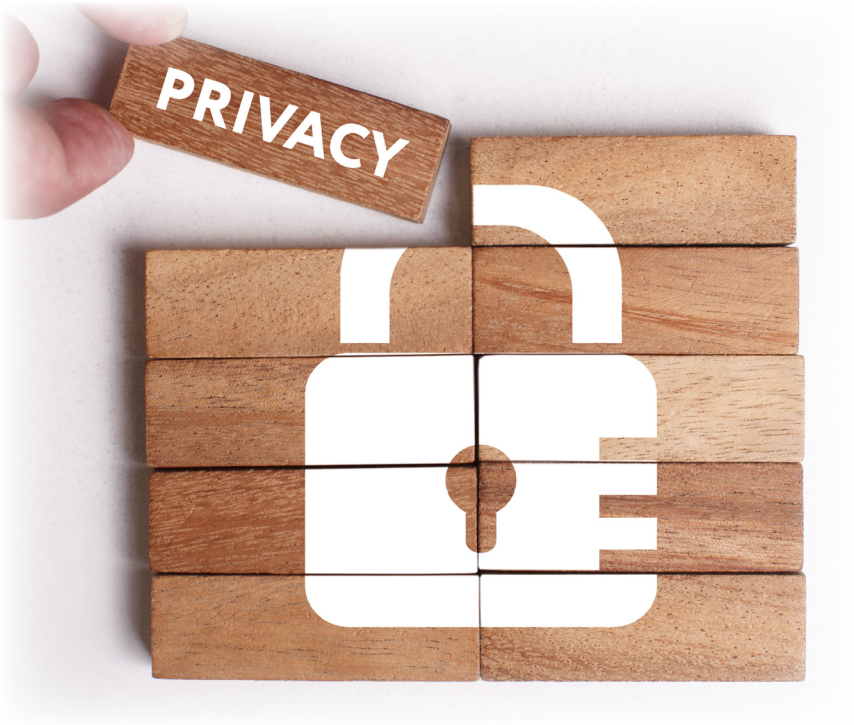
PRIVACY IN EMPLOYMENT HANDBOOK



CSEA

LOCAL 1000 AFSCME, AFL-CIO
143 Washington Avenue
Albany, New York 12210

MARY E. SULLIVAN, PRESIDENT

TABLE OF CONTENTS

INTRODUCTION

The issues surrounding workers' rights to privacy have emerged as some of the most important issues in labor relations today. Employers seek greater control over the behavior of employees in the workplace. Due to the use of email and social media many things that employees used to say to one another privately are now publicized via the internet. This, of course, can present problems if the communication is deemed by the employer to be inappropriate and work-related.

Also, employers collect a significant amount of information about their employees – from the very personal to the innocuous. How this information is safeguarded and used becomes a concern of every employee.

An employee's workspace many times is a very personal environment with family photos, personal effects and the place where certain personal documents and items may be retained on a permanent basis, or for only a very short time. Whether this space can be searched by an employer is another issue that encroaches on ones expectations of privacy. These and others are some of the issues that will be touched upon in this booklet.

When it comes to workplace privacy there are several questions to consider:

- Are you entitled to privacy in the workplace and in all matters related to your employment?
- If so, what type of privacy, and to what extent?
- What type of information does your employer have a right to obtain about you?
- Does the employer have the absolute right to control all your on-the-job activities?
- Is the employer required to negotiate with your union about matters affecting your privacy?
- Does the employer have certain rights in monitoring or controlling your off-the-job activities?
- Does the employer have a right to disclose any of the information that it has about you to third parties?

Where to find answers

The right to privacy is not governed by any one comprehensive law. Privacy rights are formulated out of various constitutional provisions, laws, regulations, and rulings. These rights are not nearly as broad as many believe them to be. This is especially true in the employment context, where employers – both public and private – have the authority, in certain circumstances, to infringe upon this "right to privacy."

It is not the intention of this booklet to be a final and definitive guide to these privacy questions. Therefore, when confronted with any privacy issue requiring legal assistance, please contact your Labor Relations Specialist or the Legal Department.

PUBLIC SECTOR WORKPLACE

First Amendment

The First Amendment to the U.S. Constitution generally protects freedom of speech, but this is not an absolute rule in the employment context and it only applies in the public sector.

As a result of several U.S. Supreme Court decisions, it is now generally accepted that public employee speech must satisfy three criteria before First Amendment protections apply:

(1) The speech must relate to a matter of public concern.

