Tuesday, October 21
4:30 pm-6:00 pm

711 We've Got An Eye On You: Employee Monitoring & Communications, Privacy, and Data Security

Julienne Bramesco
General Counsel
Colonial Parking, Inc.

Jonathan Spencer
Vice President, General Counsel, and Secretary
Shentel

Elizabeth Stivers
Assistant Vice President and Senior Counsel
Unum Group

Faculty Biographies

Julienne W. Bramesco

Julienne W. Bramesco is the vice president and general counsel for Colonial Parking Inc. in Washington, DC, where she advises the company on all legal matters related to the business, including real estate, labor and employment, and corporate governance and compliance.

Prior to joining Colonial Parking Inc., Ms. Bramesco served as associate general counsel for the ACC. She has also practiced labor and employment law in the corporate legal departments of Marriott International and Kaiser Permanente.

Ms. Bramesco has been a speaker at a number of conferences including ACC's CCU and Annual Meeting programs, and The Georgetown University Law Center Corporate Counsel Institute, where she is a member of the advisory board. She was previously a member of the DC Bar committee on continuing legal education during which time she created the education program titled "The ABC's of the NLRB," which she continues to chair. Ms. Bramesco is the author of "Is Green the New Black?" published in the October 2007 ACC Docket, and is also the co-author of "The Firing Line," published in the ACC Docket in September 2005.

Ms. Bramesco received a BA from the School of Industrial and Labor Relations at Cornell University, and is a graduate of Georgetown University Law Center.

Jonathan R. Spencer

Jonathan R. Spencer is vice president, general counsel, and corporate secretary at Shentel in Edinburg, VA, where he manages all legal issues related to the company and its subsidiaries. Mr. Spencer has 20 years of legal experience, both in private practice and as vice president and associate general counsel for Cable & Wireless.

Mr. Spencer has spoken and written on a wide range of topics relating to information technology, cyber law, employee monitoring, and privacy as well as working in-house. Mr. Spencer is also a former chair of the ACC's Information Technology and E-commerce Law Committee.

Mr. Spencer received an AB from Brown University and is a graduate of Duke University School of Law.

Elizabeth W. Stivers

Elizabeth W. Stivers is assistant vice president and senior counsel for Unum Group, working from the company's Portland, ME office. Unum is a leader in providing employee benefits (including disability, long term care, life, and voluntary benefits) for over 9,000 employees. Ms. Stivers advises on employment law matters including recording and monitoring, privacy, employee relations, ADA/FMLA/WC interplay and compliance, contracts, and benefits. She also oversees litigation involving employment matters.

Prior to joining Unum, Ms. Stivers had a judicial clerkship and was then in private practice for 16 years. Her practice included workers compensation, employment law, and general civil litigation.

Ms. Stivers has spoken at conferences on workers compensation, FMLA, and other employment issues. She has served on the board of governors of the Maine Trial Lawyers Association and is an active member of the ACC. Ms. Stivers' various charitable interests include Friends of Kakamega in Kenya and Maine Coastal Workshop.

Ms. Stivers received her BA from Colby College, studying her junior year in Paris at the Institute of European Studies, Paris IV (the Sorbonne), and l'Institut Catholique. She is a graduate of Franklin Pierce Law Center, where she won the Giles Sutherland Moot Court competition.

EMERGING TRENDS IN EMPLOYER MONITORING OF EMPLOYEE COMMUNICATIONS AND MOVEMENT

by
Joseph J. Lazzarotti[1]

Advances in technology are vastly expanding society's capabilities, connectivity and productivity in ways that can be enormously beneficial, but at the same time, uncomfortably intrusive. This is particularly true of technologies that permit one to monitor the communications and movements of others. As a group, employers are increasingly attracted to monitoring advancements and the advantages technology provides. However, many employers are unaware of the legal issues and pitfalls, many of which are just now emerging.

Consider some of the following recent applications of monitoring technologies:

- A school in Rhode Island announced that it will be implanting radio frequency identification (RFID) chips into the school bags of students in order to monitor their movement while in transit on the school bus. The RFID chips, together with global positioning system (GPS) equipment on the school bus, would enable school officials and parents to track the children's movement by accessing a school website.[2]

- Cities such as Washington, D.C., New York, and London have reputations for being monitored continuously by thousands of cameras.[3] However, because of the work of researchers from the University of Portsmouth, these cameras and others may soon be equipped with artificial intelligence software to allow CCTV cameras fitted with microphones to recognize sounds such as crowd noise and windows smashing.[4]

- The vast amount of information about persons and their relationships maintained by networking websites such as Facebook can be used to provide a wealth of information about a person, including those with whom the person associates and photographs (particularly when combined with technology that can perform facial recognition).[5]

- Tickets for the 2008 Beijing Olympics' opening and closing ceremonies will be embedded with microchips containing the bearer's photograph, passport details, addresses, e-mail address and telephone number.[6]

- Researchers express concern that MRI scanning equipment may be used to decode brain activity to detect lying, racism, and other mental activities, in the process of screening job applicants.[7]

It is easy to imagine how these and other technologies might be applied in the workplace. For example, an employer might employ GPS technology to monitor where, when, and how fast company cars are being driven. Doing so not only would help an employer better assess the performance of its employees, but also, after gathering the appropriate information, determine faster routes, reduce fuel and insurance costs, identify emerging trends in consumer demand, and so on. This article briefly discusses legal issues with regard to two specific applications of workplace monitoring: electronic communications and employee movement.

Monitoring of Electronic Communications

Few jobs do not rely heavily on the use of a computer, along with e-mail and Internet access. Accordingly, companies make substantial investments in equipment and information systems. In an effort to protect their investments, ensure high productivity and limit exposure caused by a misuse of these systems, many companies use software and other technology to monitor their employees' e-mail or Internet usage for unauthorized and potentially illegal activity.

Expectation of Privacy

In general, whether an employer is permitted to monitor an employee's e-mail or Internet usage depends on whether the employee has a reasonable expectation of privacy. Both private and public employers must consider an employee's expectation of privacy under all the circumstances, although public employers have greater restrictions because of Fourth Amendment concerns.[8] Thus, while private employers should be aware of federal and state constitutional, statutory and common law limitations,[9] they must weigh the employee's privacy rights against their legitimate business interest in conducting the monitoring.

Employees generally will not have a reasonable expectation of privacy where they are informed in advance of the company's policy to monitor employees' e-mail and Internet

[1] Joseph J. Lazzarotti is a Partner with Jackson Lewis LLP, in the firm's White Plains, N.Y. office. He advises clients regarding various issues involving retirement and welfare plans pertaining to ERISA, HIPAA, the Internal Revenue Code and other federal statutes. He also heads the firm's HIPAA and Workplace Privacy Practice and advises companies regularly regarding data privacy and security issues nationally and internationally.
[2] Gutierrez, David, U.S. School District to Begin Microchipping Students, NaturalNews.com (June 16, 2008).
[3] Hohmann, James, Washington, D.C., Puts Itself Under Surveillance, Los Angeles Times (June 16, 2008).
[4] Dixon, Guy, Smart CCTV Cameras Will Hear and See, Vnunet.com (June 25, 2008).
[5] Lewis, Harry, How Facebook Spells the End of Privacy, Boston.com (June 14, 2008).
[6] Concern About Privacy, Identity Theft with Microchipped Olympic Tickets, SI.com (May 28, 2008).
[7] Highfield, Roger, Mind Reading by MRI Scan Raises "Mental Privacy" Issues, The Telegraph (June 9, 2008).
[8] *O'Conner v. Ortega*, 480 U.S. 709 (1987).
[9] Private employers in California have constitutional concerns in this regard because that State's Constitution applies the right to privacy to the private as well as the public sector. CAL. CONST. art. I, § 1; *Hill v. Nat'l Collegiate Athletic Assoc.*, 26 Cal. Rptr. 2d 834, 842-47 (Cal. 1994).

