TOPIC:

Business Vs. “Nobody’s Business”: Searches Of Employer-Issued Technology And The University Employee’s Expectation Of Privacy

INTRODUCTION:

Both the Supreme Court and society at large have come to agree that employees should enjoy a certain reasonable expectation of privacy in their workplace effects and correspondence. [1] Yet there may be occasions when employers need to monitor employees or search their correspondence in order to control the workplace and manage the risks of the organization – a reality the Supreme Court has also recognized. [2]

Along with these competing interests, the proliferation of employer-issued technology [3] has significantly altered the notion of privacy in the workplace. Employer-issued laptops, smart phones, and mobile devices allow employees to work from the road or from home, and have blurred the boundaries between personal and workplace communications. Where it may have been clear in the past that a letter addressed to an employee carried an expectation of privacy, [4] the line may not be as clear with respect to a personal text message or email sent on an employer-issued smart phone. This new reality makes it more challenging to determine the reasonableness of an employer’s search and the scope of privacy in the workplace. Likewise, even if the employee uses her own device, she may be sending employment-related information in the form of electronic mail, documents, and texts. The intermingling of ownership and other supervisory authorities vested in both data and devices, together with shifting notions of personal privacy, have generated considerable confusion about the boundaries of the law.

For public institutions, the Fourth Amendment protects employees from unreasonable searches. Private institutions, though free from the strictures of the Fourth Amendment, may nonetheless have to abide by state constitutional provisions and laws that protect employees from unreasonable invasions of privacy by private employers. But, in the context of technology searches, the Supreme Court has been purposefully vague in defining what is “unreasonable.”

What is clear is that, while technological dimensions cannot be ignored, it is the institution’s policy that will govern the outcome of a privacy determination. Thus, public and private institutions must ensure that clear and conspicuous policies are in place. In the absence of a specific policy, the institution’s practice will then serve as a proxy in making privacy determinations.

This NACUANOTE will provide an overview of selected privacy laws and cases affecting technology in the workplace and offer suggestions for how the college or university employer can best supervise, control, and operate an efficient workplace without unreasonably invading employee privacy.
DISCUSSION:

Communication is in the midst of a technological revolution. Text messages and emails have begun to displace landline telephone calls, letters, and even face-to-face interaction as the dominant means of communication. While the methods of communication may be changing, their characteristics may still give rise to expectations of privacy that are virtually identical to, and just as reasonable as, the privacy expectations associated with messages transmitted via more traditional media.

I. The Fourth Amendment and the Workplace

The Fourth Amendment of the U.S. Constitution protects the right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures. It applies not only to traditional searches and seizures by police, but to "searches and seizures by government employers or supervisors of the private property of their employees." [5] This includes searches by public college and university employers. [6] The critical question, then, is what makes an employer's search "unreasonable" and therefore unlawful under the Fourth Amendment?

In simplest terms, the answer involves a balancing test between an employee's reasonable expectation of privacy and the employer's need to conduct the search and obtain information. [7] And, while the Supreme Court cases below provide an instructive framework for balancing these competing interests, there are still no bright line rules with respect to technology searches.

A. The Original Benchmark for Workplace Searches: O'Connor v. Ortega

The Court's plurality decision in O'Connor v. Ortega was its first attempt to reconcile privacy rights with workplace searches and has served as the seminal workplace privacy case for over 20 years. In reviewing a public employer's search of an employee's office and file cabinets, the Court first recognized that there exists a valid "societal expectation[] of privacy in one's place of work." [8] But the Court also noted that public employers may need to make reasonable work-related intrusions and conduct investigations into possible work-related misconduct, in order to ensure an effective and efficient workplace. [9] Thus, in determining what workplace searches would be considered "reasonable," the Court set forth two enduring principles.

First, the court must determine whether an employee had a legitimate expectation of privacy to begin with. This is because "some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable." [10] Thus, a court must consider the "operational realities of the workplace," and whether the employee's privacy expectation is diminished "by virtue of actual office practices and procedures, or by legitimate regulation." [11] In O'Connor, the Court found that the employee did have a reasonable expectation of privacy in his desk and file cabinets, as he did not share them, all files related to other employees were kept outside of his office, and he had occupied the same office for 17 years.

