WORKPLACE PRIVACY ISSUES:

Practical Advice for Employers and Employees

SUSAN MARTIN
MARTIN & BONNETT, P.L.L.C. 1

ABA SECTION OF LABOR AND EMPLOYMENT LAW
EMPLOYMENT RIGHTS AND RESPONSIBILITIES COMMITTEE
THIRD ANNUAL CLE CONFERENCE
WASHINGTON, D.C.
NOVEMBER 4-7, 2009

1 This paper was originally prepared by Heather Lindsay, Lindsay & Andrews, P.A. with portions incorporated with permission from Henry P. Julien, Jr. and Monique R. Gougisha, Kieswetter Wise Kaplan Prather, PLC for the ABA Section of Labor & Employment Law Employment Rights and Responsibilities Committee 2009 Mid-Winter Meeting and has been updated and reprinted in these materials with Ms. Lindsay’s permission.
I. Introduction

“Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is.” - Judith Thomson

Privacy, as it relates to the workplace, is a multi-dimensional issue. This paper focuses on three major areas that have the potential to trigger legal action over an employee’s right to privacy in the workplace: (1) surveillance/monitoring of workplace activities and electronic communications; (2) background checks and health testing, and (3) security and privacy of employee personal data. The information age, with its attendant technologies, allows speedy transmission and widespread access of information. Technology has become more advanced and sophisticated and the tension between technology and workplace privacy has become an important issue. Employers should evaluate whether the interests it seeks to protect are appropriately balanced against their employees’ rights to privacy. What privacy rights workers may have depends on numerous factors, including the laws in the applicable jurisdiction. This paper outlines some of the issues that arise with respect to workplace privacy concerns, provides some practical insights to employers and employees alike, and samples a few of the pertinent cases.

II. Surveillance/Monitoring of Workplace Activities and Electronic Performance

Sophisticated technology and high-tech equipment enable employers to monitor employees’ incoming and outgoing phone calls as well as their emails, web-page visits, computer files, and other workplace activities. E-mail and voicemail messages, in particular, are electronically stored and can be reviewed by anyone with access and the

proper equipment. Deleted e-mail messages can be retrieved intact. Data interception by remote transmission is also a powerful surveillance tool that allows stealth monitoring of all activity on one or more computers simultaneously from a remote command center. United Parcel Service, for example, has introduced “telematic review” of its package drivers utilizing data from a computerized notebook, global positioning satellite (“GPS”) receivers and hundreds of sensors mounted on its delivery vehicles to record information such as whether its drivers are driving without seat belts, braking patterns, number of deliveries and the length of time between deliveries.\(^3\)

Employers may have legitimate needs to monitor their employees while at work. However, monitoring employees, including monitoring employees’ email and internet usage system, implicates important privacy rights. Advancing technologies are providing employers with a powerful new ability to monitor the workplace but those same technologies can also increase an employer’s potential liability as employees fight back against infringement on their privacy rights.

\(\text{A. \hspace{1em} State and federal statutes governing monitoring efforts}\)

The United States Constitution, which protects against state action, applies only to privacy rights of public employees. There is no general federal right of privacy implicated by an employer engaging in surveillance of its employees on company premises. Privacy case law often arises from the common law of the states. Two federal statutes have also been utilized to limit an employer’s ability to monitor its employees’ email and computer usage: the National Labor Relations Act and the Electronic Communications and Privacy Act.

\(^3\) James A. McCall, *Human Tracking Devices and Employee Privacy*, Presentation at the Third Annual CLE Conference Nov. 4-7, 2009.
1) The National Labor Relations Act

The National Labor Relations Act ("NLRA")\(^4\) prohibits an employer from restraining or interfering with an employee’s right to engage in union activity or other protected concerted activity conducted for mutual aid or protection. Section 7 of the NLRA guarantees employees certain rights, including the right to self-organize; to form, join, or assist unions; to collectively bargain with their employer through chosen representatives; and to engage in other concerted activities. Most private employers, including those who are not currently unionized, are regulated by the NLRA.