usage. The fact that an employee may use e-mail passwords likely will do little to prevent the employer from examining e-mails where the employee knew the employer could view them and the e-mails could be forwarded by recipients to others.[10] However, employers that have a monitoring policy must enforce it. Otherwise, they risk losing the argument that the employee did not have a reasonable expectation of privacy.[11]

Thus, it is critical for employers who intend to monitor employees' electronic communications and Internet access to publish a policy informing employees that the employer may conduct such surveillance and that the employees should have no expectation of privacy in their use of company computers and networks. It is worth noting, however, that an employee's reasonable expectation of privacy can be overcome by an employer's interest in preventing illegal activity, or by its duty to investigate.[12] For example, a state appellate court in New Jersey held in a case of first impression that an employer has a duty to investigate an employee's Internet activities when it has notice that the employee is using a workplace computer to access pornography, particularly child pornography.[13] The court held further that the employer has a duty to take prompt and effective action to stop the unauthorized activity.[14]

Federal and State Statutes and Common Law

Employers also must consider other issues when they monitor, intercept or access employees' e-mail messages or Internet usage: the effects of (1) the Federal Electronic Communications Privacy Act (ECPA);[15] (2) applicable state statutes, if any, dealing with wiretapping or electronic surveillance; and (3) common law. Of course, other laws, such as those prohibiting discrimination, might be invoked to prohibit certain types of monitoring, for example, where an employer monitored the e-mail communications only of its female employees. Likewise, an employer is not permitted to monitor as a way of retaliating against employees who engaged in activity protected by federal law. Employers also may be limited in their ability to monitor employees who are subject to a collective bargaining agreement.

Electronic Communications Privacy Act. Courts have characterized this law as "famous (if not infamous) for its lack of clarity." Indeed, they refer to this subject as a "complex, often convoluted, area of the law."[16] Part of the reason for this frustration is that the sparse case law regarding electronic communications on which employers have to rely mostly interprets federal and state statutes drafted for a different application ─ the monitoring of telephone communications.

[10] *Garrity v. John Hancock Mut. Life Ins. Co.*, 2002 U.S. Dist. LEXIS 8343, at *5 (D. Mass. May 7, 2002).
[11] *Curto v. Medical World Communications, Inc.*, 2006 WL 1318387, *4-5 (E.D.N.Y. May 15, 2006) (unpublished).
[12] *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996); *Doe v. XYC Corp.*, 2005 N.J. Super. LEXIS 377, *1-2 (N.J. Super. Ct. 2005).
[13] *Doe v. XYC Corp.*, 2005 N.J. Super. LEXIS 377, *1-2.
[14] *Id.*
[15] Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).
[16] *Steve Jackson Games, Inc. v. United States Secret Service, et al.*, 36 F.3d 457, 462 (5th Cir. 1994); *United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998).

Simply, the ECPA creates civil and criminal liability if a person impermissibly: (1) ***intercepts*** an electronic communication; or (2) ***accesses*** a stored electronic communication.[17] However, ECPA is concerned only with the intentional interception, use and disclosure of the content of communications. This means that information concerning the times when e-mails are sent, how many e-mails are sent, or the amount of time spent on a computer network is not covered by ECPA.

Courts have found consistently that ECPA's definition of electronic communication includes e-mail messages.[18] However, highlighting the law's lack of clarity, the courts have struggled with what constitutes an interception of an e-mail, and when it is permissible to access e-mails in storage. For example, some courts have held that the e-mail has to be acquired contemporaneously with the transmission in order for it to be considered an "interception."[19] Others, however, have held that acquiring a communication in storage and acquiring it contemporaneously with the transmission are not mutually exclusive.[20] As to stored communications, some courts have held that accessing an e-mail received by an employee that is on the employer's server would not violate ECPA.[21] These divergent opinions require employers to tread carefully when deciding whether to monitor employee communications.

It is unclear whether monitoring employees' Internet usage falls under ECPA. As noted, ECPA prohibits the interception of the "contents" of an electronic communication.[22] "Contents" is defined as "any information concerning the substance, purport or meaning of that communication."[23] Therefore, simply monitoring the address of Internet sites an employee visits may not be a prohibited interception. This conclusion is further supported by the courts' consistent finding that the use of "pen registers" (devices which simply trace phone calls and do not record contents of the calls) does not constitute an interception of the contents of a communication as those terms are defined by ECPA.[24]

The ECPA contains three statutory exceptions: consent, business extension, and system provider. Again, employers should carefully consider whether an exception applies.

[17] 18 U.S.C.A. §2511(1)(a), 2701(a).
[18] *See Steve Jackson Games, Inc.*, 36 F.3d 457; *Wesley College v. Pitts*, 974 F. Supp. 375 (D. Del. 1997); *Eagle Investment Systems Corporation v. Tamm, et al.*, 2001 U.S. Dist. LEXIS 7349 (D. Mass. May 22, 2001).
[19] *See Steve Jackson Games, Inc.,* 36 F.3d at 462; *Konop v. Hawaiian Airlines, Inc.*, 308 F.3d 868, 878 (9th Cir. 2002).
[20] *See, e.g., United States v. Councilman*, 418 F.3d 67, 79-80 (1st Cir. 2005).
[21] *Fraser v. Nationwide Mutual Insurance Co.*, 352 F.3d 107 (3d Cir. 2003); *White v. White,* No. FM-20-00567-00 (N.J. Super. Ct. Ch. Div. Sept. 26, 2001).
[22] 18 U.S.C.A. § 2510(4).
[23] 18 U.S.C.A. § 2510(8).
[24] *Sun Kin Chan v. State of Maryland,* 78 Md. App. 287 (Md. Ct. Spec. App. 1989); *United States v. Best*, 363 F. Supp. 11 (S.D. Ga. 1973); *United States v. Kail*, 612 F.2d 443 (9th Cir. 1979), *cert. denied*, 445 U.S. 966 (1980).

- Consent. In general, an unlawful interception does not occur where the interception is made with the prior consent of one party to the communication. Consent can be implied, as where an employee uses an employer's telephone system after receiving notice that the employer may monitor calls for training and evaluation purposes.[25] Implied consent also may be established where employees sign a written notification acknowledging receipt of the company's intent to monitor. Consent may be established by e-mailing employees written notifications and requesting that they respond electronically to acknowledge receipt. If a company anticipates the need to monitor employees' electronic communications routinely, especially personal e-mail, the company should configure its computer system to display the complete or an abridged version of the written notification whenever the computer is accessed.

- Business extension. The business extension exception generally permits an interception of electronic communications where a company is doing so in the ordinary course of business using certain devices. However, the equipment used to perform the interception and the facts and circumstances surrounding the interception are critical.

  Because this exception originally was designed for the telephone equipment provided by telephone companies, courts have struggled with whether this exception applies to telephone equipment purchased at retail and even to networked computers.[26]

  Ensuring quality of service, protecting company interests and providing employee training are legitimate business reasons that may bring an interception within the ordinary course of business.[27] However, continuing to monitor a telephone call after establishing that the content clearly is of a personal nature would likely vitiate the applicability of this exception. It remains unclear whether and to what extent this exception applies to e-mail.[28] Therefore, for now employers should avoid relying solely on this exception.