Second, the Court held that even if a reasonable expectation of privacy exists, an employer may still conduct the search as long as the purpose of the search is legitimate at its inception and the scope of the search is reasonably related to the employer's objectives. [12] The Court declined to make these determinations (instead remanding the case for further consideration), but O'Connor established an analytical framework that courts still use today.

B. Workplace Searches Revisited: City of Ontario v. Quon

In the face of continuous technological change over the past two-plus decades, the Supreme Court revisited employee workplace privacy issues in its 2010 decision, City of Ontario v. Quon. [13] At issue in Quon was the City of Ontario Police Department’s search of its employee’s text messages on
his employer-issued pager. [14] Quon had been warned that the City had a policy under which it reserved the right to monitor and log all network activity, including text messages, email and internet use, with or without notice to employees. The policy further stated that “users should have no expectation of privacy or confidentiality when using these resources.” [15]

After Quon exceeded his set monthly text allowance multiple times, his supervisor requested transcripts of the texts to determine whether the overages were occurring as a result of Quon’s personal use of the pager, as opposed to proper work-related use. The resulting search revealed personal messages to Quon’s wife and an alleged mistress.

After learning that the city had searched his text messages, Quon sued the City of Ontario, alleging that the search violated his Fourth Amendment rights, the Stored Communications Act, and other state laws. A federal district court determined that while Quon had a reasonable expectation of privacy in the content of his text messages, the City of Ontario had a legitimate purpose for undertaking the search. The Ninth Circuit reversed, reasoning that even if the search was conducted for a legitimate reason, it was unreasonable in scope because the City of Ontario failed to use less intrusive means.

On review, the Supreme Court unanimously reversed the Ninth Circuit’s decision and found that the scope of the City’s search was indeed reasonable. [16] In so finding, the Court noted as a preliminary matter that employers are not required to use the “least intrusive search practicable” under the Fourth Amendment. [17] Next, the Court found that the scope of the search was reasonable because, among other things, the employer limited the search to only two months of text messages and excluded from the search any text messages sent outside work hours, demonstrating that the employer was trying not to intrude on Quon’s personal privacy.

Just as important as what the Court ruled upon, however, was what the Court specifically declined to address. Namely, the Court declined to address the first of the O’Connor principles – i.e. whether Quon had a reasonable expectation of privacy in his text messages. Because the Court found that the second prong of O’Connor was satisfied (the purpose of the search was legitimate at its inception, and the scope was reasonably related to the employer’s objectives), the search was valid regardless of whether Quon had a reasonable expectation of privacy in his texts. The Court explained its hesitation to create a firm rule regarding an employee’s expectation of privacy in text messages:

The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. . . . Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . . At present, it is uncertain how workplace norms, and the law’s treatment of them, will evolve. . . . A broad holding concerning employees’ privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. [18]

With that, the Supreme Court effectively confirmed that a public employee’s expectation of privacy in communications on employer-issued technology will depend in large part upon employer policies and practices and legitimate regulation. Once again, it is important to emphasize that no such federal constitutional expectation of privacy exists for employees of private entities.

C. Lower Court Decisions Focus on Workplace Policies

While Quon and O’Connor made clear that public employees’ expectations of privacy can be reduced or expanded by “the operational realities of the workplace,” [19] neither opinion provided clear guidance as to the level of privacy, if any, a public employee can expect in employer-issued technology. [20] Lacking this guidance, and grappling with the fact that operational realities are
frequently changing with technology, lower courts have come to rely heavily on stated policies and procedures with regard to technology. For example, the employee may retain an expectation of privacy when employer policies are imprecisely worded or inconsistently enforced:

- In *Leventhal v. Knapek*, the Second Circuit found that a public employee had a reasonable expectation of privacy in his work computer and matters contained therein despite the employer's official policy prohibiting the use of state equipment for personal business. The court noted that the employee did not share his computer with anyone, there was no general practice of the public employer to routinely search employee computers, and the employer had not made clear that employees lacked privacy rights in what was stored in the computers. [21] Importantly, the Court's decision emphasized that the employer's practice was determinative and operated as a *de facto* policy.

