A. Sections 16-11-61 and 16-11-62.
Illinois: The Illinois Eavesdropping Act makes it unlawful to knowingly intercept in person, by telephone or electronically, another person's conversations, regardless of whether one or more of the parties is aware of the eavesdropping. 720 ILCS 5/14-1 et seq.
Louisiana: The Louisiana Electronic Surveillance Act makes it unlawful to intercept or try to intercept or procure someone to intercept any wire or oral communication. La. Rev. Stat. Ann. Section 15-1301 et seq.
Michigan: Consent of all parties is required. MCL 750.539c and 750.539d
Minnesota: State law prohibits intentionally intercepting any wire, electronic or oral communication and using any device to intercept oral communication; Employers may use video surveillance, but cameras that record sounds are restricted under the wiretapping statutes. M.S.A. Section 626A.02.
Montana: Requires the knowledge of all parties to a conversation. Mont. Code Ann. Section 45-8-213.
Nevada: Requires consent of all parties. Nev. Rev. Stat. 200.620.
New Hampshire: Requires consent of all parties. N.H. Rev. Stat. Ann. 570-A-2.
Pennsylvania: Intentionally intercepting a wire, electronic transmission or telephone call is prohibited. 18 Pa. C.S. Sections 5701 et seq.

Washington: Requires consent of all parties. Wash. Rev. Code Section 9.73.030.

⇒ Two states, **Massachusetts** and **New Jersey**, have a business necessity exception that permits employers to use telephone recording devices in the course of business where there is a legitimate business reason to do so.

Information That Is Deemed Confidential

Proprietary information (such as donor lists) and private, confidential information about clients and employees must be kept secure in order to protect against violations of privacy as well as violations of federal and state laws that govern the disclosure of personal, confidential information. Electronic transmission raises challenges to maintaining confidentiality that merits thoughtful discussion among staff, and may require the nonprofit to customize internal operating procedures to maintain client and employee confidentiality. Nonprofits with social workers and medical health professionals on staff need to be aware of special ethical obligations relating to maintaining confidentiality that mental health and healthcare professionals must observe in order to avoid liability for malpractice or the loss of professional licenses.

Because of the nature of their work, nonprofits may have obligations to maintain confidential communications stemming from funding sources or contracts with government agencies to provide specialized services. Many nonprofits with state funding from disability and human services agencies will find that they are required to have extensive policies and practices to protect the confidentiality of personal health information about clients because they are "business associates" under the Health Information Portability and Accountability Act (HIPAA) P.L. 104-191 (1996), http://aspe.hhs.gov/admnsimp/pl104191.htm. Business Associates must protect the privacy of certain identifying health information in the same manner as covered entities under HIPAA. A sample business associate contract is provided by the Department of Health and Human Services on its Web site: www.hhs.gov/ocr/hipaa/contractprov.html. Employees who regularly work with the types of information that are protected from disclosure, or with clients whose personal information the nonprofit maintains, should be well versed in the nonprofit's obligations, so that violation of privacy rules does not occur. Employees should also know that due to the seriousness of privacy rules and the need to be respectful of client's confidential information, violation of the nonprofit's confidentiality policies is a serious offense, with consequences including termination of employment.

In general, HIPAA does not apply to employment records, however, some nonprofits are themselves covered entity's under HIPAA, and thus required to have various privacy policies in place in accordance with federal law. The Department of Health and Human Services has a decision tree tool on its website to assist organizations determine whether they are a "covered entity" under HIPAA: www.cms.hhs.gov/apps/hipaa2decisionsupport/default.asp. If your nonprofit electronically transmits health protected information about clients, HIPAA may require that the nonprofit implement a privacy policy and authorization procedures to clarify how and when a client authorizes disclosure of protected health information. Check with an attorney knowledgeable about HIPAA compliance to determine if and how your nonprofit should implement policies and procedures to comply with HIPAA

Personnel Files

One of the areas where employees typically have an expectation of privacy is in their own personnel files. Personnel files contain personal information that employees expect to be kept confidential. The nonprofit should develop a clear policy defining when and how employees may have access to their files. Conventional wisdom tells us that what is contained in an employee's file should not be a secret from the employee, so it does not make sense to prohibit an employee from reviewing his/her file. However, it would not be prudent to permit employees free access to their files, just as it would not be appropriate for anyone to have free access to any of the many other business records of the nonprofit. It also does not make sense to permit an employee to take the contents of the file home, or even to the copier machine or the employee's work station because of the risk of inadvertently violating the employee's confidentiality or losing the contents of the file. An employee who is reviewing a personnel file should do so in a controlled environment, with his or her supervisor or the human resource manager present to ensure that the file is kept intact. If the employer has done a good job documenting the employee's performance, nothing in the file should be a surprise to the employee.