- Service provider. The service provider exception permits the provider of the electronic communication to intercept, use or disclose it where doing so is necessary either to: (i) continue providing the service, or (ii) protect the service provider's rights or property. It is unclear whether and to what extent this exception applies to employers, particularly to their internal business e-mail systems.[29] However, the prohibition against accessing stored communications does not apply to a provider of an electronic communication service and has been held to permit employers to access messages stored on their systems.

Assuming employers under certain circumstances may qualify for the business extension and system provider exceptions, the application of these exceptions in many respects remains unclear. Therefore, the prudent employer will take steps to ensure it can rely on the consent exception.

State Statutes. Most states have laws restricting the interception of electronic communications. In many cases, they track ECPA. However, state laws can be more restrictive. For example, while ECPA requires only one party to a communication to consent to the access or recording of a telephone call, a number of states require the consent of all parties to the communication.[30] In fact, the California Supreme Court decided in *Kearney v. Solomon Smith Barney, Inc.,* that the state's two-party consent rule applied to persons outside the state calling a California resident, even where the callers were in a one-party consent state (Georgia, in that case).[31] Thus, employers wishing to monitor should consider the laws in states other those in which they are physically present.

Common Law. Courts have considered employee common law claims of invasion of privacy based on employer monitoring of employees' electronic communications through employer-provided electronic communications systems. These claims may take a number of forms. The elements necessary to support them vary from state to state. Claims typically are fashioned as an intrusion upon one's seclusion. Common law generally requires the plaintiff to prove an intentional intrusion upon his or her seclusion in a way that is highly offensive to a reasonable person. Employers usually are able to defeat such claims by showing the employee did not have a reasonable expectation of privacy. Also, employees have difficulty showing that employer monitoring is "highly offensive to a reasonable person".

In one unreported decision, the Court of Appeals of Texas held that an employee did not have a reasonable expectation of privacy in his personal e-mail folder located on his workplace computer, even though access to the system had to be obtained through a network password and the employee further restricted access to his personal folders with an additional private password.[32] The court found that the employer provided the plaintiff with a workstation so that he could perform the functions of his job. In connection with that purpose, part of the plaintiff's workstation included a company-owned computer that

[25] *Griffin v. City of Milwaukee*, 74 F.3d 824 (7th Cir. 1996); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1237 (D. Nev. 1996).
[26] *Hall v Earthlink Network, Inc.*, 396 F.3d 500, 505 (2d Cir. 2005) (networked computers are considered telephone equipment for purposes of ECPA).
[27] *See James v. Newspaper Agency Corp.*, 591 F.2d 579, 582 (10th Cir. 1979).
[28] *See* Alexander Rodriguez, *All Bark and No Byte: Employee E-Mail Privacy Rights In The Private Sector Workplace*, 47 Emory L.J. 1439 (1998).
[29] At least two court decisions support the proposition that the exceptions authorize employers to intercept and view e-mail and similar messages transmitted through computer equipment owned by the employer. *See Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996); *United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993). However, there are no cases directly on point.
[30] California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington.
[31] *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95 (2006).
[32] *McClaren v. Microsoft Corp.*, 1999 WL 339015 (Tex. App.-Dallas May 28, 1999) (unreported). *See also, Smyth v. The Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996) (court dismissed employee's claim that he was terminated in violation of the public policy for invasions of privacy when he was fired for sending an offensive e-mail to his supervisor because the employee had no reasonable expectation of privacy despite assurances that management would never intercept employee e-mail).

gave him the ability to send and receive e-mail messages. The court concluded that the e-mail messages stored on the company computer were not the plaintiff's personal property, but were merely an inherent part of the office environment.

Monitoring of Employee Movement

Many of the electronic devices we use today, from cellular telephones to personal data assistants (PDAs) to automobile navigation systems, are equipped with global positioning system (GPS) capabilities. This means that the locations of the equipment, vehicle or persons to which GPS technology is attached can be tracked remotely. Radio frequency technology, known as RFID, also is being used in the form of tags or cards to track the location of products and persons. More employers are beginning to apply these technologies broadly with greater frequency and for a variety of reasons. At this point, however, legislatures and courts are only beginning to catch up with these emerging technologies.[33] Many of the concepts that are being extended to e-mail communications systems likely will apply to these new technologies, as well, such as an employee's reasonable expectation of privacy.

Examples of state laws addressing the use of tracking technologies, some of which regulate employers, include:

- A California law making it a criminal offense for any person to use a mobile tracking device to determine the location of a vehicle without the consent of the registered owner, lessor, or lessee of the vehicle.[34] Other states with similar provisions include Vermont, Delaware, Hawaii and Tennessee.

- A Connecticut statute limiting the ability of an employer to use an electronic surveillance device or system for purposes of monitoring the activities of employees "in areas designed for the health or personal comfort of the employees or for safeguarding of their possessions."[35] In addition, except where an employer has reasonable grounds to believe that electronic monitoring may produce evidence that employees are engaged in illegal conduct or conduct creating a hostile work environment, the employer must provide written notice to employees that may be affected by the monitoring.[36]

- Legislation in four states (Missouri, California, Wisconsin and North Dakota)[37] prohibiting employers from forcing employees to have RFID chips implanted under their skin. Other states are considering similar legislation.

- A Washington enactment barring "skimming," or lifting information from RFID tags without the knowledge of the owner.[38]

In a case of first impression in Connecticut, a state court found that the state's monitoring statute referred to above was not applicable to an employer vehicle. Connecticut's monitoring statute requires employers engaging in monitoring to provide notice to employees of the kinds of monitoring that might occur. In *Vitka v. City of Bridgeport*, a city employee used a City-provided motor vehicle equipped with GPS technology and claimed he did not receive the statutorily required notice and that the monitoring was otherwise impermissible.[39] The court found, however, that the City's vehicle was not in an "area[] designed for the health or personal comfort of the employees or for safeguarding of their possessions." In addition, the notice statute defines electronic monitoring as the "collection of information on an employer's premises." Accordingly, the court found that because monitoring of a motor vehicle in this case was not on the employer's premises, notice was not required.

While to date there is no general federal ban or restriction on the use of monitoring technology, organized labor and other groups have tried to use existing federal law to stop employers from tracking employees in this manner. For example, a NLRB Advice Memorandum held that a trucking company did not have a duty to bargain with the union representing its employees over the installation of GPS in its trucks.[40] However, employers still must consider the employee's "reasonable expectation of privacy" with respect to such technology and whether the technology is so intrusive as to invade upon that expectation under the circumstances. For example, although not an employment law case, a Washington court found a GPS tracking device to be a "particularly intrusive method" of surveillance.[41] Of course, in states where there is a constitutional right to privacy, such as California and Washington, the employer's right to monitor in this fashion may be more limited.