In a long awaited decision involving workplace privacy issues in 2007, the National Labor Relations Board ("NLRB") held that employers have the right to implement and enforce a policy prohibiting employees from using the company’s email system for “non-job-related solicitations” provided the policy is not applied in a discriminatory manner.\(^5\) Although the union appealed the Board’s determination, it did not challenge on appeal the lawfulness of a company policy that bars union access to a company’s e-mail system on a neutral basis. Rather, the union contended, and the D.C. Circuit agreed, that the company’s stated reasons it disciplined employees for using the company’s computers to solicit on behalf of the union were post hoc rationales that had never previously been communicated or enforced and that in enforcing the purported ban on emails, the company acted in a discriminatory manner and committed unfair labor practices.\(^6\) Although this decision was in the context of a unionized company, the holding is equally applicable to employers who are not presently unionized, including

\(^5\) The Guard Publishing Company, 351 NLRB No. 70 (12/16/07).
\(^6\) Guard Publishing Co. v. N.L.R.B., 571 F.3d 53, 60 (D.C. Cir. 2009).
those involving possible union organizing campaigns or with respect to non-union companies where employees may be engaged in protected concerted activities as defined in the Act.7

2) The Federal Wiretapping Act

The Electronic Communications Privacy Act of 1968 ("ECPA"),8 commonly known as the Federal Wiretapping Act, governs the interception or acquisition of the contents of electronic communications, such as telephone calls or emails. The Act makes it unlawful – with certain exceptions – to intentionally intercept wire, oral, or electronic communications, and provides a civil remedy to victims. To establish liability under the ECPA, a plaintiff must show that a defendant: (1) intentionally, (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept, (3) the contents of (4) an electronic communication, (5) using a device.9 This law applies to the interception of telephone conversations, as well as email that is “in transit” (as opposed to stored on a company’s computer system).10 Whether an email has been “intercepted” (as opposed to “stored”) has been the subject of much litigation.11

---

7 In another case involving the NLRA and workplace privacy issues, the Ninth Circuit issued a unanimous decision in Local Joint Executive Board of Las Vegas et al. v. NLRB, 540 F.3d 1072 (9th Cir. 2008) upholding the NLRB’s three-factor test for determining whether employer surveillance activity of potential union members is coercive and therefore in violation of the NLRA. The three-factor test examines “the duration of the observation, the employer’s distance from its employees when observing them, and whether the employer is engaged in other coercive behavior during its observation” when determining whether employer observation is coercive.

8 18 U.S.C. § 2510 et. seq.

9 See In re Pharmatrak, 329 F.3d 9, 18 (1st Cir. 2003).

10 See, e.g., Brahmana v. Lembo, 2009 WL 1424438 (N.D.Cal. May 20, 2009) (claim that employer forwarded stored personal emails was not cognizable claim under ECPA but court denied motion to dismiss claim that employer used “software and hardware monitoring tools such as local area network analyzers and key loggers” as premature pending further discovery on the issues of how any alleged monitoring took place and whether it affected interstate commerce).

11 See, e.g., United States v. Councilman, 418 F.3d 67 (1st Cir. 2005) (en banc) (contemporaneous acquisition of e-mails was considered “interception” of messages under ECPA); Theofel v. Farcy Jones, 359 F.3d1066 (9th Cir. 2004) (email communications that had already been delivered and were stored on
Under the ECPA, if consent has been obtained, the communication lawfully may be intercepted so long as there is a lawful purpose for the interception. Accordingly, employers may generally monitor email and internet usage if the employee has consented to such monitoring. Consent may be actual or implied. An employer may require, for example, an acknowledgment of a computer and internet usage policy which makes clear that searches may occur, and that the employee has no reasonable expectation of privacy in the data. However, an employer should take note of recent decisions that limit employer’s rights. For example, a New Jersey court recently held that “[a] policy imposed by an employer, purporting to transform all private communications into company property merely because the company owned the computer used to make private communications or used to access such private information during work hours—furthers no legitimate business interest.”

3) The Stored Communications Act


an internet service provider’s server after the delivery of the email communication did not constitute interception under ECPA). See also Brahmana, supra, at n.9.
4) **The Fourth Amendment**

In *Quon v. Arch Wireless Operating Co.* 529 F.3d 892 (9th Cir. 2008), *rehearing denied* with concurrence, 554 F.3d 769 (2009); *cert granted* ___ U.S. ___ 2009 WL 1146443 (2009), the court held that police department employees’ Fourth Amendment rights to privacy were violated and that a service provider violated the SCA when the employer searched the content of text messages sent and received using City owned pagers that were archived by the wireless service provider and disclosed in response to a request by the employer. The Supreme Court granted certiorari to determine whether police officers had a reasonable expectation of privacy in their pagers where, despite an official policy banning personal use, an unwritten policy allowed some personal use. The Court also agreed to review whether Fourth Amendment law permitted the Ninth Circuit to analyze whether less intrusive methods were available. Valid Fourth Amendment claims for an unreasonable search were also found in *Nanducci v. Moore*, 572 F.3d 313 (7th Cir. 2009) where the court ruled that the public employee plaintiffs had reasonable expectations of privacy at work and that the employees had stated sufficient claims for Fourth Amendment violations to survive summary judgment.