- In *Stengart v. Loving Care Agency, Inc.*, the New Jersey Supreme Court held that an employee has a reasonable expectation of privacy in communications with her lawyer via a personal, password-protected email account, even if accessed on an employer-issued computer. [22] In addition to preserving the sanctity of the attorney-client privilege, the Court found that Stengart had a subjective expectation of privacy because she took steps to protect her emails, sending them from her personal, password-protected account and not saving her password to the employer-issued computer. [23] Also importantly, the Court concluded that the employer's email policy was unclear and permitted "occasional personal use," thereby creating ambiguity as to whether personal email was employer or private property. [24] In holding that Stengart had a reasonable expectation of privacy, the New Jersey Supreme Court recognized the employer's practice as a proxy for an explicit policy.

By contrast, where there are clear, explicit, and reasonable policies, lower courts have declined to recognize a reasonable expectation of privacy in employee emails and other documents and records created on employer-issued technology. [25]

- The Fourth Circuit held in *United States v. Simmons* [26] that a government employee lacked a legitimate expectation of privacy in the files he downloaded from the Internet because of a workplace policy. In a routine security check of the workplace firewall protection, the employer discovered Simmons had downloaded material unrelated to government business despite an explicit policy stating the employer would audit or monitor "all file transfers, all websites visited, and all email messages." [27]

- In *Biby v. Board of Regents of the Univ. of Nebraska*, [28] the Eighth Circuit reviewed a case in which the public university employer had a policy informing computer users "not to expect privacy if the employer has a legitimate reason to conduct a search," specifically including searches "responding to a discovery request in the course of litigation." [29] The University sought to produce files from Biby's computer in response to a discovery request, and Biby claimed the search violated his Fourth Amendment rights. [30] In light of the policy, the court found that Biby failed to show he had a reasonable expectation of privacy in his computer files. [31] Moreover, in the context of discovery and in anticipation of litigation, Biby also underscores the importance of circulating litigation-hold letters notifying employees of not only the requirement to preserve information contained on employer-issued technology such as smartphones, cell phones, computers, laptops, pagers, or tablets, but also the prospect that such information may be
searched by the employer. In sum, the lesson of Biby is twofold: (1) A well balanced policy provides an employer with greater leverage to conduct a search, especially in the context of litigation; and (2) litigation-hold letters are necessary to notify employees that information contained on employer-issued technology may be searched in furtherance of discovery requests related to pending litigation.

- The Tenth Circuit held in United States v. Angevine [32] that a public university professor had no legitimate expectation of privacy in pornographic files stored on his computer where the university's computer policy stated: “The contents of all storage media owned or stored on University computing facilities are the property of [the] University,” and “[T]he University reserves the right to view or scan any file or software stored on the computer or passing through the network, and will do so periodically . . . to audit the use of University resources.” [33] It is important to emphasize that this case arose out of criminal conduct. In this respect, the additional lesson here is that should an institution suspect criminal wrongdoing through employer-issued technology, the matter should be forwarded to campus or local police so that law enforcement can initiate an investigation and utilize subpoena power and/or obtain a warrant.

In short, and irrespective of the technology, these decisions confirm that where there is an explicit policy setting forth terms under which technology and facilities are monitored, the balancing of privacy interests weighs heavily in favor of the employer.

II. Federal Statutes Affecting Privacy in the Workplace

While Fourth Amendment claims are germane only to public institutions, public and private institutions alike must abide by federal laws protecting employee privacy in the workplace. Most applicable to employer-issued technology would be the Electronic Communications Privacy Act of 1986 ("ECPA") and one of its subparts, the Stored Communications Act.

The ECPA prohibits the unauthorized interception, acquisition, disclosure, or use of the contents of any oral, wire, or electronic communications. [34] Despite this seemingly broad prohibition, the ECPA contains a number of exceptions under which an employer may lawfully intercept or search employee communications. For instance, under the “service provider exception,” if the employer itself is providing the wire or electronic communications service – as many colleges and universities do – the employer may intercept communications sent over that service in the normal course of business in order to protect the employer’s rights or property. [35] Additionally, the “consent” exception permits an employer to lawfully intercept a communication where one of the parties to the communication has given consent. [36] Importantly, consent need not be express – it may be implied if the party knows there is a policy of monitoring or intercepting the communications at issue. [37] It should be noted that the Stored Communications Act [38] extends the reach of the ECPA to prohibit unauthorized access of any stored wire or electronic communications, including emails or voicemails. Like the ECPA, it is subject to the service provider and consent exceptions. [39]

