Ten Tips for Preparing an Effective Acceptable Use Policy

By Philip L. Gordon, Esq., Littler Mendelson, P.C.

September 2014

IMPORTANT NOTICE

This publication is not a do-it-yourself guide to resolving employment disputes or handling employment litigation. Nonetheless, employers involved in ongoing disputes and litigation will find the information extremely useful in understanding the issues raised and their legal context. The Report is not a substitute for experienced legal counsel and does not provide legal advice or attempt to address the numerous factual issues that inevitably arise in any employment-related dispute.

PHILIP L. GORDON, ESQ.

Philip L. Gordon is a shareholder in the Denver office of Littler Mendelson, P.C., the nation's largest law firm representing only management in employment and labor law matters. He co-chairs the Firm's Privacy and Background Check Practice Group. Mr. Gordon regularly counsels clients on the full range of workplace privacy and data protection issues, including the monitoring of employees' electronic communications and social media activity; background checks; "Bring Your Own Device" programs; location tracking; compliance with HIPAA and other federal, state and international data protection laws; and security incident preparedness and response.

Mr. Gordon sits on the Advisory Board of BNA's *Privacy and Security Law Report* and has served on the Editorial Board and Educational Advisory Board of the International Association of Privacy Professionals. He also has taught privacy law as an adjunct professor at the University of Colorado Law School. Mr. Gordon is the principal author of Littler's Workplace Privacy Blog, which is located at www.littler.com/blog/workplace-privacy-counsel. He is a graduate of Princeton University and New York University School of Law. After law school, he served as a judicial clerk on the United States Court of Appeals for the Tent Circuit. Mr. Gordon can be contacted at pgordon@littler.com or at (303)-362-2858.

Corporate computers and information and communications systems (collectively, "electronic resources") remain the workhorse for most businesses, even as alternatives, such as third-party text messaging services, external social media, and cloud computing, flourish. Employees rely on corporate electronic resources for e-mail, calendaring, business contacts, Internet access, document creation and storage, and a multitude of other business applications. Consequently, for employers, it is critical to establish and maintain their right to inspect all information stored on, and to monitor all communications transmitted by, corporate electronic resources. The corporate acceptable use policy is the linchpin of that effort.

Preparing an effective acceptable use policy is far more challenging today than it was just a few years ago. Simply invoking the mantra, "employees have no expectation of privacy," as some employers have done in the past, will not suffice. Recent technology developments, new laws and regulations, and novel judicial precedent have exposed employers to litigation for inspecting information stored on, and monitoring communications transmitted by, *their own* electronic resources.

The ten tips below are intended to aid employers who either want to implement an acceptable use policy for the first time, or who need to update their policy. These ten tips are not a comprehensive list of every point that should be addressed in an acceptable use policy. Rather, they are designed to help employers avoid some common pitfalls.

1. **Define The Policy's Scope.** An acceptable use policy should inform employees at the outset of the systems, devices, information, and communications that fall within the policy's scope. Given the proliferation of corporate computing and communications platforms, an employer may need to conduct a careful inventory to confirm that the policy's scope has been comprehensively defined. Systems that might be overlooked include, for example, corporate text messaging, voice-mail, internal social media platforms, and corporate cloud computing accounts.

2. **Analyze The Policy's Application To Personal Devices.** As employees increasingly turn to personal mobile devices to conduct their employers' business, employers need to carefully consider whether they can effectively incorporate those devices into an acceptable use policy, or whether they should address them in a separate policy. Personal devices raise two distinct challenges for employers. First, because employees own the devices, employers cannot access them without the employee's consent and, relatedly, employees generally do have a reasonable expectation of privacy in their personal device vis-à-vis the employer. [1] Second, information stored on, and communications transmitted by, a personal device generally do not "touch" corporate electronic resources unless the employer and employee make configuration adjustments to permit interconnection. Employers can condition such configuration adjustments on the employee's consent to inspection and monitoring of the personal device as described in the acceptable use policy. Even then, a separate policy may still be necessary to address personal devices. For example, a bring-your-own-device (BYOD) policy typically addresses issues that do not fit in a corporate acceptable use policy, such as reimbursement of expenses associated with the personal device, servicing of the personal device by third parties, and the employer's installation of security controls on the personal device.

3. **Establish The Business Purpose For Providing Corporate Electronic Resources.** An acceptable use policy should inform employees that the employer is providing the electronic resources only to advance the employer's business interests. When employees use corporate electronic resources, they must conduct themselves in an ethical and lawful manner and in accordance with all relevant company policies. The acceptable use policy should also notify employees that they are responsible for their use of electronic resources and will be held accountable for all use of their corporate

1 *See, e.g., Riley v. California,* 134 S. Ct. 2473, 2494-95 (2014) ("Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'").

account. Finally, employees should be reminded to compose communications transmitted by corporate electronic resources with the same formality and professionalism that they apply to any other form of business communication.