5) **State Law**

Several states have statutes analogous to the ECPA. For example, the New Jersey Wire Tapping and Electronic Control Act prohibits third parties from gaining unauthorized access to, or disclosure of, emails.\(^{16}\) This statute, however, includes two exceptions – both of which are applicable in the employment context. The first exception allows for unauthorized access if an inspection is performed in the normal course of

---

business for business purposes or if the inspection was done to protect the employer’s rights or property. The second exception applies to monitoring that is consented to by one of the parties to the communication.

Virginia has two laws relevant to employer monitoring of employee email, voicemail and internet use. First, Virginia has a wiretapping law that is modeled on the federal law, with substantially similar coverage. Also, Virginia’s computer trespass law, Va. Code § 18.2-152.5, prohibits use of a computer or computer network to intentionally examine any employment, salary, credit or other financial or personal information relating to any other person unless the examiner has authority to do so. Violators of the statute are subject to civil and criminal penalties.

California is one of at least thirteen states that prohibits monitoring or recording telephone calls without the consent of all parties to the communication. In a unanimous decision with national implications, California’s Supreme Court held that out-of-state businesses are prohibited from secretly monitoring or recording their telephone calls with California residents, even if that conduct takes place in a state where only one party’s consent is required to lawfully monitor or record a telephone call. At a minimum, this ruling appears to require all employers whose employees communicate by telephone with any of California’s residents to re-examine their policies and practices for monitoring and recording telephone calls.

17 Va. Code § 19.2-61-70.3.
18 Other states that require the consent of all parties to record a telephone conversation include: Connecticut, Delaware, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania and Washington.
Florida, a state which requires all parties to consent to recording of conversations, also provides a civil cause of action “against any person or entity who intercepts, disclose, or uses, or procures any other person or entity to intercept, disclose, or use, such communications.” The term “person” includes “any employee or agent of the State of Florida or political subdivision thereof, of the United States, or of any other state or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.” Under Florida law, an oral communication cannot be intercepted and disclosed without the consent of the parties if there is a reasonable expectation of privacy.

Other cases have recognized that employees may have privacy rights grounded in state law. See Section IV, infra. For example, the Ninth Circuit held that a California state law claim for privacy could proceed against an employer who secretly videotaped employees in a workplace restroom and that such action was not preempted by the LMRA even though the employees were covered by a collective bargaining agreement.

B. Effective and appropriate monitoring policies

Establishing an effective and appropriate policy is one way to protect an employer from against alleged privacy violations. However, the employer must also make appropriate efforts to disseminate the policy and implement it in a consistent and even-
handed manner.\textsuperscript{24} Below are few points parties should consider in determining whether an existing policy is appropriate:

1. Whether the policy explains when and how monitoring and inspections will occur. Adequate notice of the intent to monitor and the form of monitoring (\textit{i.e.,} its frequency and its purpose) is imperative.

2. Whether the policy also identifies company property, whether it uses a broad definition, and whether it indicates that employees should have no expectation of privacy in company property. If there is a restriction on the use of computers such as for business purposes only, that policy needs to be clear and it should strictly prohibit unauthorized use of email or the internet for any other purpose, including but not limited to, downloading pornographic, offensive, or harassing communications, copyrighted or trade secret information, or any other non-business related information.

3. Whether the policy prohibits attempts to appropriate the employer's trade secrets or copyrighted information, or to disable or compromise the security of information contained in the company's computers.

4. Whether the policy makes clear that passwords are intended simply to prevent outsiders from obtaining access to information on the employer's system, but are not an indication that the employee has any privacy rights in the contents on the computer.

5. Because needs regarding monitoring and inspection may change over time (particularly since technology is constantly advancing), whether the policy allows for future modifications by the company.

An employer should use caution, however. A violation of a company policy regarding computer usage does not necessarily mean that an employer is always justified in reviewing an employee’s personal emails. For example, a court recently held that a company was not justified in obtaining attorney-client communications that an employee sent from his web-based email account on a company computer even though the employee might have been breaching company policy regarding internet usage in sending such communications: “we conclude a breach of a company policy with regard to the use of its computers does not justify the company's claim of ownership to personal communications and information accessible therefrom or contained therein.”