There is a great deal of uncertainty as to how ECPA is applied in the context of technology-based privacy. One reason for the current disconnect between privacy expectations and the statutory protections of the ECPA is that the legislation was drafted in the early stages of internet and email technology that has fundamentally changed the way we communicate, store, and use information. The courts have thus been confounded by the ECPA, and because of broad exemptions contained in the ECPA and the SCA, commentators generally agree that the federal statutes are ineffective in providing employees with any privacy protections relative to work-related email messages and other forms of electronic communications. [40] In light of the uncertainty surrounding the ECPA and the SCA, it is imperative for an institution to create its own policy in order to minimize potential liability,
though with an understanding that employer policies cannot take precedence over ECPA requirements.

**III. State Constitutions and Statutes Affecting Privacy in the Workplace**

Many states also have provisions in their own constitutions and statutes that go beyond the protections of the Fourth Amendment. Indeed, some state constitutions expressly grant an individual right to privacy. For example, the Illinois Constitution provides: “The people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means.” California courts have held that the California constitution goes even further; creating an inalienable right to privacy that can be enforced against both government and private actors. Thus, it is possible that state courts could require employers to meet a higher standard for protecting an employee’s privacy under a state constitution than would be required under the Fourth Amendment.

Some states have also enacted statutes requiring notice of employer monitoring activities. For example, a Delaware statute provides that employers shall not monitor telephone, email, or internet usage unless notice is given to the employee every day that these resources are accessed, or the employee acknowledges such a policy. A similar Connecticut statute requires that employers provide notice of their monitoring policy “in a conspicuous place which is readily available for viewing by its employees.” In Illinois, public employers are subject to the Illinois Eavesdropping Act, which prohibits recording either private or public conversations without consent of all parties. It should be noted, though, that courts have held that employees “impliedly consent” to such monitoring if they are aware of an employer’s policy to monitor employee communications. Again, this demonstrates that employers need to adopt policies clarifying that the employer has a right to monitor employee emails, text messages, and internet usage on employer-owned devices.

**IV. Common Law Privacy Claims**

Beyond legislative and regulatory efforts, the common law provides a small amount of protection to employees against excessive monitoring. Even in states where there is no constitutional or statutory right to privacy, an employee may be able to sue his employer under a common law invasion of privacy theory, most likely unreasonable intrusion upon seclusion. According to the Restatement (Second) of Torts, “One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.” In order to intentionally intrude upon the seclusion of another, the employer must have "penetrated some zone of physical or sensory privacy . . . or obtained unwanted access to data" by electronic or other covert means, in violation of the law or social norms.

While employees may be able to find protection under the common law tort of “invasion of privacy” or “intrusion upon seclusion,” courts are in conflict about whether an employee has any reasonable expectation of privacy in electronic communications that are facilitated by use of their employer’s equipment. As with claims under the Fourth Amendment, courts considering common law invasion of privacy claims will typically weigh the interest of the employer in conducting the search against the employee’s privacy interests. Even if employees can establish a privacy expectation, they still may lose, in most cases, if the legitimate business interests of the employer outweigh their privacy interest.

On the whole, courts are less likely to find for the employee in these tort suits when the monitoring is conducted on or within employer property. And, just as a strong, clear technology monitoring policy
can diminish an employee’s legitimate expectation of privacy under the Fourth Amendment, it can also undercut an employee’s assertion that a search was “offensive to a reasonable person” under common law theories.

V. Open Records Laws Diminish Employee Expectations of Privacy

For public institutions, freedom of information laws can also diminish an employee’s privacy interest in information conveyed via employer-issued technology. The language of such laws varies by state but typically provides that public entities shall make their public records available to any person for inspection or copying, except where specifically exempted by law. [54] Such laws are grounded in the principle that the public should be able to access public records and information about the workings of their government. [55]

Importantly, most state freedom of information laws include exemptions for materials which, if released, would constitute an unwarranted invasion of privacy. Nonetheless, most documents created by a public employee for his or her own use may still constitute public records that the employer is obligated by freedom of information laws to preserve and disclose.

