Electronic Communications:
E-Mail, Voicemail, Telephones, Internet and Computers

Key Points

- Put employees on notice through policies that they should have no expectation of privacy arising from their use of employer-owned/supplied communication devices, including: e-mail, voicemail, telephones, Internet and computers.

- As with Solicitation and Distribution policies, uniform application and enforcement is key.

Electronic Communications Generally

Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510-22,2701-11.

- Title I, 18 U.S.C. §§ 2510-12, ("Wiretap Act"): prohibits unauthorized and intentional "interception" of wire, oral and electronic communication. 18 U.S.C. § 2511. Definition of wire communications includes telephone calls and voice mail. Briggs v. American Air Filter Co.., 630 F.2d 414 (5th Cir. 1980). Definition of electronic communication includes e-mail. 18 U.S.C. § 2510(12).

- Title II, 18 U.S.C. §§ 2701-11, ("Stored Communications Act"): prohibits unauthorized accessing of electronically stored communications.

  Exceptions:

  "System Provider" – applies to entities that provide wire or electronic communication service. Courts generally hold that employer qualifies as a "system provider" with respect to its internal e-mail and voice mail systems. Courts are divided as to whether this exception allows employers to monitor employee use of e-mail on external servers (e.g., Hotmail, Gmail) accessed on employer's computers.

  One-Party Consent – interception permissible where only one of the parties to communication offers consent. ***Consent can be express or implied***. Implied consent is narrowly construed. Blumofe v. Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003). Consent is not judged by what a reasonable employee "should have known" concerning employer's monitoring practices, but rather is based upon notice actually provided by

employer to employee. Griggs-Ryan v. Smith, 904 F.2d 112, 116-17 (1st Cir. 1990).

Business Use – to extent employer qualifies as "supplier" and is "acting in the ordinary course of business," employer monitoring of business calls may be permissible. Some courts have supported this proposition. Most all courts are in agreement that personal calls do not fall within "ordinary course of business." Application to voice mail and e-mail is uncertain.

Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030

- Statute of broad application with criminal and civil penalties (including private right of action) where individuals access and/or destroy data without authorization.

- Limited success to date applying CFAA to employer claims against employees for computer-related misconduct.

E-Mail

Massachusetts General Laws, Ch. 214, Section 1B:

"A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages."

- Balance between employer's legitimate business interests and employee's reasonable expectation of privacy.

- Trial court in Massachusetts held that employees may have an expectation of privacy in e-mail communications under this statute, in absence of explicit policy by employer putting employees on notice of e-mail monitoring. See Restuccia, et. al. v. Burke Technology, Inc., Middlesex Superior Court, C.A. No. 95-2125, 1996 WL 1329386 (August 13, 1996). (Jury later determined that employer did not breach statute, where it put forward evidence that employer's e-mail monitoring practices were "common knowledge" and that e-mails in question were reviewed for productivity purposes. See Restuccia, et. al. v. Burke Technology, Inc., Middlesex Superior Court, C.A. No. 95-2125 (November 22, 1999), 28 M.L.W. 1078 (Jan. 17, 2000).

- U.S. District Court in Massachusetts held that employees terminated for receiving sexually explicit e-mail did not have causes of action for invasion of privacy, unlawful interception of wire communications or

other claims. Employer had explicit policy, reminded employees of policy, and notified employees of periodic situations in which other employees were disciplined under the policy. Court found no reasonable expectation of privacy by employees. Court also noted that even if reasonable expectation were established, employer's obligations to prevent workplace harassment under federal and state anti-discrimination statutes would likely trump such privacy rights. See Garrity v. John Hancock Mutual Life Ins. Co., No. 00-12143-RWZ (D.Mass. 2002).

National Labor Relations Act

- Evolving area of the law.

- NLRB has recently held that employees do not possess a statutory right to use employer's e-mail system for Section 7 purposes. "The [Employer's] communications system, including its e-mail system, is the [Employer's] property, and was purchased by the [Employer] for use in operating its business." Guard Publishing Co., 351 NLRB 1110, 1114 (December 16, 2007), enf. granted in part, denied in part 571 F.3d 53 (2009).

- Employer policy prohibiting use of e-mail system for "non job-related solicitations" is facially valid. Id.