(2) The employee's speech must fall *outside* of job duties.

(3) The employee's interest in free expression must outweigh the government's interest in the efficient and effective provision of services.

This final provision is a balancing test that considers when, where, and how the speech was made. This becomes especially important when an employee is involved with policy issues; it makes it more likely that the government's interests in controlling that employee's speech will prevail. For example, when higher level government employees make statements that contradict official government policy, First Amendment protection is almost non-existent.

The First Amendment to the Constitution protects freedom of association, as well as freedom of speech. However, this right can be limited – to a degree – in the employment context. For example, one federal court has held that prison guards' rights to association can be limited with respect to their association with ex-convicts. In contrast, a federal court has ruled that public employees have a right to maintain a marital relationship free

from undue employer interference. In the latter case, the husband alleged he was fired because his wife had previously sued the state for wrongful termination.

The U.S. Supreme Court has determined that promotions, transfers, and recall of employees could not be based on political affiliation, as long as the employee is not in a position of policy-making power or partisan political work.

It should be noted that some courts have recognized that the First Amendment freedom of speech and freedom of association protect union membership. Therefore, the First Amendment may be implicated if a public employer takes action against an employee based on his/her union membership,.

Fourth Amendment

The Fourth Amendment to the U.S. Constitution governs the ability of a public sector employer to intercept employee communications, search offices and belongings, and track employees' movements. It generally prohibits unreasonable search and seizures by the government, including public employers. The standard for determining whether there is a Fourth Amendment right in the context of public employment is whether the employee has a "legitimate expectation of privacy" and if so, whether that privacy interest outweighs the public employer's need for the interception.

In 2010, the U.S. Supreme Court held in City of Ontario, Cal. v. Quon that although a city police officer had a reasonable expectation of privacy in text messages sent on a city-owned pager, the city's search and review of the text messages was, nevertheless, reasonable and thus did not violate either the Stored Communications Act or the defendant's Fourth Amendment rights.

PRIVATE SECTOR WORKPLACE

Constitutional protections such as the First Amendment freedoms of speech and association and the Fourth Amendment right against search and seizure apply only to government action. Unlike the public sector, private sector employers are not government entities and therefore their employees are not entitled to those rights in the workplace. In fact, private sector employees' speech is not protected from retaliation by their employer unless there is some contractual or statutory (e.g. Legal Activities Law, etc.) protection.

The National Labor Relations Act (NLRA) protects employees' rights to engage in protected communications about their employment, including discussions of wages or other terms and conditions of employment with co-workers, unions or the government. Workplace rules that temper these employee rights under the NLRA are unlawful.

It should be clear that employers have broad legal authority to access their employees' electronic communications, including e-mail messages and telephone conversations.

Additionally, employers can limit the content of messages and downloaded material. Employer policies in this regard may include notice to employees that the e-mail system is for business purposes only and that vulgar, derogatory, or harassing messages are prohibited. Such guidelines may constitute what an employer deems appropriate behavior.

SEARCHES AND SURVEILLANCE

Searches

New York does not recognize a right to privacy in the employment context. As a result, an employee can't claim such a right when his or her employer retrieves an employee's electronic communication records for just cause.

The first issue that must be addressed when a public employer performs a search is whether the employee has a legitimate expectation of privacy. If the employer issues policies or notices to the employee stating that they have no expectation of privacy in their desks, file cabinets, computers, telephones, etc., or that these items are subject to search, then no legitimate expectation of privacy exists.

> **Even if a public employee has an expectation of privacy at his/her office, desk, or file cabinets, the U.S. Supreme Court has held that they can be searched if the public employer had reasonable cause – as opposed to the higher criminal law standard of probable cause – to search for purposes of supervision and control, and the efficient operation of the workplace.**

This standard can be satisfied by meeting one of two prongs:

- The search is a non-investigatory, work-related intrusion (e.g. looking for work-related materials in an employee's desk), or
- The search is an investigation of employee malfeasance or misconduct.

The search must be reasonable in scope. In other words, the public employer may not search areas that could not contain what it is searching for. For example, if an employer is looking for an email about an event that occurred two months ago, it cannot look at emails that are a year old.

In the context of arbitration, when determining whether an employer has violated a collective bargaining agreement by engaging in a search, the question for the arbitrator is whether the search was reasonable under the relevant circumstances. For example, a reasonable search of employee purses, briefcases, or lockers could be conducted in

circumstances where management has had problems with thefts or other serious issues. An employer may reserve the right to make random searches in such instances.