The Illinois Attorney General recently issued an opinion on this very issue, holding that electronic records relating to the transaction of government business are “public records” subject to disclosure under the Illinois Freedom of Information Act, even if the communication was generated on a public official’s personal electronic device or email account. [56] The request specifically sought “[a]ll electronic communications, including cell phone text messages, sent and received by members of the city council and the mayor during city council meetings and study sessions . . . .” [57] The requester clarified that his request applied to “city-issued and personal cell phones, city-issued or personal email addresses and Twitter accounts.” [58] In its opinion, the Attorney General explained that because the communications requested in the FOIA were “prepared by or used by one or more members of a public body in conducting the affairs of government,” they were subject to FOIA.

In view of this opinion and state freedom of information laws, it seems that when an employer specifies that communications using employer-issued technology are public records, subject to monitoring and auditing pursuant to freedom of information laws, the employee (or public official) cannot show that he or she expected the messages to be private or that society would treat as reasonable any such expectation.

VI. Practical Tips

In light of the foregoing, it is clear that while college and university employees may rightfully expect a certain degree of privacy in their communications and documents stored on employer-issued technology, institutions also have the right to limit those privacy expectations through policies and practices designed to effectively and efficiently manage the workplace. Colleges and universities should therefore consider the following practical tips:

1. Enact policies explicitly stating that (a) the institution reserves the right to monitor, inspect, or audit any communications made using employer-issued technology, or any data stored on such technology; (b) all such communications or data are property of the institution; and (c) the employee has no expectation of privacy in such communications or data.

2. Remember that vague, general, or unenforced policies may lead to employees having a greater expectation of privacy.
3. For public colleges and universities, provide notice that any and all communications made via employer-issued technology are subject to review according to state freedom of information laws.

4. Consider policies and procedures that prohibit university officials from conducting institutional business through personal electronic devices and email accounts.

5. Consider state as well as federal laws, recognizing that many state constitutions and statutes provide greater privacy protection than the U.S. Constitution and federal law.

6. Remember that even with a clear policy, searches cannot be unreasonable. Thus, when conducting searches, audits, or monitoring activities, identify the work-related reason for the search, and tailor the scope of the search to that reason, to avoid unnecessary litigation.

7. In the event criminal wrongdoing is suspected, forward the matter to the campus or local law enforcement so that a warrant can be obtained to conduct a search.

CONCLUSION:

The Supreme Court has made clear that employee expectations of privacy will differ in significant ways depending on the specific case and workplace involved. The underlying premise of O'Connor and, more recently, Quon is that both public and private colleges and universities must be clear and consistent with policies concerning privacy and the acceptable use of employer-issued technology. By establishing such policies in compliance with state and federal law, the employer eliminates any subjective expectation of privacy that conflicts with those terms.

FOOTNOTES:


FN2. See id. at 723 ("[T]he governmental interest justifying work-related intrusions by public employers is the efficient and proper operation of the workplace.").

FN3. Employer-issued technology is referred to broadly, as there are several technological modes employees use to communicate and to perform employment responsibilities. Examples of employer-issued technology include, but are not limited to, smartphones, cell phones, computers, laptops, pagers, or tablets.

FN4. United States v. Van Leeuwen, 397 U.S. 249, 251 (1970) (letters and packages are "free from inspection by postal authorities"); United States v. Hernandez, 313 F.3d 1206, 1209 (9th Cir. 2002) ("It has long been established that an addressee has both a possessory and a privacy interest in a
mailed package.

FN5.
See O’Connor, 480 U.S. at 715.

FN6.
Id. at 714 (“The strictures of the Fourth Amendment . . . have been applied to the conduct of government officials in various civil activities. Thus, we have held in the past that the Fourth Amendment governs the conduct of school officials. . . .”) (citing New Jersey v. T.L.O., 469 U.S. 325 (1985)). Counsel for private institutions will nonetheless benefit from this discussion, as courts often look to Fourth Amendment analysis when adjudicating state constitutional or common law privacy claims.

FN7.
Id. at 719-20 (“In the case of searches conducted by a public employer, we must balance the invasion of the employees’ legitimate expectations of privacy against the government’s need for supervision, control and the efficient operation of the workplace.”); Jill L. Rosenberg, Is Big Brother Watching: Monitoring Employee Communications and Employee Privacy, Practising Law Institute Litigation and Administrative Practice Course Handbook Series – Employment Discrimination Law and Litigation (2011), at 423.

FN8.
O’Connor, 480 U.S. at 717.

FN9.
Id. at 719-20.

FN10.
See id. at 717-19.

FN11.
Id. at 717.