---

[33] Some examples of legislative efforts include a bill (S.B. 1841, Reg. Sess. (Cal. 2004)) introduced in the 2003-04 session the California Legislature which would have required an employer to give notice of its intent to collect information on employee activities by means of "electronic devices." That bill was vetoed. Michigan and Pennsylvania entertained bills that targeted employer monitoring of electronic communications and that required detailed employee notification of such monitoring. S.B. 893, 187th Gen. Assem., Reg. Sess. (Pa. 2003); S.B. 675, 92d Legis., 1st Reg. Sess. (Mich. 2003). Neither of these proposed bills was enacted. Finally, the Massachusetts Legislature considered an act that would have allowed an employer to use electronic surveillance to collect information so long as the information is collected at the employer's premises and is confined to the employee's work. This act (S.B. 2190. 183d Gen. Court, Reg. Sess. § 2(a) (Mass. 2003)) would have prevented entirely employers from electronically monitoring their vehicles or mobile workers during business hours. The bill did not make it out of committee.

[34] Cal. Penal Code § 637.7. *See also* Vermont, V.T.C.A., Penal Code § 16.06(b); Delaware, 11 Del.C § 1335 (2006); Hawaii, Hi. Stat. Ann. § 803-42(a)(7); Tennessee, T.C.A. § 39-13-606(a).

[35] Conn. Gen. Stat. § 31-48b. (No employer or agent or representative of an employer shall operate any electronic surveillance device or system, including, but not limited to, the recording of sound or voice or a closed circuit television system, or any combination thereof, for the purpose of recording or monitoring the activities of his employees in areas designed for the health or personal comfort of employees or for safeguarding of their possessions, such as rest rooms, locker rooms or lounges.) *See also* W. Va. Code § 21-3-20.

[36] Conn. Gen. Stat. § 31-48d.

[37] Mo. H.B. 1883; Cal. S.B. 362; Wis. Code. Ann § 146.25; N.D. Code Ann. § 12.1-15-06.

[38] Wash. S.B. 1031.

[39] *Vitka v. City of Bridgeport*, 2007 Conn. Super. LEXIS 3486 (Conn. Super. Ct. Dec. 31, 2007).

[40] Roadway Express, Inc., Case 13-CA-39940-1 (NLRB Apr. 15, 2002). *See also Otis Elevator Co. v. Local 1, Int'l Union of Electors,* 2005 WL 2385849, *8 (S.D.N.Y. 2005).

[41] *State v. Jackson*, 76 P.3d 217 (Wash. 2003).

The application of these technologies also raises questions under statutes that are not monitoring-specific, such as:

- Tracking technologies may violate state laws protecting the privacy of non-work-related activities.
- Tracking technologies may violate federal prohibitions on interfering with concerted activity such as labor organizing.
- GPS may provide evidence of wage and hour law compliance or violations, as well as service requirements under Department of Transportation regulations.

Further, new technologies not yet in use may have implications in both areas of workplace monitoring discussed in this article – electronic communications and employee movement. For example, Microsoft Corp. recently filed a patent application for a "unique monitoring system" that would aggregate user activity data across users and devices to detect, among other things, "frustration or stress in the user via physiological and environmental sensors."[42] Such a system may be used to determine if a system user needs assistance or how to better reallocate assignments to better utilize resources. This level of monitoring, particularly because of information that can be learned through physiological and environmental sensors, very likely may raise additional issues, such as whether monitoring would constitute a medical inquiry that violates the voluntariness requirement under the Americans with Disabilities Act.

* * *

Workplace monitoring provides many advantages for employers, while creating a number of legal risks, some of them not yet fully defined. Before implementing such a program, employers must carefully consider applicable state and federal laws, as well as how those laws apply to emerging technologies.

[42] Microsoft Corporation, Patent Application Pub. No. US 2007/0300174 A1, App. No. 11/426,818 (Filed June 27, 2006).

TITLE: ELECTRONIC SYSTEMS USE

POLICY STATEMENT: The Company's electronic computer and communication systems are Company assets and are to be protected from unauthorized access, disclosure, modification, and destruction, whether accidental or intentional. It is the Company's policy that the electronic and telecommunication systems (telephone, voice mail, e-mail, video and teleconferencing, Intranet and Internet access, information systems such as CD ROM and online services, computer hardware and computer software) owned or leased by the Company are to be used primarily for professional purposes. Any personal use of these systems must be minimal and must always be of a professional nature and conform to generally accepted professional communications format and content. Personal use must not in any way interfere with the work responsibilities of an employee or their co-workers.

In addition to the system hardware and software, all files and contents of any communications, including all electronic files and messages, are the property of the Company, whether composed, received or sent by an employee. While employees may have individual accounts or passwords, employees should not assume that any message, file or information created, received, transmitted or stored on these systems is private. The Company reserves the right, but not the obligation, to access, review, copy and delete any message or other information on the systems and disclose such information for any purpose without notice to the employee. Any personal use shall be at the users own risk and the Company shall not be liable to the user for any loss or damage resulting from such use, the operation (or failure to perform) of the Company's electronic computer and communication systems or from the Company exercising any of its rights.

By using the Company's electronic and telecommunications systems, users are deemed irrevocably to have given their consent to the Company to access, review, copy, or delete all such materials for any purpose and to disclose them to any party it deems appropriate including disclosure to law enforcement authorities.

An employee's participation in and use of computer, e-mail and telecommunications services, such as e-mail, text messages, blog, web-site postings and news groups, not only portrays an image of the individual, but also the Company itself. Employees should act so as not to damage the reputation or interests of the Company

All electronic and telecommunication systems use at the Company must comply with all federal and state laws, company policies, and company contracts. This includes, but is not limited to, the following:

1. Users may not use the systems for illegal or unlawful purposes, including, but not limited to, receiving, downloading or sending proprietary information, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).

2. Users are prohibited from using the systems in any way that violates the Company's equal opportunity, sexual harassment or other policies. To this end, users are prohibited from accessing, retrieving, copying or sending any sexually explicit materials including offensive jokes and cartoons. E-mail messages that contain foul, inappropriate, or offensive language or those containing gender, racial or ethnic slurs or sexual innuendos, are prohibited. In addition, employees are reminded that use of the systems must always be in a manner consistent with the Company's mission and must not misrepresent or reflect unfavorably on the Company.

3. Users should limit their personal use of the systems. The Company allows occasional or incidental use for communication with family and friends, independent learning, and public service. The Company prohibits use of its systems to solicit for charitable or commercial ventures, or in any way that violates the Company's solicitation policy. Mass unsolicited mailings, access for non-employees to Company resources or network facilities, competitive commercial activity, dissemination of chain letters, or the use of the systems to proselytize for religious, political or other causes is prohibited.

4. Access to the systems is provided through personal login identifications and passwords. Users are responsible for all activities conducted through their password and should make use of system provided protection features to prevent others from obtaining access to the system through their personal login identification or password. Users must not attempt to access materials that are restricted to others or which are not required by user to perform their job. Users are responsible for reporting any misuse of the systems to their supervisor.

5. In the interest of maintaining network performance, users should not download or install any software on the systems without prior approval. Users should also not send unreasonably large electronic mail attachments.

6. In the interest of maintaining network security, users should not access the corporate network with personal devices (such as laptops) without prior approval. Memory devices (such as zip drives and USB drives) and other storage media (other than diskettes and CDs) may not be used unless approved or provided by the Company.

All the Company confidential information that is transmitted, received or stored via any Company electronic communication system will be treated as any other confidential information. Such information should be transmitted only to individuals with a legitimate need to know.

It is the responsibility of all Company employees to report any violation of this policy to your supervisor or department head.

Violations of this policy are subject to disciplinary action up to and including termination and if appropriate may be referred to law enforcement authorities.

The Company reserves the right to change this policy at any time.

QUESTIONS AND ANSWERS
ELECTRONIC SYSTEMS USE POLICY

1. Q: At times I receive offensive electronic communications from external parties, what are my responsibilities for handling these?