III. Background Checks and Health Testing

A. Background checks – the positives and pitfalls.

While employers have a legitimate need to ensure they hire the best possible candidates, reference and background checking methods which impermissibly disclose protected information or private facts can give rise to a cause of action. The degree and type of permissible checking may vary from position to position, but the same degree of checking for all applicants for the same position should be done to avoid actual or apparent discrimination, especially since background investigation processes which have the effect of denying employment to individuals in protected classes may be found to be

26 Most states have a cause of action for "public disclosure of private facts" or "false light." Improper reference and background checking may trigger liability under these causes of action.
discriminatory.\textsuperscript{27} For example, credit checks are usually considered unnecessary for employees who will not be handling money or other financial assets. Similarly, checking on a qualification which is unrelated to the job position, but which the applicant may have disclosed on his or her resume, will not always be considered to be necessary or reasonable and could be considered discriminatory.

For several years now, the Fair Credit Reporting Act (FCRA)\textsuperscript{28} and parallel state laws have restricted when and how an employer may conduct background checks on applicants and employers and how such information may be used. Generally, these restrictions apply when the employer conducts background checks through an outside entity. Restrictions normally do not apply when an employer obtains information directly, such as by calling a school or university to verify that the applicant or employee did in fact attend and graduate. Notice and consent requirements must be followed when an employer decides not to hire an applicant or takes action against an employee based on the results of a background check. Significantly, before adverse action is taken, the FCRA requires that the employer provide the applicant or employee with a copy of the report and a written description of the individual’s rights under the FCRA.\textsuperscript{29} This allows a potential employee an opportunity to correct any inaccurate information in the report. After taking the adverse action, the employer is required to provide another written notice with specific disclosures and information.\textsuperscript{30}

\begin{footnotes}
\item[27] With respect to arrest inquiries, for example, there is a proven adverse impact based on race. \textit{See e.g., Reynolds v. Sheet Metal Workers}, 498 F. Supp. 952, 960 (DDC 1980), \textit{aff’d}, 702 F.2d 221 (D.C. Cir. 1981).
\item[28] 15 U.S.C. §§ 1681, \textit{et seq.}
\end{footnotes}
Criminal background checks raise specific concerns since employers might need to be aware of past criminal behavior in order to prevent potential violence in the workplace for which they may be liable under a theory of negligent hiring. However, criminal background checks should only seek information about convictions and not arrests, and employers should assess and balance the job duties and scope of responsibility against the seriousness of the criminal behavior. Questions often arise, however, when criminal background information is readily available from online or alternative sources. For example, “Megan’s Law,” a federal statute enacted in 1996, requires every state to create a registry for convicted sex offenders and make certain information about those offenders available to the public. This information is available online and anyone can access these websites and search for registered sex offenders by name. In the employment context, two questions often arise with respect to Megan’s Law: (1) may an employer check the Megan’s Law website to determine whether employees or applicants for employment are listed there, and (2) must an employer check the Megan’s Law website?

Several states, such as California, prohibit the use of sex offender information on the state Megan’s Law website with regard to employment unless it is used to protect “a person at risk.” At the same time, there is no statute or court ruling requiring an employer to check the Megan’s Law website. The laws of negligent hire and retention, however, require that employers use care in screening applicants for employment in order to eliminate any foreseeable risk of harm to customers, co-workers or to members of the public. As An employer may be liable for negligent hire and retention, for example, where

---

31See the Restatement (Second) of Torts § 317 for the reasonable care standard some states have adopted for this tort.
a sex offender engages in sexually harassing conduct towards a co-worker. In some states, checking the sex offender registry may be relevant in a claim of negligent hire and retention.

A willfulness or reckless disregard tort theory of liability may be available against an employer who is aware of an employee’s criminal background. For example, if an employer is aware that an employee is prohibited by the terms of his probation from contact with minors, but nonetheless employs such a person in a capacity that allows him or her to supervise employees who are minors, then that employer may be liable for recklessness. Such theories of liability may not be successful if the employer can establish that the “tasks, premises, or instrumentalities” entrusted to the offending employee were not necessary to the accomplishment of the harm.

In addition, employers should take care to guard the information obtained while performing these checks. A clear privacy policy should advise the prospective employee that the company will limit collection of employee information to that needed for business and legal purposes, protect the confidentiality of all personal information in employee records, and limit access to private records to staff members who have an authorized business need to know or to parties who have obtained a court order or subpoena for specified employee records.