Surveillance

Employee surveillance may implicate both First and Fourth Amendment rights. In addition, the National Labor Relations Act and the Taylor Law protect employees from being placed under surveillance – electronic or otherwise – by their employer under certain circumstances.

In a 2008 Public Employment Relations Board ("PERB") case, an Administrative Law Judge ("ALJ") dismissed a union's improper practice charge regarding a county's installation of a global positioning system (GPS) in County vehicles operated by public works department employees. The union argued that the installation of the system violated the county's duty to bargain and unlawfully subjected unit members to surveillance. However, the Judge concluded the utilization of the GPS technology was a management prerogative because it related to the "manner and means by which an employer is providing services to the public."

Also, the installation of GPS technology in village-owned vehicles enabled the village to monitor a vehicle's location and its occupants in real time, and monitor how fast the vehicle was moving. The GPS also enabled the village to generate reports of the vehicle's whereabouts on a particular date going back 12 months, and set up e-mail notification alerts regarding any GPS-equipped vehicle. The Judge noted that the scope of the impact of the information, as well as any implications arising from it, could be addressed within the context of impact bargaining.

The National Labor Relations Board ("NLRB") has found that the installation and use of surveillance cameras in the work place are not among the class of managerial decisions that lie at the core of entrepreneurial control. The NLRB concluded that the use of surveillance cameras was a change in the employer's methods used to reduce workplace theft or detect other suspected employee misconduct with serious implications for its employees' job security, which in no way touches on the discretionary "core of entrepreneurial control." As such, the NLRB found the use of surveillance cameras to be mandatorily negotiable.

A **PERB** ALJ followed this NLRB ruling in finding for CSEA in a 2011 ruling, holding that the installation of the cameras constituted a new work rule that was a mandatory subject of bargaining. The ALJ also found that usage of the video cameras to monitor employee performance and behavior implicated employee job security because the cameras provided an enhanced investigatory tool to determine employee misconduct, and as such, employee discipline was a stated consequence of such monitoring.

In 2012, the U.S. Supreme Court held in *U.S. v. Jones* that law enforcement's use of GPS surveillance was an illegal search because the attachment of the device to the car was a physical trespass on the owner's personal property. This is a key distinction

because the court did not hold that the electronic monitoring of a person's movement is an unconstitutional invasion of that person's constitutionally protected privacy, even when it is conducted over an extended period of time.

In 2013, the New York Court of Appeals ruled in *Cunningham v. New York State Department of Labor* that the Fourth Amendment and the State Constitution's protection against unreasonable searches was violated when a public employer conducted secret GPS surveillance of an employee's private vehicle over the course of a month, without first obtaining a warrant, because the search was not reasonable in its scope. The Court took issue with tracking the employee on nights, weekends, and during a vacation. However, the Court did not find that the GPS surveillance itself was a violation, holding that when an employee chooses to use his personal vehicle for work purposes, GPS tracking is considered a workplace search.

Drug Testing

Federal regulations under the Omnibus Transportation Employee Testing Act ("OTETA") require employees who operate commercial motor vehicles for the performance of their duties to be subject to drug and alcohol testing. These regulations require pre-employment testing, post-accident testing, random testing, reasonable suspicion testing, return to duty testing, and follow-up testing. A determination of reasonable suspicion must be made by a trained supervisor based on specific, contemporaneous, describable observations concerning the appearance, behavior, speech, or body odors of the driver, and may include indications of the chronic and withdrawal effects of controlled substances.

In 2005, New York State's Third Department of the Appellate Division held that a private employer's request that an employee submit to a drug test is reasonable if the employer had a reasonable belief that the employee was under the influence of drugs during his shift. Another court has struck down a provision requiring the random drug testing of teachers.

It is CSEA's position that for employees who are not covered by federal regulations, drug and alcohol testing is a subject which an employer must negotiate. We have often negotiated "reasonable cause-based policies" upon an employer's demand. However, in many situations such a demand could be deemed an unreasonable search and seizure under the U.S. Constitution and a union cannot be required to waive its members' constitutional rights. In certain instances, the analysis could be different if an employer had compelling safety reasons to justify random testing.