4. **Define The Permissible Parameters For Non-Business Use.** Because prohibitions against non-business use of corporate electronic resources will virtually always be honored in the breach, employers generally are better off establishing specific rules for non-business use of those resources. These rules can include the following: (a) non-business use must be limited and cannot interfere with anyone's productivity; (b) non-business use is *not* private and *is* subject to monitoring; (c) non-business use must comply with all relevant company policies; and (d) any non-business information will be deleted from corporate electronic resources at any time in the employer's discretion. Employers also should consider addressing whether employees may access personal social media using corporate electronic resources and, if permitted, refer them to the corporate social media policy for more detail.

5. **Preserve The Company's Right To Inspect And Monitor.** Under U.S law, employers generally are presumed to have the right to inspect all information stored on, and to monitor all communications transmitted by, their own corporate resources. [2] The acceptable use policy should unequivocally express the employer's intention to exercise those rights by stating that (1) all information stored on, and communications transmitted by, corporate electronic resources are the employer's property; (2) employees should not expect any information or communication to be private vis-à-vis the employer; (3) the employer will, in its discretion, inspect any information stored on, and monitor any communication transmitted by, corporate electronic resources; and (4) neither the employer's failure to exercise its rights with respect to any information or communication nor any statement by any employee (except a written statement by a designated senior executive) modifies these rights in any way.

6. **Provide Specific Notice Of Any Real-Time Monitoring.** Employers should carefully select monitoring technology and fully understand its capabilities before implementing it. Employers generally have the right under federal and state anti-wiretap laws to review any information in storage on their own electronic resources. However, when the monitoring technology effectuates an "interception" of an electronic communication, such as e-mail, i.e., acquires the content of the communication in transit, anti-wiretap laws may apply. [3] By way of illustration, one appellate court has held that activating an e-mail auto-forwarding feature, without the intended recipient's consent, to forward a duplicate copy of e-mail to someone other than the intended recipient results in an interception in violation of federal anti-wiretap law.[4] Such monitoring would be lawful in most states with the prior informed consent of at least one party to the communication, and in a minority of states, with the prior consent of all parties to the communication. Because the wiretap laws are highly technical criminal statutes and often permit recovery of civil damages, employers should consider implementing only monitoring technology that does not intercept electronic communications in real time, or if there is a business need for real-time monitoring, consulting legal counsel before implementing the technology. Legal counsel can work with the employer to develop language for inclusion in the acceptable use policy and in the disclaimer commonly placed at the end of sent e-mail and also to prepare other notices that can be used to obtain consent of employees and other individuals subject to real-time monitoring.

7. **Analyze The Application Of Non-U.S. Privacy Laws.** Technology has made it easier for small and mid-sized businesses to employ personnel outside the U.S. These non-U.S. employees may have very different expectations and more legal

2 18 U.S.C. § 2701(c)(1); *Fraser v. Nationwide Mut. Ins. Co.,* 352 F.3d 107, 114-15 (3rd Cir. 2003) (holding that the plaintiff's employer did not violate the Stored Communications Act by accessing the plaintiff's stored e-mail messages because the e-mails were stored in the employer's own e-mail system).

3 18 U.S.C. § 2511(2)(c).

4 *U.S. v. Szymuszkiewicz*, 622 F. 3d 701, 707 (7th Cir. 2010) (holding that an employee violated the Federal Wiretap Act by autoforwarding his supervisor's e-mails to himself without the supervisor's consent).

rights regarding their use of corporate electronic resources. In France, for example, employees have the right to use their employers' electronic resources for private and personal communications in certain circumstances *regardless* of what the employer states in its acceptable use policy.[5] Consequently, U.S. employers who use monitoring technology outside the U.S. may need to modify certain provisions of their U.S.-centric acceptable use policy before implementing it in a foreign country.

8. **Prohibited Conduct.** The acceptable use policy should include a non-exclusive list of prohibited conduct. The types of conduct commonly included on this list include the following: (a) unauthorized access to, and disclosure of, confidential business information; (b) discrimination or harassment based on any legally protected characteristic; (c) viewing sexually explicit material; (d) unauthorized downloading of software or copyrighted material; (e) sending or receiving malicious code; (f) falsifying identity by using another employee's e-mail account; (g) using peer-to-peer file-sharing software; (h) sending bulk or chain e-mail; and (i) game playing and gambling.

9. **Restrictions On Solicitations.** The National Labor Relations Board (NLRB) currently is considering a case that could have a substantial impact on employers' ability to prevent employees from using corporate electronic resources to engage in union organizing and other protected labor activity.[6] Under current law, employers cannot specifically prohibit use of their electronic resources for union organizing or other protected labor activities, but they can establish broad restrictions on solicitation that have the incidental effect of restricting union-related activities.[7] For example, employers can prohibit employees from using corporate electronic resources to solicit for, or engage in other activities on behalf of, any outside business venture, political campaign, religious group, or membership organization. Employers who choose to take an approach like this one are required to enforce the policy in a way that does not discriminate against union and other protected labor activity.