32 In Priest v. Brummer, 2008 WL 2788759 (N.D. Ind. Jul. 18, 2008), where a sex offender harassed his co-worker with comments, touching, and lewd notes describing his violent fantasies about the plaintiff. The employer settled. See also Pourgholam v. Advanced Telemarketing Corp., 2004 WL 1283963, 4 (N.D. Tex. June 9, 2004) (in denying summary judgment to employer on a harassment claim, the court noted that the summary judgment record contained evidence that harasser was a registered sex offender with two felony convictions for sexual offenses and evidence that Defendant obtains background checks on prospective employees as a condition of employment).

33 Hansen v. Board of Trustees Hamilton Southeastern School Corp., 551 F.3d 559 (7th Cir. 2008).


35 An employer’s duty is “limited to preventing the tasks, premises, or instrumentalities entrusted to an employee from endangering foreseeable victims.” Thompson v. Wang, 2008 WL 4967997 (Wash.App. Div. 1 Nov. 24, 2008).
Generally the following factors are important to consider the steps an employer may take to obtain relevant information, while minimizing the risk of violating an employee’s privacy interests:

1. Whether the employee is required to fill out an application form which is signed and attested to for accuracy and whether the employee has acknowledged that any falsification, material omission or misrepresentation may result in failure to receive an offer of employment, or, if hired, may result in a dismissal from employment.

2. Whether the responsibilities of the position require background checks and whether the different background checks should be performed for every position. Employers should perform the same checks for everyone applying for the same position in order to prevent a finding that the checks were discriminatory or retaliatory.

3. Whether the employee is notified ahead of time, in writing, of the types of reference and background checks that will be conducted in order to determine that they are qualified for the job and whether the employee obtains written consent from the employee or applicant to perform such checks.

4. If credit, motor vehicle and/or criminal checks are required for the position, whether the procedures outlined in the Fair Credit Reporting Act are followed and the appropriate notices given. If an adverse action is taken based on information contained in a credit, motor vehicle and/or criminal report, the employee must be notified and advised of his or her rights in accordance with the Act.

5. Whether all attempts to check references and the information obtained are documented.
6. Whether the employer should speak to an employee's former supervisor rather than simply speak with the Human Resources department.

7. Whether legally protected information is sought while checking references. Employers cannot and should not seek information from a third party about which you could not ask the candidate directly.

8. Whether personnel files are kept in the Human Resources department and whether the files are maintained under lock and key. Employers should ensure that personnel files are not left in a public place where anyone may have access to them. Make sure that electronic versions of these documents are password protected. Employers should not disclose information in personnel files to everyone, even another management employee, unless that person has a business reason to know information contained in the files. Employers should also uniformly and consistently discipline employees who violate procedures aimed at protecting employees' privacy rights.

B. Health Testing

Health tests are likely to be the most invasive of all employment procedures and most likely to give rise to privacy claims. For example, where employees are subject to random drug tests, those tests should in fact be random. As a result, employers need to be extremely vigilant to ensure that all such testing is necessary, and then, that it is properly carried out.

As a general matter, applicants should be offered a position first before being required to undergo medical testing, and the employer should pay for any such testing. Drug and alcohol testing may be performed if an offer is made, and an applicant may be excluded from employment if tests reveal the current use of drugs or alcohol. An
applicant may not be excluded based on a past history of drug or alcohol use. However, in *Raytheon v. Hernandez*, 540 U.S. 44 (2003) the Court upheld a company’s unwritten policy not to rehire a former employee who resigns for violation of its rules of conduct where the employee had tested positive for cocaine. Once the person is hired, testing is allowed for business necessity, or in order to comply with other laws and regulations, for example Department of Transportation regulations governing truck drivers.

Regardless of the type of tests, employers should keep the following principles in mind:

1. There must be a specific business-related reason for a test and the test must measure something specific and objective.
2. The use of any test results must be clearly identified, and the results of each test must be applied uniformly in hiring, firing or promotion decisions.
3. Do not give tests if the results will not be considered.
4. Keep all test results confidential, especially medical, psychological, and drug and alcohol testing, but make the results of the test available to the employee.
5. Make sure tests are performed by a licensed professional and are not more invasive than necessary to obtain valid test results.