A minority of state laws require an employer to give an employee access to personnel files and to provide the employee with a copy of the file. Absent a statutory right to access personnel files, employers are free to determine their own policies. As with all policies at the workplace, care should be taken to implement the personnel file policy consistently, ensuring that all employees are treated equally with respect to access to their files.

Drug Testing and Suspected Drug Abuse

It is always a challenge to know what to do when an employee is suspected of drug abuse. One option is to demand that the employee take a drug test on the spot. There are practical and legal problems with this approach. A safer option is to treat the suspected drug use as a performance issue and discipline the employee based on performance failings, rather than suspected drug use. Nevertheless, there are times when knowing for certain whether an employee is abusing drugs or alcohol is best. In those cases, suspending the employee and requiring the employee to be tested for substance abuse prior to making a determination whether the employee should return to work is the prudent practice.

NOTE!

Random drug testing is mandatory for employees with commercial drivers' licenses:

The federal Omnibus Transportation Employees Testing Act of 1991, 49 C.F.R Section 382 (1994), requires employers to randomly test employees who drive vehicles and hold commercial drivers licenses (CDLs) on a periodic basis. Random testing is required because driving is considered a "safety sensitive" position. Since most nonprofits only have a few employees who hold CDLs, many nonprofits have joined with other organizations to form a cooperative testing collaboration, resulting in less expensive testing.

The Drug-Free Workplace Act of 1988, U.S. Code Title 41, Section 701 et seq., www.law.cornell.edu/uscode/html/uscode41/usc_sec_41_00000701----000-.html, requires *some* federal contractors and grantees (those receiving 25K+ in federal funding) to agree that they will provide drug-free workplaces as a condition of receiving a contract or grant from a federal agency. Failure to adhere to the requirements of the act may cause the nonprofit to lose the federal contract or grant and/or be unable to qualify for federal funding in the future.

The Drug Free Workplace Act requires a covered nonprofit to:

Publish a statement (written policy) notifying employees that the unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance is prohibited in the person's workplace. The statement should also notify employees of any punitive actions that will be taken. There is also a posting requirement.
Establish a Drug-Free awareness program to inform employees about
(i) the dangers of drug abuse in the workplace;
(ii) the policy of maintaining a drug-free workplace;
(iii) any available drug counseling, rehabilitation, and employee assistance programs; and
(iv) the penalties that may be imposed upon employees for drug abuse violations.
Make it a requirement that each employee be given a copy of the workplace substance abuse policy.

Under the act, employees are required to inform their employer of any drug-related criminal conviction or sentencing within five days. The act does not *require* drug testing.

⇒ **Is your nonprofit covered by the Drug Free Workplace Act?**

- √ Does the nonprofit have a federal grant?
- √ Does the nonprofit have a federal contract valued at $25,000 or more?
- √ Does the nonprofit have any subcontracts that include a drug-free workplace requirement?
- √ Is the nonprofit subject to any federal agency regulations, such as those of the Department of Education, HUD, or the Department of Health and Human Services?

If you answered "yes" to any of these questions, your nonprofit should develop a policy that adheres to the requirements of the Drug Free Workplace Act. Even if your nonprofit is not required to comply with the act, the act provides guidelines for developing a drug-free workplace policy.

Drug Testing

Requiring an employee to take a drug test is a risky issue unless the state law where the nonprofit is located has provided specifically that private employers may require employees to take a drug test. A drug test is often considered a violation of constitutional privacy rights, because it is akin to a search of the body. To justify a drug test, a nonprofit must be very certain that there is either a supportive state law, or a strong suspicion of illegal substance use *combined* with a risk to human safety. Even with strong support in the state's law or with factual evidence, there are practical difficulties with drug testing due to false negative and false positive tests.

Consequently, most employment lawyers advise clients to treat suspected drug or alcohol use as a performance issue, and to discipline employees on that basis. In many states, if suspected substance abuse results in an accident or injury at the workplace, the employer is on stronger grounds to require a drug or alcohol test as a condition of continued employment. In other states, having a "reasonable suspicion" of drug use is sufficient to require an employee to undergo a test. It is important to know what the state law or court cases in your state have decreed with respect to drug testing.

Many states permit testing but only if the employer has a written policy in place ahead of time to notify employees about testing procedures. In some states, employers with comprehensive written policies may be eligible for discounts on workers compensation insurance premiums.