Polygraph or Lie Detector Tests

Public employees are exempt from the federal Employee Polygraph Protection Act of 1988 (EPPA), which prohibits the use of any type of lie detector test by most private sector employers. Private employers are generally prohibited from requiring or requesting that any employee or job applicant take a lie detector test, as well as

discharging, disciplining, or discriminating against an employee or prospective employee for refusing to take such a test. A lie detector test may be permitted, however, if an employee is reasonably suspected of involvement in a workplace incident that resulted in economic loss to the employer.

Except for the use of psychological stress evaluators, which are specifically prohibited from being used under New York law, public employees must assert a constitutional privilege to not be subjected to a polygraph examination. Where a collective bargaining agreement exists, employees should grieve the use of polygraph examinations as a violation of the contract if the contract does not explicitly permit such examinations. The use of polygraph examination by a public employer is a mandatory subject of bargaining under the Taylor Law. However, if the investigation is being conducted by a police agency in relation to a crime, the Taylor Law has no applicability.

EMAIL, VOICEMAIL, AND OTHER ELECTRONIC COMMUNICATIONS

Background

Many employers monitor employee internet connections and e-mail usage. Though it is unclear whether a specific CSEA member employer does so, members should understand the possibility that their electronic communications are monitored.

Legal Application

Foremost, there is no expectation of privacy over communications once they are sent to and received by another person. If the recipient chooses to share the email, text message, or voicemail with others there is no violation of the sender's privacy rights.

The Electronic Communications Privacy Act (ECPA), a federal provision, generally prohibits the intentional interception of most telephone, e-mail, or other electronic communications. However, two broad exceptions to this rule permit employers to monitor the electronic communications of their employees at work.

The first exception allows employer interception of employee electronic communication in the following two circumstances:

> (1) Where the person intercepting the communication is a party to the communication and,
>
> (2) Where one of the parties to the communication has consented to its interception.

"Consent," in this regard, may be express or implied. For example, express consent could be obtained through the signing of an electronic consent form that includes a provision allowing for employer interception of workplace electronic communication. Implied consent could be provided, for example, in the instance of an employee using a

work computer after being advised that such usage is evidence of consent to their communications being monitored. However, the mere knowledge that an employer's system is capable of intercepting telephone messages does not constitute consent.

The second exception allows employers to intercept employees' electronic communications if the employer has a legitimate business-related reason to do so. For example, an employer can intercept communications to prevent breaches of confidentiality, prevent trade secret theft, investigate employee misconduct, or to conduct system maintenance. Additionally, employers may monitor communications with respect to monitoring the quality of services being provided. This rationale should not apply to an employee's personal calls, assuming such personal calls are otherwise permitted.

The Stored Wire and Electronic Communications and Transactional Records Access Act (SWECTRAA) prohibits access of certain stored electronic communications. However, exemptions permit employers to access certain electronic communications, such as stored e-mail messages and voicemail. Also, like the ECPA, employee consent to employer access to stored electronic communications may be express or implied. SWECTRAA exempts conduct authorized by the person or entity providing the electronic communication service, which in most employment cases will be the employer.

The Society for Human Resources Management (SHRM) encourages employers to issue an electronic communications policy. SHRM recommends that any such policy address employee privacy and notification of equipment use guidelines. The organization also encourages employers to obtain express consent from the employee through signed statements acknowledging receipt of the rules and that the communications may be monitored. You should know your employer's policy.

In regard to whether an employee's electronic communication contributes to a hostile work environment, the standard is the same as face-to-face communication: the speech must be so pervasive as to negatively alter working conditions. For example, a single display of a pornographic picture, or an email containing an ethnic or sexual joke that was sent to a limited number of people, may not fall into this context.

Disciplinary Arbitration

Disciplinary arbitrators review employee electronic communication on a case by case basis, but apply standards consistent with those stated elsewhere in this publication.

PERB Standards for Public Sector Union Communications

In a 2008 PERB case between the New York State Correctional Officers and Police Benevolent Association and the NYS Department of Corrections, an ALJ held that a correctional officer's e-mail alerting co-workers that time spent working on Election Day should be claimed as premium holiday pay under their collective bargaining

agreement was protected speech. The ALJ found that the e-mail was conveyed in the employee's capacity as a union officer and the communication expressed the officer's belief as to what was permitted under the bargaining agreement. The ALJ also noted that the communication did not lose its protection merely because it encouraged employees to go to work as a protest against certain reporting requirements. Thus, the ALJ held it would be improper to discipline the employee at issue for sending such an electronic communication.