**IV. Security and Protection of Employee’s Personal Information**

Identity theft has become one of the fastest growing crimes in America. Breaches of personal information have affected hundreds of thousands, if not millions, of

---


37 In *Krieg v. Seybold*, 481 F.3d 512 (7th Cir. 2007), the court upheld a public employer’s termination of a “safety-sensitive” employee who refused to submit to a random drug test, concluding that the random drug test did not violate the employee’s Fourth Amendment right against unreasonable searches.
individuals. Instances of stolen laptops and PDAs, unauthorized entries into electronic databases and similar attacks on personal information are frequent. With that said, employers have an inherent need to obtain personal identifying information about employees and applicants for various reasons, such as identification and verification of employment status, background checks, benefits and leave administration and contact information. How employers use, maintain and protect such information is increasingly subject to legislation (and litigation) in many states. Below are some legal and legislative updates on how various states are tackling the issues associated with the rapid growth of data privacy and security laws affecting employers:

A. Identity Theft Legislation

Numerous states have adopted identity theft legislation which may impact the employment relationship. For example, in 2007 Oregon adopted the Consumer Identity Theft Protection Act (S.B. 583), a comprehensive data security law that creates two significant obligations for Oregon businesses (and companies that do business in Oregon).38 First, businesses must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of personal information. This will likely require taking steps such as performing a risk assessment, preparing written policies and training employees. Second, businesses must notify state residents of data breaches involving their computerized personal information.

The Oregon law requires businesses to take affirmative steps to secure the personal information it maintains, which would include personal information of employees and job applicants. This means that employers in Oregon can now be held

accountable for the misuse or lack of safeguards for the personal information of their employees or job applicants. Employers will be deemed compliant with the Act’s security maintenance requirements where they implement an “information security program” that contains administrative, technical and physical safeguards.

B. Washington’s Fair Credit Reporting Act

S.B. 5827, effective July 22, 2007, amends Washington’s Fair Credit Reporting Act\(^39\) to prohibit the use of consumer credit reports for employment purposes unless the information on that report is substantially related to the employee’s job duties. Under the amendment, employers are prohibited from using information concerning an applicant or current employee’s creditworthiness, credit standing, or credit capacity unless the information either is (1) “substantially job related and the employer’s reasons for the use of such information are disclosed” to the individual in writing or (2) required by law.\(^40\) Washington’s recent limitations on the use of credit information in employment are significant for employers who regularly use credit reports for background checks on job applicants or investigation of current employees. The law’s stated purpose is to require an employer to establish the need for a credit report based on the actual job duties of the current or prospective employee. However, the law does not define when a credit report’s information is “substantially related” to an employee’s job duties – an omission that could lead to potential challenge and litigation.


\(^40\) Wash. Rev. Code § 19.182.020(2)
Governor Ed Rendell signed this legislation on June 29, 2006. Employers doing business in Pennsylvania should review their practices regarding the use and disclosure of social security numbers in light of this new law, which increases protection against theft and improper use. The new law prohibits certain activities involving social security numbers (“SSN”) including: (1) publicly posting an individual’s SSN in any manner; (2) printing an individual’s SSN on any card required for the individual to access the products or services provided by the entity subject to the new law; (3) requiring an individual to transmit his or her SSN over the internet (unless the transmission is encrypted); and (4) printing an individual’s SSN on any materials that are mailed to an individual (except where required by federal or state law – such as a W-2 form).

D. Illinois’ Right to Privacy in the Workplace Act

The Right to Privacy in the Workplace Act, Public Act 095-0138, 41 which became effective on January 1, 2008, prohibits any individual from refusing to hire, terminate employment, or otherwise disadvantage any person because he or she uses “lawful products,” generally understood to mean alcohol and tobacco, away from the job site on non-working time. The Act also requires employers using the federal E-Verify system (formerly known as the Basic Pilot/Employment Eligibility Verification Program) to comply with certain training, posting and privacy requirements. An employee can lodge a complaint with Illinois’ Department of Labor to have alleged violations investigated and addressed. 42

42 http://www.state.il.us/Agency/idol/laws/Law55.htm
E. Reminders for New York Lawyers

Effective January 1, 2008, the General Business Law imposed two specific obligations on New York employers to protect the privacy of SSNs. First, section 399-dd of the statute limits what businesses operating in the state can do with SSNs. Second, to the extent a New York business maintains SSNs to conduct its business or trade, the law says it must: (1) take reasonable measures to ensure that officers and employees have access to such numbers only for legitimate or necessary purposes related to the conduct of such business or trade; and (2) implement safeguards necessary or appropriate to preclude unauthorized access to SSNs and to protect the confidentiality of such numbers.