10. **Refer To The Acceptable Use Policy In A Log-In Banner.** The acceptable use policy is designed to notify employees and other users of corporate electronic resources of the "rules of the road" when using corporate electronic resources. Employers can use a log-in banner to increase awareness of the policy. A log-in banner is a message that appears each time a user logs into the corporate network that briefly summarizes the key elements of the acceptable use policy and provides a link to that policy for additional information.

CONCLUSION

Employers should strongly consider implementing an acceptable use policy or updating one that currently is in effect. The policy's principal objective should be to inform employees up front about the employer's expectations for their use of corporate electronic resources and about the employer's ability through the use of monitoring technology and otherwise to enforce those expectations. In addition, a carefully drafted and thorough acceptable use policy can serve as a defense when an employer's conduct with respect to its own electronic resources is challenged. Employers should keep in mind that rapid changes in user and monitoring technology and an evolving legal framework mean that the acceptable use policy should be revisited at least annually to confirm that it is accurate, comprehensive and adequately addresses recent developments.

5 *GAN Assurance IARD v. M.X.*, Case No. 10-17284 (2011) (holding that the employer could access but not rely on an "intimate" e-mail between a manager and another employee with whom he was having an affair for making an employment decision).

6 *Purple Commc'ns, Inc.*, Case Nos. 21-CA-095151, 21-RC-091531, 21-RC-091584 (Nov. 21, 2013).

7 *Register Guard*, 351 NLRB 1110, 1114 (2007).

Littler U.S. Office Locations

Albuquerque, NM
505.244.3115

Anchorage, AK
907.561.1214

Atlanta, GA
404.233.0330

Birmingham, AL
205.421.4700

Boston, MA
617.378.6000

Charlotte, NC
704.972.7000

Chicago, IL
312.372.5520

Cleveland, OH
216.696.7600

Columbia, SC
803.231.2500

Columbus, OH
614.463.4201

Dallas, TX
214.880.8100

Denver, CO
303.629.6200

Detroit, MI*
313.446.6400

Fresno, CA
559.244.7500

Gulf Coast
251.432.2477

Houston, TX
713.951.9400

Indianapolis, IN
317.287.3600

Kansas City, MO
816.627.4400

Las Vegas, NV
702.862.8800

Lexington, KY*
859.317.7970

Long Island, NY
631.247.4700

Los Angeles, CA
Downtown
213.443.4300

Los Angeles, CA
Century City
310.553.0308

Memphis, TN
901.795.6695

Miami, FL
305.400.7500

Milwaukee, WI
414.291.5536

Minneapolis, MN
612.630.1000

Morgantown, WV
304.599.4600

Nashville, TN
615.383.3033

New Haven, CT
203.974.8700

New York, NY
212.583.9600

Newark, NJ
973.848.4700

Northern Virginia
703.442.8425

Northwest Arkansas
479.582.6100

Orange County, CA
949.705.3000

Orlando, FL
407.393.2900

Overland Park, KS
913.814.3888

Philadelphia, PA
267.402.3000

Phoenix, AZ
602.474.3600

Pittsburgh, PA
412.201.7600

Portland, OR
503.221.0309

Providence, RI
401.824.2500

Reno, NV
775.348.4888

Rochester, NY
585.203.3400

Sacramento, CA
916.830.7200

San Diego, CA
619.232.0441

San Francisco, CA
415.433.1940

San Jose, CA
408.998.4150

San Juan, PR
787.765.4646

Santa Maria, CA
805.934.5770

Seattle, WA
206.623.3300

St. Louis, MO
314.659.2000

Walnut Creek, CA
925.932.2468

Washington, D.C.
202.842.3400

*In Detroit, Littler Mendelson, PLC and in Lexington, Littler Mendelson, P.S.C., both are wholly-owned subsidiaries of Littler Mendelson, P.C.

SpectorSoft Locations

Corporate Offices

SpectorSoft Corporation
1555 Indian River Drive
Vero Beach, FL 32960
1.888.598.2788
Toll Free Phone/Support 24/71.772.770.5670

West Palm Beach
1555 Palm Beach Lakes Blvd.
West Palm Beach, FL 33401

International

United Kingdom
C2, Dukes Street
Woking
Surrey, GU21 5BH
+44 1483 397744

Littler Global Office Locations

Barranquilla, Colombia
57.5.385.6071

Bogotá, Colombia
57.1.317.4628

San José, Costa Rica
506.2545.3600

Santo Domingo, Dominican Republic
809.472.4202

San Salvador, El Salvador
503.2206.9642

San Pedro Sula, Honduras
504.2516.1133

Mexico City, Mexico
52.55.5955.4500

Monterrey, Mexico
52.81.8851.1200

Panama City, Panama
507.830.6552

Caracas, Venezuela
58.212.610.5450

Valencia, Venezuela
58.241.824.4322