A. Virtually all electronic mail users receive messages and/or pictures which may be in violation of this policy. A first step is to delete the message upon receipt. If the sending party continues to send you messages of this type, it is your responsibility to request the sender, if known, to discontinue this behavior. If it is a party with which we do not have a legitimate relationship, inform your supervisor and work through the Help Desk

2. Q. What if I receive an electronic communication from or observe an activity of one of our own employees that may be in violation of this policy?

A. The responsibility varies. If the content is clearly in violation of the policy, such as sexually explicit materials, you should inform your supervisor immediately. If the content is more a matter of poor taste, and you believe out of character, you have the option to approach the individual and suggest the activity may be in violation of the policy. Regardless of your first response, if the behavior continues it is your responsibility to inform your supervisor.

3. Q. What if I've informed my supervisor, and he/she does not agree that the activity is a potential violation of this policy?

A. As in all areas of our daily work activities, if you have a material disagreement with your supervisor, the matter should be elevated to the person your supervisor reports to. Though it is preferred that you communicate this directly to your supervisor and jointly elevate this discussion, in some instances you may feel elevating the matter without your supervisor is appropriate.

4. Q. What specific responsibilities do information technology personnel have in supporting this policy, since they have access to our communications?

A. Our information technology personnel may encounter questionable content randomly through their daily activities, such as ensuring only Shentel-licensed software is loaded on a computer when performing an upgrade. It may also be encountered purposely through monitoring, the latter of which is done only through strict guidelines approved by executive management. The responsibility upon identifying suspect content is the same as described to Question 2 above.

5 Q. What information about the Company can I post on my Facebook or Myspace page or in a Blog or a posting on a website?

A. Your Internet postings should not disclose any information that is confidential or proprietary to the company or to any third party that has disclosed information to the Company.
If you comment on any aspect of the company's business or any policy issue in which the company is involved and in which you have responsibility, you must clearly identify yourself as a Company employee in your postings or blog site(s) and include a disclaimer that the views are your own and not those of the Company In addition, Company employees should not circulate postings they know are written by other Company employees without informing the recipient that the author of the posting is a Company employee. Your Internet posting should reflect your personal point of view. Because you are legally responsible for your postings, you may be subject to liability if your posts are found defamatory, harassing, or in violation of any other applicable law. You may also be liable if you make postings which include confidential or copyrighted information (music, videos, text, etc.) belonging to third parties. All of the above mentioned postings are prohibited under this policy and could result in disciplinary action up to and including termination of employment.

When posting your point of view, you should neither claim nor imply you are speaking on the Company's behalf, unless you are authorized in writing by your manager to do so. If you identify yourself as a Company employee on any Internet posting, refer to the work done by the Company or provide a link to a Company website, you are required to include the following disclaimer in a reasonably prominent place: "the views expressed on this post are mine and do not necessarily reflect the views of [COMPANY NAME]." Your Internet postings should not include the Company's logos or trademarks, and should respect copyright, privacy, fair use, financial disclosure, and other applicable laws

6. Q. What about mobile phones and PDAs?

A. Because employees can purchase mobile phones and PDAs under the Company's Unlimited Usage Plan[1], unlimited personal usage of such mobile phones and PDAs are permittedl; however, any use of such devices for the receipt of work related e-mails or messages is subject to this policy.

[1] Note: un-reinbursed personal usage of a company provided mobile phone could result in taxable income for the employee (and a related payroll tax and withholding obligation for the company), accordingly, the company in this case has developed a plan pursuant to which employees and the company split the cost of an unlimited usage plan thereby allowing the employee unlimited usage without incurring any tax liability.

NOTICE: This opinion is subject to formal revision before publication in the bound volumes of NLRB decisions. Readers are requested to notify the Executive Secretary, National Labor Relations Board, Washington, D.C. 20570, of any typographical or other formal errors so that corrections can be included in the bound volumes.

The Guard Publishing Company d/b/a The Register-Guard *and* Eugene Newspaper Guild, CWA Local 37194. Cases 36–CA–8743–1, 36–CA–8849–1, 36–CA–8789–1, and 36–CA–8842–1

December 16, 2007

DECISION AND ORDER

BY CHAIRMAN BATTISTA AND MEMBERS LIEBMAN, SCHAUMBER, KIRSANOW, AND WALSH

In this case, we consider several issues relating to employees' use of their employer's e-mail system for Section 7 purposes. First, we consider whether the Respondent violated Section 8(a)(1) by maintaining a policy prohibiting the use of e-mail for all "non-job-related solicitations." Second, we consider whether the Respondent violated Section 8(a)(1) by discriminatorily enforcing that policy against union-related e-mails while allowing some personal e-mails, and Section 8(a)(3) and (1) by disciplining an employee for sending union-related e-mails. Finally, we consider whether the Respondent violated Section 8(a)(5) and (1) by insisting on an allegedly illegal bargaining proposal that would prohibit the use of e-mail for "union business."

After careful consideration, we hold that the Respondent's employees have no statutory right to use the Respondent's e-mail system for Section 7 purposes. We therefore find that the Respondent's policy prohibiting employee use of the system for "non-job-related solicitations" did not violate Section 8(a)(1).

With respect to the Respondent's alleged discriminatory enforcement of the e-mail policy, we have carefully examined Board precedent on this issue. As fully set forth herein, we have decided to modify the Board's approach in discriminatory enforcement cases to clarify that discrimination under the Act means drawing a distinction along Section 7 lines. We then address the specific allegations in this case of discriminatory enforcement in accordance with this approach.

Finally, we find that the Respondent did not insist on its bargaining proposal prohibiting the use of e-mail for "union business." Therefore, we dismiss the allegation that the Respondent insisted on an illegal subject in violation of Section 8(a)(5) and (1).

I. BACKGROUND

On February 21, 2002, Administrative Law Judge John J. McCarrick issued the attached decision. The Respondent and the General Counsel each filed exceptions and a supporting brief, and the Charging Party filed cross-exceptions and a supporting brief. The General Counsel and Charging Party each filed an answering brief to the Respondent's exceptions. The Respondent filed an answering brief to the General Counsel's exceptions and a reply brief to the Charging Party's answering brief.

On January 10, 2007, the National Labor Relations Board issued a notice of oral argument and invitation to the parties and interested amici curiae to file briefs. The notice requested that the parties address specific questions concerning employees' use of their employer's e-mail system (or other computer-based communication systems) to communicate with other employees about union or other Section 7 matters. The Board's questions included, among other things, whether employees have a Section 7 right to use their employer's e-mail system to communicate with one another, what standard should govern that determination, and whether an employer violates the Act if it permits other nonwork-related e-mails but prohibits e-mails on Section 7 matters.

The General Counsel, the Charging Party, the Respondent, and various amici filed briefs.[1] On March 27, 2007, the Board held oral argument.

The Board has considered the decision and the record in light of the exceptions, briefs, and oral argument and has decided to affirm the judge's rulings, findings, and conclusions in part,[2] to reverse them in part, and to adopt

[1] The General Counsel filed a preargument brief and a brief in response to the Respondent's and amici's briefs. The Charging Party and the American Federation of Labor and Congress of Industrial Organizations (AFL–CIO) jointly filed a preargument brief. The Charging Party also filed a reply brief to the Respondent's and amici's briefs. The Respondent filed a preargument brief, a reply brief to the General Counsel's brief, and a reply brief to the brief jointly filed by the Charging Party and the AFL–CIO. Amicus briefs were filed by the Council on Labor Law Equality, Employers Group, the HR Policy Association, the Minnesota Management Attorneys Association, Proskauer Rose LLP, the National Employment Lawyers Association, the National Workrights Institute, and the United States Chamber of Commerce.