FN12.
Id. at 730.

FN13.
130 S.Ct. 2619 (2010).

FN14.
Id.

FN15.
Id. at 2629.

FN16.
Id. at 2628-29.

FN17.
Id. at 2632.

FN18.
Id. at 2630.
FN19.
O’Connor, 480 U.S. at 717.

FN20.
Many states have statutes that affect an employer’s right to monitor the workplace. See ARIZ. REV. STAT. ANN. § 13-3012; CAL. PENAL CODE § 632; COLO. REV. STAT. § 18-9-305; DEL. CODE ANN. 11, § 1336; D.C. CODE ANN. § 23-542; FLA. STAT. CH. 934.03; GA. CODE ANN. § 16-11-66; HAW. REV. STAT § 803-42; IDAHO CODE §§ 18-6702, 18-6720; IL. 720 ILCS 5/14 and 5 ILCS 430; IOWA CODE ANN. § 8082.B; KAN. STAT. ANN § 210-4001; S 22-2514; LA. REV. STAT. ANN § 15:1303; MD. CODE ANN. CTS. & JUD. PROC. § 10-402; MINN. STAT. § 626A.02; MISS. CODE ANN. § 41-29-531; MO. ANN. STAT. § 542.402; NEB. REV. STAT. § 86-702; NEV. REV. STAT. § 200.620; N.H. REV. STAT. ANN. §§ 570-B:3; 570-A:2; N.J. REV. STAT. § 2A:156A-4; N.M. STAT. ANN. § 30-12-1; N.D. CENT. CODE § 12.1-15-02; OHIO REV. CODE ANN. § 2933.52; OKLA. STAT. TIT. 13, § 176.4; OR. REV. STAT. § 165.543; PA. CONS. STAT. ANN. § 5704; R.I. GEN. LAWS § 11-35-21; TEX. PENAL CODE § 16.02; UTAH CODE ANN. § 77-023A-4; VA. CODE ANN. § 19.2-62; W. VA. CODE § 62-1D-3; WIS. STAT. § 968.31; WYO. STAT. § 7-3-602.

FN21.
Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001). Notably the search was still held to be reasonable.

FN22.
Stengart v. Loving Care Agency, 990 A.2d 650 (2010). Note that this case involved a common law invasion of privacy tort, as opposed to a Fourth Amendment claim, but the Court admittedly undertook an analysis similar to that of a Fourth Amendment case.

FN23.
Id.

FN24.
Id. By contrast, where the employer’s policy clearly prohibits personal use, this “no personal use” policy combined with a policy allowing for employer monitoring and the employee’s knowledge of these two policies diminishes any expectation of confidentiality,” even in communications with one’s attorney. Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436 (2007).

FN25.
See also U.S. v. Ziegler, 456 F.3d 1138, 1144 (9th Cir. 2006); United States v. Thorn, 375 F.3d 679, 682 (8th Cir. 2004).

FN26.
206 F.3d 392 (4th Cir. 2000).

FN27.
Id. at 398.

FN28.
419 F.3d 845 (8th Cir. 2005).

FN29.
Id. at 850.

FN30.
Id. at 847.

FN31.
Id. at 851.

FN32.
United States v. Angevine, 281 F.3d 1130 (10th Cir. 2002).

FN33.
Id. at 1132.

FN34.
See 18 U.S.C. §§ 2510-22; 2701.

FN35.
See 18 U.S.C. § 2511(2)(a)(i); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114-15 (3d Cir. 2003) (finding that company’s search of employee’s email was valid under the “service provider exception” because the email was stored on Nationwide’s system).

FN36.

FN37.
See, e.g., United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987); Rosenberg supra, n.7 at 442.

FN38.

FN39.
See 18 U.S.C. § 2701(c).

FN40.

FN41.

FN42.
See, e.g., ALASKA CONST. art. I, Sec. 22; ARIZONA CONST. art. II, Sec. 8; CALIFORNIA CONST. art. I, Sec. 1; FLORIDA CONST. art. I, Sec. 23; HAWAII CONST. art. I, Sec. 6; ILLINOIS CONST. art. I, Sec. 6; LOUISIANA CONST. art. I, Sec. 5; MONTANA CONST. art. II, Sec. 10; SOUTH CAROLINA CONST. art. I, Sec. 10; WASHINGTON, CONST. art. I, Sec. 7.