- Employee use of employer-provided e-mail system for union-related activity will be scrutinized for discriminatory application as with alleged violation of non-solicitation/distribution policies. Board adopts new test that "unlawful discrimination consists of disparate treatment of activities or communications of a similar character because of their union or other Section 7-protected status." Id at 1118. Board notes:

> an employer clearly would violate the Act if it permitted employees to use e-mail to solicit for one union but not another, or if it permitted solicitation by antiunion employees but not by prounion employees. In either case, the employer has drawn a line between permitted and prohibited activities on Section 7 grounds. However, nothing in the Act prohibits an employer from drawing lines on a non-Section 7 basis. That is, an employer may draw a line between charitable solicitations and non-charitable solicitations, between solicitations of a personal nature (e.g., a car for sale) and solicitations for the commercial sale of a product (e.g., Avon products), between invitations for an organization and invitations of a personal nature, between solicitations and mere talk, and between business-related use and non-business-related use. Id.

- NLRB found discriminatory enforcement by the Employer with respect to one out of three e-mails in question. The Board majority found that the Employer permissibly disciplined employees for two e-mails that the Employer deemed group "solicitations" prohibited by its computer use policy. Notably, the U.S. Court of Appeals reached a contrary result finding, based upon the facts of the case, that the Employer's discipline of employees for sending all three e-mails constituted discriminatory enforcement because the Employer's policy made no distinction concerning the "organizational status" of-mail usage. See Guard Publishing v. NLRB, 571 F.3d 53 (D.C. Cir. 2009).

- This case demonstrates that, as with solicitation, distribution and bulletin board cases, the issue is one of uniform application of a facially permissible policy. Changes to policy or enforcement of existing policy in the face of union activity will likely result in finding of unfair labor practice.

Blogs

Section 230, Communications Decency Act (CDA), 47 U.S.C. § 230

- Broadly immunizes website owners ("service providers") from liability based on content posted by third parties.

- Evolving case law in situations where employees create/maintain blogs discussing workplace.

Screen Savers

- Screen savers bearing union messages may constitute protected activity, in face of discriminatory enforcement by employer. See St. Joseph's Hospital, 337 NLRB No. 12 (2001) (Board draws analogy between screen saver and traditional bulletin board).

Telephones

Federal Wiretap Act, 18 U.S.C. §§ 2510-22: generally makes it unlawful for any person to intentionally intercept any wire, oral, or electronic communication. 18 U.S.C. §§ 2511. Employer may monitor phone or oral communications with employee's consent. 18 U.S.C. §§ 2511 (c), (d).

- Some court decisions have allowed employers to monitor/record employee phone calls, made in ordinary course of business, via a phone extension where "legitimate business interests" are present. Such interests have included concerns about dissemination of confidential/proprietary information and maintaining records of emergency calls.

M.G.L. c. 272, s. 99: precludes interception of oral or wire communications without the consent of all parties to the communication. Limited development under case law, but see Garrity, supra., where U.S. District Court imposed narrow definition of term "intercept" and found statute inapplicable to received e-mails. Mass. Wiretap Act applies to e-mail interception, and does contain "service provider" exception allowing employer to monitor its own systems in "ordinary course of business."

Text Messages

- Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008), cert. granted sub. nom. Ontario, California v. Quon, U.S. No. 08-1332 (12/14/09)

- U.S. Supreme Court to consider whether: (1) police department search of personal text messages sent and received by police lieutenant on department-owned pager violates Fourth Amendment (search and seizure); and (2) whether wireless provider violated Stored Communications Act (SCA) by providing city with transcripts of text messages.

- Public sector case – applicability to private sector is open question

- Police Department did not have policy specific to text messaging, but did have comprehensive policy warning that use of e-mail and computers was not confidential, could be monitored and that all website access would be recorded and periodically reviewed.

Developing Policies: Internet Usage and E-Mail

- Spectrum ranging from "business purposes only" to full usage for personal purposes

- Many employers develop policy detailing that Internet / e-mail are primarily for business purposes, but permit "incidental" personal use on non-working time that does not involve illegal or potentially offensive/harassing conduct.

- Uniform enforcement is key

Developing Policies: Monitoring Electronic Communications

- Explicit notice to employees is key – no expectation of privacy in any communications made, transmitted, or received on employer-provided electronic equipment.
- Employer-owned equipment vs. non-employer-owned equipment
- Ensure compliance with applicable law (e.g., Mass. Wiretap Act)
- Uniform enforcement is key (e.g., Section 7)

543807v1