Even assuming constitutional issues are obviated by obtaining an employee's written consent to a drug test, there are practical issues relating to the reliability of testing and what do to with the results. What will the nonprofit do if the employee tests positive? What if the test results return a "false positive" or a "false negative?" Does the nonprofit have a reliable testing service which preserves the chain of custody of the sample so that the validity of the results will not be challenged? How will the confidentiality of test results be maintained? These and other issues have caused many employers to move gingerly into the realm of drug testing.

Since the federal ADA protects recovering drug abusers and alcoholics, even if the nonprofit were to find that an employee tested positive for illegal substances, there is a good chance that the nonprofit would be obligated to accommodate the employee rather than fire him or refuse to hire him. The bottom line is: What policy is going to result in the least harm, and the least risk? Most nonprofits err on the side of caution: After confirming that their director's and officer's liability insurance policy covers employment law claims, they prefer to face the risk of a lawsuit for wrongful discharge or failure to hire, than the aftermath of employee misconduct as a result of substance abuse.

Additional Background

Laws that address an employee's right to privacy include:

1. The United States Constitution (The First and Fourth Amendments apply to all persons, granting the right to free speech and protection from unreasonable searches and seizures. Together, they have been interpreted as granting a constitutional Right to Privacy.) The Right to Privacy, while not explicitly articulated in the Constitution, has been inferred and judicially created through case law, most notably, *Roe v Wade* (granting a woman the right to make choices about terminating her own pregnancy), and *Griswold v. Connecticut* (holding that a state law banning the use of contraceptives is unconstitutional as an invasion of a married couple's right to privacy).

- Court cases have consistently held that in the right conditions, a private employee does ***not*** have a right to privacy at the workplace. ***But***, legislation has carved out areas where employees' privacy rights must be respected by the employer.

The Right to Privacy broadly impacts the following:

Background checking—criminal background history checks
Consumer credit checks
Drug testing at the workplace
Video surveillance at the workplace
Use of computers, e-mail, blogging, voice mail and other technology
Outside work—employees working two jobs

2. **Individual States' Constitutions** create a constitutional claim that an individual's state constitutional rights were violated.

3. **Federal Laws That Govern Consumer Credit Reports:**

The Federal Consumer Credit Reporting Act (FCCRA): The Fair Consumer Credit Reporting Act, 15 U.S.C. § 1681 et seq. ("FCCRA"), http://www.ftc.gov/os/statutes/fcra.htm, and the fair consumer credit reporting laws of some states, require employers to obtain written authorization for background checks and to provide written notice when an employer uses outside sources, such as credit bureaus, to collect background information on applicants or employees.

❑ The FCCRA requires employers to put applicants on notice that a consumer report will be sought and used to evaluate qualifications for employment. If an employer uses the report on an applicant or employee's background (whether educational history, driving records, employment, credit history, or criminal history) to make a decision resulting in an adverse employment action (such as disqualifying an applicant or terminating an employee) the employer must inform the applicant of this fact in writing, and provide the applicant or employee with a copy of the report.

❑ The Web site of the Federal Trade Commission (FTC), www.ftc.gov/bcp/conline/pubs/buspubs/credempl.htm, provides an outline of the requirements for employers to follow when using outside consumer credit agency reports.

4. **Federal and State Laws Governing Criminal History Background Checks:**

Can an employer have access to conviction records? (Usually, sometimes it's mandated.) Arrest records? (Usually not.)

In April 2006 the EEOC issued guidelines about race and sex discrimination that specifically address whether it is permissible for employers to ask about and consider past criminal activity during recruitment. [See EEOC Compliance Manual No. 915.003, issued 4/19/06, www.eeoc.gov/types/race.html. The position of the federal government is that an employer may not exclude applicants based on arrests that do not lead to conviction unless there is a business justification (defined as both job-related and fairly recent.) A business justification can rarely be demonstrated for across-the-board exclusions on the basis of *arrest* records.

State Laws: Before deciding whether to conduct criminal record checks on applicants or employees, know your state law! Many states have laws that *mandate* pre-hire criminal record checks for certain categories of employees, (e.g., home health care workers and child care workers) resulting in applicants or employees with a prior conviction will not be eligible for employment.

⇒ In most other situations it is possible to gain information about prior criminal convictions, but it is *safest to always get written authorization from the employee to conduct the criminal history record check*.

State specific information on the laws that govern access to conviction and arrest records is beyond the scope of this Webinar. For more information about the laws that govern background record checking in your state, please contact the Nonprofit Risk Management Center.