FN43.
ILLINOIS CONST. art. I.

FN44.
See CAL. CONST. art 1, § I (“All 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”); see also Hill v. Natl. Collegiate Athletic Assn., 7 Cal. 4th 1 (1994) (“[T]he Privacy Initiative in article I, section 1 of the California Constitution creates a right of action against private as well as government entities.”); Porten v. Univ. of San Francisco, 64 Cal. App. 3d 825, 829 (1976) (“Privacy is protected not merely against state action; it is considered an inalienable right which may not be violated by anyone.”).

FN46.

FN47.
720 ILCS § 5/14-1(a).

FN48.
See Shefts v. Petrakis, 758 F.Supp.2d 620 (7th Cir. 2010) (holding that employer did not violate the Illinois Eavesdropping Act by monitoring employee’s emails and text messages contained on employer-owned devices, because employee impliedly consented to monitoring by being well aware of employer’s policy regarding the monitoring of such communications).

FN49.
See Rosenberg supra., n.7, at 459 (citing RESTATEMENT 2d OF TORTS § 652A). Other possibilities include: appropriation of name or likeness, public disclosure of private facts, or public portrayal in a false light.

FN50.
Rest. 2d of Torts § 652B.

FN51.

FN52.
The Fourth, Seventh and Tenth Circuits have held that defendants have no reasonable expectation of privacy in their work computers in light of the employer’s computer use policy. See United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000); Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002); United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002). But the Second and Fifth Circuits have held on particular sets of facts that employees did have a reasonable expectation of privacy in their office computers. See Leventhal v. Knapek, 266 F.3d 64, 73 (2nd Cir. 2001); United States v. Slanina, 283 F.3d 670, 676 (5th Cir. 2002), vacated, 537 U.S. 802 (2002).

FN53.
See, e.g., Holmes v. Petrovich Development Co., LLC, 191 Cal.App.4th 1047, 1069 (2011) (concluding that an employee had no reasonable expectation of privacy in her personal email messages sent to her attorney using her employer’s computer and consequently could not prevail on an invasion of privacy claim); TBG Ins. Services Corp. v. Superior Court, 96 Cal.App.4th 443, 452 (2002) (“[U]se of computers in the employment context carries with it social norms that effectively diminish the employee’s reasonable expectation of privacy with regard to his use of his employer’s computers.”).

FN54.
See, e.g., the California Public Records Act, Cal. Gov’t Code § 6253(b) (“Except with respect to public records exempt from disclosure by express provisions of law, each state or local agency, upon a request for a copy of records that reasonably describes an identifiable record or records, shall make the records promptly available to any person upon payment of fees covering direct costs of duplication, or a statutory fee if applicable. Upon request, an exact copy shall be provided unless impracticable to do so.”).

FN55.
AUTHOR:

Jeffrey M. Brown, former University Counsel, Northeastern Illinois University.

Until May, 2012, Jeffrey M. Brown served as University Counsel for Northeastern Illinois University as well as its Ethics and FOIA Officer. He joined Northeastern in 2004 and was promoted in 2008 to be the chief legal officer for the University. As University Counsel, Mr. Brown was responsible for managing all of Northeastern's legal affairs and representing the University in traditional labor matters. Mr. Brown has also dedicated significant time and effort to pro bono appellate projects in state and federal court, including arguing a case of first impression regarding wiretapping before the Illinois Supreme Court. Mr. Brown presently serves as the Associate Chief Labor Counsel for the City of Chicago. In this capacity, he serves on the City's bargaining team that negotiates contracts with over forty labor unions and manages all of the City's litigation in traditional labor matters. He also acts as lead counsel in many of the City's important and complex cases before the Illinois Labor Relations Board and in state court. Mr. Brown is a graduate of James Madison College at Michigan State University and the John Marshall Law School in Chicago, Illinois and is licensed to practice law before the Illinois Supreme Court, the Northern District of Illinois and its Trial Bar, the United States Court of Appeals for the sixth and Seventh Circuits, as well as the United States Supreme Court.

RESOURCES:


- Jill L. Rosenberg, Is Big Brother Watching: Monitoring Employee Communications and Employee Privacy, Practising Law Institute, PLI Order No. 29714 (2011).

"To advance the effective practice of higher education attorneys for the benefit of the colleges and universities they serve."