Also, to protect individuals if there is a breach of the integrity of a business computer system containing personal information, New York enacted a breach notification statute (section 899-a of the General Business Law). This law requires a business to notify individuals whose personal information (which could include SSNs, among other items) is breached under certain circumstances. Notification to designated state agencies, including the Attorney General’s office, is also required. This statute underscores the need to focus on privacy measures and safeguards, especially for electronically maintained personal information, such as driver’s license numbers and bank account numbers. Even with preventative measures in place, businesses still must have a plan for responding to a data breach.43

---

43 The New York Supreme Court Appellate Division ruled in a 3-2 decision that punitive damages can be awarded for a grossly negligent breach of confidential medical information even if the breach was not intentional or malicious. Randi A.J. v. Long Island Surgi-Center, 46 A.D.3d 74, 82 (NY App. 2007).
V. Privacy Theories of Liability Pursued by Plaintiffs

Monitoring and searching of employees and testing of applicants and returning employees can lead to litigation, with significant economic consequences. As to the right to privacy within the workplace in the public sector, the United States Supreme Court in *O’Connor v. Ortega* stated that “the employee’s expectation of privacy must be assessed in the context of the employment relation.”

Depending on that context, employees may have a reasonable expectation of privacy in their offices. For example, in Wisconsin, a lawyer stated a claim for invasion of privacy, where he alleged that his partners removed personal property and items from his office and opened sealed personal correspondence. Pursuant to the Wisconsin statute, a prevailing plaintiff is entitled to equitable relief, compensatory damages, and attorneys’ fees.

In a recent case in Utah, a plaintiff presented evidence that as a result of being recorded without his permission by a co-worker, he suffered paranoia and anxiety such that he became distrustful of his co-workers. The evidence also showed that the plaintiff’s anxiety manifested itself in a loss of sleep and appetite. This evidence was sufficient to establish damages as a result of the invasion of the plaintiff’s privacy by his co-worker. Nonetheless, the court declined to award damages as a result of the violation of the Federal Wiretap Act because the co-worker’s recordings occurred only over the course of nine days, no evidence established that she shared the recordings with the

---

45 Wisconsin defines an invasion of privacy as “intrusion upon the privacy of another of a nature highly offensive to a reasonable person, in a place that a reasonable person would consider private or in a manner which is actionable for trespass.” Wis. Stat. § 995.50
47 Wis. Stat. § 995.50.
plaintiff’s supervisor, and she derived no profit from her illegal recording of the plaintiff. The court did, however, award attorneys’ fees to the plaintiff pursuant to the Federal Wiretap Act.

Accessing personal email of an employee without authorization subjects the employer to liability pursuant to the Stored Communications Act,\textsuperscript{50} for example. Such a violation could have other undesirable consequences, such as a preclusion of evidence. In a recent case, defendant employees alleged to have stolen confidential information and related claims were successful at precluding the use of damaging emails as evidence based on the theory that the emails were obtained in violation of law.\textsuperscript{51} In that case, the thirty-four emails at issue were not sent from or received on the company email system or computer; rather, a private email account was accessed on company computers.\textsuperscript{52} The emails at issue were stored on third-party computer systems and protected by passwords, but a plaintiff obtained them because the email account information and password were stored on a company computer. Although the company’s email policy stated that employees had no right to privacy with respect to electronic information within the company’s system, no evidence supported the conclusion that the company policy was clearly communicated and consistently enforced. Moreover, the court interpreted the policy language to authorize access to emails from third-party accounts only where those emails were saved on the company’s computers. Accordingly, the court precluded the use of the thirty-four emails except for impeachment purposes.\textsuperscript{53}

\textsuperscript{50} 18 U.S.C. § 2707.
\textsuperscript{52} 587 F. Supp. 2d at 560.
\textsuperscript{53} Because the emails were not intercepted contemporaneously with their transmission, there was no violation of the Federal Wiretapping Act, 18 U.S.C. § 2510-11; however, the unauthorized access to the stored communications was a violation of the Stored Communications Act, 18 U.S.C. § 2707.
The threshold issue is whether the employee has a reasonable expectation of privacy, and the wording of the employer’s policy is examined to evaluate that issue. Where an employer prohibits personal use of office computers, for instance, an employee may not have a reasonable expectation of privacy. Nonetheless, an employee with exclusive use of a computer in a private office may have a reasonable expectation of privacy despite a policy prohibiting personal use of the employer’s equipment.