[2] In addition to our other findings set forth herein, we adopt the judge's conclusion that the Respondent violated Sec. 8(a)(1) by maintaining an overly broad rule prohibiting employees from wearing or displaying union insignia while working with the public. We agree with the judge that the Respondent failed to show special circumstances for the rule. We also reject the Respondent's argument that the allegation is time-barred by Sec. 10(b) because the rule was promulgated more than 6 months before the unfair labor practice charge. Although the rule may have been promulgated outside the 10(b) period, the complaint also alleges, and the judge stated in his conclusions of law, that the Respondent violated Sec. 8(a)(1) by "maintain[ing]" the rule. The maintenance during the 10(b) period of a rule that transgresses employee rights is itself a violation of Sec. 8(a)(1). *Eagle-Picher Industries*, 331 NLRB 169, 174 fn. 7 (2000); *Trus Joint MacMillan*, 341 NLRB 369, 372 (2004); *Control Services*, 305 NLRB 435 fn. 2 & 442 (1991).

the recommended Order as modified and set forth in full below.[3]

II. FACTS

A. The Respondent's Communications Systems Policy

The Respondent publishes a newspaper. The Union represents a unit of about 150 of the Respondent's employees. The parties' last collective-bargaining agreement was in effect from October 16, 1996 though April 30, 1999. When the record closed, the parties were negotiating, but had not yet reached a successor agreement.

In 1996, the Respondent began installing a new computer system, through which all newsroom employees and many (but not all) other unit employees had e-mail access. In October 1996, the Respondent implemented the "Communications Systems Policy" (CSP) at issue here. The policy governed employees' use of the Respondent's communications systems, including e-mail. The policy stated, in relevant part:

> Company communication systems and the equipment used to operate the communication system are owned and provided by the Company to assist in conducting the business of The Register-Guard. Communications systems are not to be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.

The Respondent's employees use e-mail regularly for work-related matters. Throughout the relevant time period, the Respondent was aware that employees also used e-mail to send and receive personal messages. The record contains evidence of e-mails such as baby announcements, party invitations, and the occasional offer of sports tickets or request for services such as dog walking. However, there is no evidence that the employees used e-mail to solicit support for or participation in any outside cause or organization other than the United Way, for which the Respondent conducted a periodic charitable campaign.

B. Prozanski's E-Mails and Resulting Discipline

Suzi Prozanski is a unit employee and the union president. In May and August 2000, Prozanski received two written warnings for sending three e-mails to unit employees at their Register-Guard e-mail addresses. The Respondent contends that the e-mails violated the CSP.

1. May 4, 2000 e-mail

The first e-mail involved a union rally that took place on the afternoon of May 1, 2000. Earlier that day, Managing Editor Dave Baker sent an e-mail to employees stating that they should try to leave work early because the police had notified the Respondent that anarchists might attend the rally. Employee Bill Bishop sent a reply e-mail to Baker and to many employees. Bishop's e-mail message also attached an e-mail the Union had received from the police stating that the *Respondent* had notified the police about the possibility of anarchists. Thus, Bishop's e-mail implied that Baker was mistaken or untruthful when he told employees that the police had notified the Respondent about the anarchists.

The rally took place as scheduled. Afterward, Prozanski learned that certain statements in Bishop's e-mail had been inaccurate. On May 2, Prozanski told Baker that she wanted to communicate with employees to "set the record straight." Baker told her to wait until he talked to Human Resources Director Cynthia Walden. On May 4, Prozanski had not heard back from management about her request, so she told Baker that she was going to send an e-mail response. Baker said, "I understand."[4] Prozanski then sent an e-mail entitled, "setting it straight." She composed the e-mail on her break but sent it from her work station. A few hours later, Baker told Prozanski that she should not have used company equipment to send the e-mail.

Prozanski's e-mail began: "In the spirit of fairness, I'd like to pass on some information to you. . . . We have discovered that some of the information given to you was incomplete. . . . The Guild would like to set the record straight." The e-mail then set forth the facts surrounding the call to police about anarchists attending the rally. The e-mail was signed, "Yours in solidarity, Suzi Prozanski."

On May 5, Baker issued Prozanski a written warning for violating the CSP by using e-mail for "conducting Guild business."[5]

[3] We shall modify the judge's conclusions of law and recommended Order and substitute a new notice to conform to our findings and to the Board's standard remedial language.

[4] The judge found that Baker said, "OK, I understand." The record supports the finding that Baker said, "I understand," but not that he said "OK" or otherwise expressly gave Prozanski permission to send the e-mail.

[5] The warning stated in full:

> On May 4, you used the company's e-mail system expressly for the purpose of conducting Guild business. As you know, this is a violation of the company's Communications Systems Policy. This is the second time this week that the policy was disregarded by officers of the Guild.
>
> In our conversation on the afternoon of May 4, you acknowledged to me that the e-mail system was not to be used for Guild business and that you "should have known better." I agree. What's even more troubling to me, though, is that the message you sent—on the company's e-mail system—is now posted on the Guild bulletin board, compounding the problem. Employees who see that e-mail message are likely to assume that it's OK to use the company's e-mail for purposes other than company business. And, of course, that's not true. If you composed and sent this e-mail on work time, that would also be inappropriate. This letter will become part of your personnel file.

Baker also disciplined Bishop for his earlier e-mail about the union rally. (The reference in Prozanski's warning to "the second time this week" is apparently a reference to Bishop's e-mail.) The complaint does not allege that Bishop's discipline or the enforcement of the CSP against Bishop was unlawful.

2. E-Mails on August 14 and 18, 2000

Prozanski received a second written warning on August 22, 2000, for two e-mails sent on August 14 and 18. The August 14 e-mail asked employees to wear green to support the Union's position in negotiations. The August 18 e-mail asked employees to participate in the Union's entry in an upcoming town parade. As with the May 4 e-mail, Prozanski sent these e-mails to multiple unit employees at their Register-Guard e-mail addresses. However, this time she sent the e-mails from a computer in the Union's office, located off the Respondent's premises. Prozanski testified she thought that the May 5 warning was for using the Company's equipment to send the message, and that there would be no problem if she sent e-mails from the Union's office instead. On August 22, however, Walden issued Prozanski a written warning, stating that Prozanski had violated the CSP by using the Respondent's communications system for Guild activities. The warning quoted the CSP's prohibition on "non-job-related solicitations."

C. Respondent's Bargaining Proposal Concerning E-Mail Use

About October 25, 2000, during bargaining, the Respondent presented the Union with "counterproposal 26," which proposed the following contract language:

> The electronic communications systems are the property of the Employer and are provided for business use only. They may not be used for union business.

On November 15, 2000, the Respondent clarified to the Union in writing that counterproposal 26 "only prohibits use of the systems *for union business*." (Emphasis in original.) The Respondent stated that its existing CSP "will govern the use of systems in situations 'other than' union business."

On November 16, 2000, the Union stated that it would not respond to the proposal because the Union viewed the proposal as illegally restricting Section 7 rights. On November 30, 2000, the Union filed a charge alleging that the Respondent violated Section 8(a)(5) by proposing counterproposal 26. The Region dismissed the charge on March 31, 2001.