NLRB Standards for Private Sector Union Activity

The NLRB has held that an employer cannot discriminate against the use of electronic communications for union activity if it permits the use of electronic equipment for other non-business related communications, like a solicitation for raffle tickets. The NLRB has also advised that an employer's prohibition of all non-business use of e-mail, including permitted union-organizing messages, is overbroad and unlawful on its face. Further, in *Purple Communications*, the NLRB found that employees who have been given access to their employer's email system for work-related purposes have a presumptive right to use that system for protected communications on nonworking time, unless the employer can demonstrate that special circumstances necessitate a restriction. However, due to the political nature of the NLRB, it may reverse the decision in *Purple Communications*.

SOCIAL NETWORKING

"Good rule of thumb, don't post anything on the Internet that you might regret later."

- Aljolynn Sperber, Marketing Maven Public Relations

There is no expectation of privacy in postings on social media where privacy settings are not used. If anyone can view an employee's postings then they can be used by the employer. Even when privacy settings are set so that only approved "friends" or "followers" can view postings, there are no privacy implications if a "friend" or "follower" chooses to share the posting with the employer.

Employers have been issuing policies that intend to suppress the use of social networking in manners that limit employees' discussion of their job or criticism of the employer. These restrictions can impact the ability of employees to discuss terms and conditions of employment or problems they are having with their employer.

In 2017 the NLRB issued a new test for evaluating an employer's work rules as interfering with protected rights. The NLRB will find a work rule unlawful if it explicitly restricts employees' protected concerted activity. If the rule is not explicitly unlawful, the Board will evaluate two things: (1) the rule's potential impact on protected concerted activity; and (2) the employer's legitimate business justifications for maintaining the rule. If the justifications for the rule outweigh the potential impact on

employees' rights, the rule is lawful. Conversely, if the potential impact on employees' rights outweighs the justifications for the rule, it is unlawful. The NLRB used this new test to find that an employer's rule prohibiting camera enabled devices was lawful.

PERB has yet to render a decision regarding employee privacy in the social networking context.

Increasingly, both public and private employers have been implementing social media policies for employee usage. Though members should be mindful as to what information they post online due to its permanent nature, it appears that the legal trend is on the side of protecting employees from undue discipline as a result of postings related to terms and conditions of employment.

INFORMATION ABOUT EMPLOYEES

Legal Activities

The New York Legal Activities Law prohibits employee discipline or discrimination in compensation, promotion, hiring, or other terms and conditions or privileges of employment because of an employee's participation in the following protected activities:

- Political activities
- Legal recreational activities
- Legal use of consumable products before or after working hours
- Membership in a union or the exercise of certain rights related to union activity

Physical Exams

Employers may require physical examinations to determine whether an employee is physically fit to perform the duties of his or her position. The New York State Court of Appeals has held that all public employees have some diminished expectation of privacy in respect to inquiries into their physical fitness to perform the duties of their job. For example, employees in the health field may be required to ensure that they are free of health impairments that are risks to patients and others.

However, under the Americans with Disabilities Act ("ADA"), an employer can only require a physical examination once it has made a bona fide offer of employment without regard to a physical or mental disability of an individual who is otherwise qualified to perform the functions of the job. Information acquired from any such exam must be treated as a confidential medical record.

Background Checks

In New York an employer may perform criminal background checks on applicants, but only after it has informed the applicant, in writing, of its intent to perform the background check. An employer – public or private – may not disqualify job applicants solely based on criminal history, unless otherwise mandated by law. Any such disqualification must be job related and consistent with business necessity. New York State, through Article 23-A of the New York Correction Law, aims to "break the cycle" of repeat offenders by creating a higher bar for employers to deny employment solely based on the existence of an applicant's or employee's criminal history. The law requires a number of factors an employer must balance in considering an applicant with a prior conviction. Article 23-A sets forth these factors:

- state public policy encouraging the employment of previously convicted persons;
- specific duties and responsibilities necessarily associated with the employment;
- bearing the offense will have on the person's fitness or ability to perform one or more such duties or responsibilities;
- time elapsed since the offense;
- person's age at the time of the offense;
- seriousness of the offense;
- information produced, attesting to the person's rehabilitation and good conduct;
- legitimate interest of the employer in protecting property, specific persons, or the general public.

Additionally, Article 15 of the New York Executive Law states that it is unlawful to make inquiries about – or act adversely on – any arrest which is no longer pending, where the criminal action terminated in favor of the arrested individual.