Additionally, employees may assert false light invasion of privacy in states where the tort is recognized based on the use of employee information. For example, in *Meyerkord v. The Zipatoni Company*, Meyerkord sued his former employer, which provides marketing services to businesses, because he was falsely listed as the “registrant” for the employer’s account with Register.com for the purpose of registering websites. After his employment ended, Meyerkord was listed as the registrant for a company’s website that became the subject of controversy by bloggers, consumers, and consumer activist groups. The Missouri Court of Appeals held, as a matter of first impression, that the tort is cognizable in Missouri where a person, with actual malice or knowing disregard as to the falsity of the publicized information, places another before the public in a false light, that person may be liable for resulting damages.

Because being required to submit to drug testing is not in itself an adverse action by an employer, the cases concerning drug testing usually pertain to allegedly non-

---


55 See, e.g., *Leventhal v. Knapek*, 266 F.3d 64, 74 (2d Cir. 2001).


57 Collected cases reflecting other jurisdictions recognizing the tort can be found at footnote 1 of the *Meyerkord* decision.

58 *Pegram v. Honeywell, Inc.*, 361 F.3d 272, 282 (5th Cir. 2004).
random testing or inconsistent application of a drug testing policy. In one recent case, a manufacturing employee who tested positive twice for amphetamines and methamphetamine and was therefore terminated sued the former employer based on a theory of age discrimination. The employee was suspended after the first positive test, and he attempted, unsuccessfully, to show that the positive result was due to taking prescribed medication. After the employee completed his suspension, he was tested again, and once again the result was positive. As a result, the employee was fired. The employee was over forty, and his replacement was not within the protected class. Although the plaintiff asserted a prima facie case of discrimination, there was no evidence that the employer was inconsistent with respect to its drug testing policy; accordingly, the claim was dismissed at summary judgment for the plaintiff’s failure to meet his burden to establish pretext.

As to medical records, plaintiffs do not have a private cause of action to enforce rights protected by HIPAA with respect to the confidentiality of medical records. Rather, relief is limited to enforcement of the statute by the Secretary of Health and Human Services as specifically provided for in the statute. Section 1983 official capacity actions because of asserted violations of privacy by state actors with respect to


medical records have also been unsuccessful. For example, the Sixth Circuit has refused to recognize any general constitutional right to privacy in medical information: “Disclosure of plaintiff's medical records does not rise to the level of a breach of a right recognized as ‘fundamental’ under the Constitution.”

State laws concerning the confidentiality of medical records may provide a private cause of action, however.

Moreover, state constitutional rights to privacy may allow plaintiffs to state a claim for violation of privacy with respect to the disclosure of confidential medical and personal information. California law recognizes a constitutional right to privacy in an individual's medical history. For example, California Constitution Article 1, § 1, states that “[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.” To state a cause of action pursuant to this article, a plaintiff “must establish each of the following: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy.”

In Kina v. United Air Lines, Inc., Kina was fired after a health care provider released to the employer detailed and sensitive information obtained during extensive

---

62 Jarvis v. Wellman, 52 F.3d 125, 126 (6th Cir.1995); see also J.P. v. DeSanti, 653 F.2d 1080 (6th Cir.1981); Doe v. Wigginton, 21 F.3d 733 (6th Cir.1994).
fitness-for-duty examinations,\textsuperscript{67} which the employer required after Kina had been on medical leave for depression. Kina alleged that he was fired because of the information disclosed by the health care provider, which Kina claimed “had no possible relationship to his ability to perform the essential functions of his job, or any other vacant position for which he was qualified.”\textsuperscript{68} Kina alleged multiple claims, including an invasion of privacy claim against the health care provider for its unauthorized disclosure of information to Kina’s employer. The court held that Kina had stated a claim for invasion of “informational privacy” protected by the California Constitution.\textsuperscript{69}

These are just a few examples of how privacy is defined in the employment context. Multi-state and multi-national employers and businesses should review applicable legislation and case law developments to ensure compliance and avoid unnecessary litigation risks. Employers should approach the issues with a thorough attention to detail with respect to legal compliance and policy development and enforcement. Employees can pursue remedies through the ever-evolving law of torts in addition to federal and state statutes and constitutions to address privacy concerns. Because the employment environment continues to change with advances in technology, we should be prepared to participate in the development of legislation that justly balances the divergent interests of employers and employees with respect to workplace privacy.

\textsuperscript{67} The myriad assessments required included phone interviews with family members, blood and urine testing, and psychological testing.

\textsuperscript{68} \textit{Id.} at *9. Kina had worked as a storekeeper.

\textsuperscript{69} California also recognizes “autonomy privacy” which relates to the right to make intimate personal decisions or conducting personal activities without observation, intrusion, or interference.