5. Federal Laws Governing Drug and Alcohol Use at the Workplace.

The Drug-Free Workplace Act of 1988, U.S. Code Title 41, Section 701 et seq., www.law.cornell.edu/uscode/html/uscode41/usc_sec_41_00000701----000-.html
The Drug-Free Workplace Act of 1988 requires *some* federal contractors and grantees (those receiving 25K+ in federal funding) to agree that they will provide drug-free workplaces as a condition of receiving a contract or grant from a federal agency. Failure to adhere to the requirements of the act may cause the nonprofit to lose the federal contract or grant and/or be unable to qualify for federal funding in the future.

The Drug Free Workplace Act requires a covered nonprofit to:

Publish a statement (written policy) notifying employees that the unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance is prohibited in the person's workplace. The statement should also notify employees of any punitive actions that will be taken. There is also a posting requirement.
Establish a Drug-Free awareness program to inform employees about
(i) the dangers of drug abuse in the workplace;
(ii) the policy of maintaining a drug-free workplace;
(iii) any available drug counseling, rehabilitation, and employee assistance programs; and
(iv) and the penalties that may be imposed upon employees for drug abuse violations.
Make it a requirement that each employee be given a copy of the workplace substance abuse policy.

6. State Laws that Limit Drug/Alcohol Testing: Only five individual state's laws specifically restrict or limit an employer's right to test an employee for alcohol or drug use. Example: Minnesota provides that employers may request or require employees to undergo drug/alcohol testing as part of a routine physical examination provided the test is requested or required no more than once a year and employees are given two weeks notice. Employers can also require employees to undergo testing if they have reasonable suspicion that an employee is under the influence of drugs or alcohol; Random testing is only permitted if the employee is in a safety-sensitive job. Minn. Stat. Ann. 181.950 et seq.

Meanwhile, 13 states have laws ***permitting drug-testing*** with some limitations: Florida, Georgia, South Carolina, Alabama, Mississippi, Louisiana, Tennessee, Arkansas, Ohio, Arizona, Utah, Idaho and Iowa.

- The remaining states have no specific statute that addresses an employer's right to require drug tests as a term or condition of employment, leaving open the possibility that an employee could exert a constitutional claim that being forced to submit to a drug test at the work place is unconstitutional.

7. Federal Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. 2510 et seq., http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002510----000-.html. The ECPA extended traditional privacy principals to a new set of technologies: e-mail, cellular phone calls, and paging devices. The ECPA prohibits the interception of electronic communications, without the consent of one party to the communication. However, once the communication has been received and is stored (e.g., e-mail that has been read and is still present in a computer) the communication can no longer be "intercepted," so accessing and reading that e-mail is not a violation of the law.

- A Virginia case is instructive: The court found that searching the hard drive of an employee's computer for an e-mail message is not an interception of an electronic communication within the meaning of the ECPA. *United States v. Simmons*, 92 F. Supp. 324 (E.D. Va 1998).
- On the other hand, it was clearly a violation of the ECPA when an employer installed a "voice logger" that monitored telephone conversations of employees 24/7. *Sanders v. Robert Bausch Corp*. 38 F. 3rd 736 (4th Cir 1994).

8. State Privacy Laws re: Monitoring or Recording of Conversations/Phone Calls
The general rule is: If one party to the communication is aware of or has consented to the interception, then there is no invasion of privacy. However, several states have laws that completely prohibit an employer from "eavesdropping" on employee conversations or that require all parties to a conversation to provide consent.

Examples:
California: No person other than an authorized law enforcement officer may wiretap or eavesdrop on confidential communications.
Georgia: It is unlawful for any person, through use of any device, without the consent of all persons observed, to observe, photograph, or record another in a private place.
Illinois: It is a violation of the Illinois Eavesdropping Act to knowingly intercept in person, by telephone or electronically, another person's conversations, regardless of whether one or more of the parties is aware of the eavesdropping.
Pennsylvania: Intentionally intercepting a wire, electronic transmission or telephone call is prohibited.
New Hampshire: It is a felony to intercept communications without the consent of *all* parties.

⇒ In contrast, in **New Jersey**, the state law contains an exception for employers to use telephone recording devices in the course of business to protect the "employer's rights or property"

⇒ Most state privacy laws do not specifically address electronic surveillance, (only interceptions of calls/wiretapping), but employees could state a claim of violation of privacy rights by showing that they had a reasonable expectation of privacy that the employer's surveillance violated.

9. Tort Law: Invasion of Privacy and "intrusion upon the seclusion of another." To determine whether there has been an "intrusion upon the seclusion of another," the courts look to whether the injured person had an "*expectation of privacy*" that was violated. Example: An employee has a legitimate expectation that s/he will not be videotaped in a restroom; but a child care worker who is aware that the day care center regularly uses video surveillance for security purposes, has no expectation of privacy in areas of the building where the cameras are visibly placed.