PERB applies a balancing test to employer requirements for background checks for existing employees. PERB will balance the employer's interests against the intrusiveness to the employees. If the employees' interests outweigh the employer's, then the background checks are a mandatory subject of bargaining and must be negotiated with the union before implementation.

Improper Interview Questions

Employers are not allowed to ask questions about the following subjects:

- Ancestry or marital status;
- Sexual preferences and family;
- Age (they can ask, however, whether you are between the ages of 18-70);
- Religion;
- United States citizenship;

- Birthplace;
- Time spent living in the United States;
- Foreign addresses;
- Whether you own or rent your home;
- Physical or mental limitations that are not job-related;
- Arrest record, however, employers can inquire about conviction of a crime. But note that for all employment in New York City an employer ***cannot*** inquire about criminal convictions before offering employment. For all employment in Westchester County and for applications for employment working for the State of New York an employer is ***not*** permitted to ask if an applicant has been convicted of a crime in the initial application.

Disclosure of Records

Public Officers Law §87 prohibits disclosure of records by New York State if the disclosure of such information would constitute an unwarranted invasion of privacy. These records include disclosure of employment, medical or credit histories, and personal references of applicants for employment. This provision does not apply to local government employees.

If the right of an employee to gain access to his or her personnel file is not already established under the collective bargaining agreement, then it may be possible to gain access based on arguments advocating for the employee's due process and liberty interest.

The New York Fair Credit Reporting Act regulates the dissemination of consumer reports and imposes certain requirements on employers who request them. In such an instance, the employer must notify the employee that it is seeking such a report. For an employer to gain access to the more detailed "investigative consumer report," the employee's authorization is required.

New York law prohibits employers from conducting adverse employment actions because an employee has a wage assignment or income execution against him or her.

Disclosure of Social Security Numbers

Some federal courts have recognized a right to privacy with respect to social security numbers under the umbrella of "informational privacy" right. But this does not mean that a governmental agency cannot disclose social security numbers in all cases. There may be instances where the government's interest outweighs an individual's privacy rights.

New York specifically prohibits any private person, firm, partnership, association, or corporation from engaging in the following activities:

- intentionally communicating an individual's social security number to the general public;
- printing an individual's social security number on any card or tag required for the individual to access products, services or benefits provided;
- requiring an individual to transmit his or her social security number over the internet, unless the connection is secure or the number is encrypted;
- requiring an individual to use his or her social security number to access an internet website, unless a password or unique PIN number is also required;
- printing an individual's social security number on any materials mailed to the individual, unless otherwise required by state or federal law – in which case, the number must not be visible without opening the envelope.

Genetic Testing

Under Title II of the federal Genetic Information Nondiscrimination Act of 2008 ("GINA"), it is illegal to discriminate against employees or applicants because of genetic information. GINA prohibits the use of genetic information in making employment decisions by restricting employers and other employment-related entities (such as employment agencies, labor organizations and joint labor-management training and apprenticeship programs) from requesting, requiring or purchasing genetic information, and strictly limits the disclosure of genetic information. Though it is usually unlawful for an employment-related entity to acquire genetic information about an employee, there are six narrow exceptions to this rule:

- Genetic information (such as family medical history) may be obtained as part of health or genetic services, including wellness programs, offered by the employer on a voluntary basis, if certain specific requirements are met.
- Inadvertent acquisitions of genetic information.
- Family medical history may be acquired as part of the certification process for FMLA leave (or leave under similar state or local laws, or pursuant to an employer policy).
- Genetic information may be acquired through commercially and publicly available documents like newspapers.
- Genetic information may be acquired through a genetic monitoring program that monitors the biological effects of toxic substances in the workplace where the monitoring is required by law or, under carefully defined conditions, where the program is voluntary.
- Acquisition of genetic information by employers who engage in DNA testing for law enforcement purposes.

CONCLUSION

An employee's right to privacy is much narrower than many may believe. However, it is clear that employees still retain some level of privacy rights. Technology and methods of communication constantly create the opportunity for employer monitoring and surveillance. Both private and public employers have broad rights to access information that many employees may believe is private and privileged. It is important for employees to be mindful of these rights and their own when engaged in employment.

Clearly, if you have questions or such an issue related to your employment you should first contact your local officers who can then relay the information to your Labor Relations Specialist ("LRS"). The LRS can then communicate directly with the Legal Department about the specific question.

Local 1000, AFSCME, AFL-CIO
143 Washington Ave., Albany, NY 12210

Mary E. Sullivan, President