In April 2001, the Union requested, and the Respondent provided, additional information on the scope of counterproposal 26. On April 21, the parties also discussed the proposal at the bargaining table. The Union's lead negotiator, Lance Robertson, noted that the Union's unfair labor practice charge had been dismissed. Although Robertson continued to press for additional clarification of the proposal, he also told the Respondent: "I'm here to bargain a proposal." At the hearing, he testified that the Union's position as of April 21 was that it "neither accepted nor rejected" counterproposal 26. The Union never made a counterproposal. The parties stipulated that counterproposal 26 has been the Respondent's position since October 25, 2000.

On April 24, 2001, the Union filed a new charge alleging that the Respondent had proposed and "refus[ed] to withdraw" counterproposal 26. On August 13, 2001, the Region revoked its dismissal of the previous charge.

III. THE JUDGE'S DECISION

Noting that an employer may lawfully limit employee use of the employer's equipment or media, the judge found that the Respondent did not violate Section 8(a)(1) by maintaining the CSP. However, the judge found that the Respondent did violate Section 8(a)(1) by discriminatorily enforcing the CSP to prohibit union-related e-mails while allowing a variety of other nonwork-related e-mails. The judge also found that the Respondent violated Section 8(a)(3) and (1) by disciplining Prozanski for her May 4 and August 14 and 18 e-mails. Finally, the judge found that the Respondent violated Section 8(a)(5) and (1) by insisting on counterproposal 26, which the judge found was a codification of the Respondent's discriminatory practice of allowing personal e-mails but not union-related e-mails.

IV. POSITIONS OF THE PARTIES AND AMICI

A. The General Counsel

The General Counsel argues that under *Republic Aviation Corp. v. NLRB*, 324 U.S. 793 (1945), rules limiting employee communication in the workplace should be evaluated by balancing employees' Section 7 rights and the employer's interest in maintaining discipline. The General Counsel contends that e-mail cannot neatly be characterized as either "solicitation" or "distribution." Nevertheless, e-mail has become the most common "gathering place" for communications on work and nonwork issues. Because the employees are rightfully on the employer's property, the employer does not have an indefeasible interest in banning personal e-mail just because the employer owns the computer system. The

General Counsel distinguishes the Board's decisions that find no Section 7 right to use an employer's bulletin boards, telephones, and other equipment[6] on the basis that those cases did not involve interactive, electronic communications regularly used by employees, nor did they involve equipment used on networks where thousands of communications occur simultaneously. However, the General Counsel concedes that the employer has an interest in limiting employee e-mails to prevent liability for inappropriate content, to protect against system overloads and viruses, to preserve confidentiality, and to maintain productivity.

The General Counsel therefore proposes that broad rules prohibiting nonbusiness use of e-mail should be presumptively unlawful, absent a particularized showing of special circumstances. The General Counsel would evaluate other limitations on employee e-mail use (short of a complete ban) on a case-by-case basis.

With respect to whether an employer may prohibit employees from sending union-related e-mails while allowing other personal e-mails, the General Counsel notes that this conduct would violate Section 8(a)(1) under current Board precedent. The General Counsel disagrees with the Respondent's contention that employees communicating about a union are working on behalf of an "outside organization."

B. The Charging Party and Amicus AFL–CIO

The Charging Party and AFL–CIO jointly filed a preargument brief. They contend that where an employer allows employees to use the e-mail system to communicate with each other on nonbusiness matters generally, the employees are already rightfully on the employer's property, in the sense that they have been allowed access to the e-mail system. Thus, it is the employer's management interests, not its property interests, that are implicated. The employer may impose a nondiscriminatory restriction on e-mail communications during working time, but may impose additional restrictions only by showing that they are necessary to further substantial management interests.

In a reply brief, the Charging Party argues that if the Board is faced with a conflict between property rights and Section 7 rights, the Board must balance the two sets of interests. The Board should first determine the impact of the restriction on employee rights, and then determine the effect on the employer's property rights of forbidding the restriction.

With respect to enforcement of the CSP, the Charging Party and AFL–CIO argue that, because the Respondent allowed personal use of e-mail generally, the Respondent violated the Act by enforcing the CSP against Prozanski for sending union-related messages.

C. The Respondent

The Respondent argues that there is no Section 7 right to use the Respondent's e-mail system. E-mail, as part of the computer system, is equipment owned by the Respondent for the purpose of conducting its business. The Respondent notes that under Board precedent, an employer may restrict the nonbusiness use of its equipment. The Respondent argues that *Republic Aviation* and other cases dealing with oral solicitation are inapposite because they do not involve use of the employer's equipment. The Respondent observes that the Union and employees here have many means of communicating in addition to e-mail.

With respect to whether an employer has discriminatorily enforced its e-mail prohibition, the Respondent argues that the correct comparison is not between personal e-mails and union-related e-mails. Rather, the Respondent argues that in order to determine whether discriminatory enforcement has occurred, the Board should examine whether the employer has banned union-related e-mails but has permitted outside organizations to use the employer's equipment to sell products, to distribute "persuader" literature, to promote organizational meetings, or to induce group action. The Respondent argues that under this standard, the enforcement of the CSP against Prozanski was not discriminatory.

D. Amici Supporting the General Counsel and Charging Party

The National Employment Lawyers Association (NELA) argues that employer e-mail systems are no different from lunchrooms or breakrooms, and that any attempt to proscribe e-mail communications on nonworking time would contravene *Republic Aviation*. With respect to enforcement of the CSP against Prozanski, NELA notes that the Respondent's CSP prohibits only "non-job-related" solicitations. NELA contends that the union-related e-mails for which Prozanski was disciplined should be considered job-related.

The National Workrights Institute argues that e-mail is becoming the predominant method of business communication, and that most employer e-mail policies allow some personal use. However, the Institute contends that most policies are vague and applied on an ad hoc basis, and such uncertainty chills employee use of e-mail for Section 7 purposes. Thus, the Institute argues, banning union-related e-mails, either officially or in practice, should be deemed to violate Section 8(a)(1).

[6] These cases are discussed in sec. V,A below.

E. Amici Supporting the Respondent

Amici supporting the Respondent emphasize the employer's property interest. They argue that an employer should be permitted to impose nondiscriminatory restrictions on e-mail use, just as the employer may do with respect to its other equipment. The HR Policy Association, the Minnesota Management Attorneys Association, and the United States Chamber of Commerce contend that e-mail does not fit neatly into the Board's analytical framework for workplace solicitation and distribution. The Employers Group and the HR Policy Association also contend, alternatively, that if the Board does decide to analyze e-mail as either solicitation or distribution, e-mail should be considered more analogous to distribution. The Employers Group and the United States Chamber of Commerce further argue that an employer that does allow personal e-mail use must be permitted to impose reasonable, nondiscriminatory limits on e-mail use, such as those relating to the size of messages, the size of attachments, and the number of recipients.

Amici supporting the Respondent generally argue that an employer does not violate the Act simply because it permits some personal e-mails while prohibiting solicitations on behalf of unions or other organizations.

V. DISCUSSION

For the reasons set forth below, we agree with the judge that the Respondent did not violate Section 8(a)(1) by maintaining the CSP. We also agree with the judge that the Respondent's enforcement of the CSP with respect to Prozanski's May 4 e-mail was discriminatory and therefore violated Section 8(a)(1). Likewise, the written warning issued to Prozanski for the May 4 e-mail violated Section 8(a)(3) and (1).

However, we reverse the judge and dismiss the allegations that the Respondent's application of the CSP to Prozanski's August 14 and 18 e-mails was discriminatory. We also find no 8(a)(3) violation as to Prozanski's discipline for those e-mails. Finally, we reverse the judge and dismiss the allegation that the Respondent violated Section 8(a)(5) and (1) by insisting on counterproposal 26.

A. Maintenance of the CSP

The CSP, in relevant part, prohibits employees from using the Respondent's e-mail system for any "non-job-related solicitations." Consistent with a long line of cases governing employee use of employer-owned equipment, we find that the employees here had no statutory right to use the Respondent's e-mail system for Section 7 matters. Therefore, the Respondent did not violate Section 8(a)(1) by maintaining the CSP.

An employer has a "basic property right" to "regulate and restrict employee use of company property." *Union Carbide Corp. v. NLRB*, 714 F.2d 657, 663–664 (6th Cir. 1983). The Respondent's communications system, including its e-mail system, is the Respondent's property and was purchased by the Respondent for use in operating its business. The General Counsel concedes that the Respondent has a legitimate business interest in maintaining the efficient operation of its e-mail system, and that employers who have invested in an e-mail system have valid concerns about such issues as preserving server space, protecting against computer viruses and dissemination of confidential information, and avoiding company liability for employees' inappropriate e-mails.

Whether employees have a specific right under the Act to use an employer's e-mail system for Section 7 activity is an issue of first impression. In numerous cases, however, where the Board has addressed whether employees have the right to use other types of employer-owned property—such as bulletin boards, telephones, and televisions—for Section 7 communications**,** the Board has consistently held that there is "no statutory right . . . to use an employer's equipment or media," as long as the restrictions are nondiscriminatory.[7] *Mid-Mountain Foods*, 332 NLRB 229, 230 (2000) (no statutory right to use the television in the respondent's breakroom to show a prounion campaign video), enfd. 269 F.3d 1075 (D.C. Cir. 2001). See also *Eaton Technologies*, 322 NLRB 848, 853 (1997) ("It is well established that there is no statutory right of employees or a union to use an employer's bulletin board."); *Champion International Corp.*, 303 NLRB 102, 109 (1991) (stating that an employer has "a basic right to regulate and restrict employee use of company property" such as a copy machine); *Churchill's Supermarkets*, 285 NLRB 138, 155 (1987) ("[A]n employer ha[s] every right to restrict the use of company telephones to business-related conversations. . . ."), enfd. 857 F.2d 1474 (6th Cir. 1988), cert. denied 490 U.S. 1046 (1989); *Union Carbide Corp.*, 259 NLRB 974, 980 (1981) (employer "could unquestionably bar its telephones to any personal use by employees"), enfd. in relevant part 714 F.2d 657 (6th Cir. 1983); cf. *Heath Co.*, 196 NLRB 134 (1972) (employer did not engage in objectionable conduct by refusing to allow prounion employees to use public address system to respond to antiunion broadcasts).[8]

[7] The separate allegation that the Respondent discriminatorily enforced the CSP is discussed in sec. V,B below.

[8] We do not rely on *Adtranz*, 331 NLRB 291 (2000), enf. denied 253 F.3d 19 (D.C. Cir. 2001), cited by the judge. In *Adtranz*, there were no exceptions to the judge's dismissal of an allegation that the employer

Our dissenting colleagues, however, contend that this well-settled principle—that employees have no statutory right to use an employer's equipment or media for Section 7 communications—should not apply to e-mail systems. They argue that the decisions cited above involving employer telephones—*Churchill's Supermarkets* and *Union Carbide*—were decided on discriminatory enforcement grounds, and therefore their language regarding an employer's right to ban nonbusiness use of its telephones was dicta. The Board, however, reaffirmed *Union Carbide* in *Mid-Mountain Foods*, supra, citing it for the specific principle that employees have no statutory right to use an employer's telephone for nonbusiness purposes. See 332 NLRB at 230.

Nevertheless, our dissenting colleagues assert that the issue of employees' use of their employer's e-mail system should be analyzed under *Republic Aviation v. NLRB*, 324 U.S. 793 (1945), by balancing employees' Section 7 rights and the employer's interest in maintaining discipline, and that a broad ban on employee nonwork-related e-mail communications should be presumptively unlawful absent a showing of special circumstances. We disagree and find the analytical framework *of Republic Aviation* inapplicable here.

In *Republic Aviation*, the employer maintained a general rule prohibiting all solicitation at any time on the premises. The employer discharged an employee for soliciting union membership in the plant by passing out application cards to employees on his own time during lunch periods. The Board found that the rule and its enforcement violated Section 8(a)(1), and the Supreme Court affirmed. The Court recognized that some "dislocation" of employer property rights may be necessary in order to safeguard Section 7 rights. See 324 U.S. at 802 fn. 8. The Court noted that the employer's rule "entirely deprived" employees of their right to communication in the workplace on their own time. Id. at 801 fn. 6. The Court upheld the Board's presumption that a rule banning all solicitation during nonworking time is "an unreasonable impediment to self-organization . . . in the absence of evidence that special circumstances make the rule necessary in order to maintain production or discipline." Id. at 803 fn. 10. Otherwise, employees would have no time at the workplace in which to engage in Section 7 communications.[9]

In contrast to the employer's policy at issue in *Republic Aviation*, the Respondent's CSP does not regulate traditional, face-to-face solicitation. Indeed, employees at the Respondent's workplace have the full panoply of rights to engage in oral solicitation on nonworking time and also to distribute literature on nonworking time in nonwork areas, pursuant to *Republic Aviation* and *Stoddard-Quirk*. What the employees seek here is use of the Respondent's communications equipment to engage in additional forms of communication beyond those that *Republic Aviation* found must be permitted. Yet, "Section 7 of the Act protects organizational rights . . . rather than particular means by which employees may seek to communicate." *Guardian Industries Corp. v. NLRB*, 49 F.3d 317, 318 (7th Cir. 1995); see also *NLRB v. United Steelworkers (Nutone)*, 357 U.S. 357, 363–364 (1958) (The Act "does not command that labor organizations as a matter of law, under all circumstances, be protected in the use of every possible means of reaching the minds of individual workers, nor that they are entitled to use a medium of communications simply because the Employer is using it."). *Republic Aviation* requires the employer to yield its property interests to the extent necessary to ensure that employees will not be "entirely deprived," 324 U.S. at 801 fn. 6, of their ability to engage in Section 7 communications in the workplace on their own time. It does not require the most convenient or most effective means of conducting those communications, nor does it hold that employees have a statutory right to use an employer's equipment or devices for Section 7 communications.[10] Indeed, the cases discussed above, in which the Board has found no Section 7 right to use an employer's equipment, were decided long after *Republic Aviation* and have been upheld by the courts. See, e.g., *NLRB v. Southwire Co.*, 801 F.2d 1252, 1256 (11th Cir. 1986) (no statutory right to use an employer's bulletin board); *Union Carbide Corp. v. NLRB*, 714 F.2d 657, 663 (6th Cir. 1983) ("As recognized by the ALJ, Union Carbide *unquestionably* had the right to regulate and restrict employee use of company property.") (emphasis in original).

The dissent contends that because the employees here are already rightfully on the Respondent's premises, only the Respondent's managerial interests—and not its property interests—are at stake. That would be true if the issue here concerned customary, face-to-face solicitation and distribution, activities that involve only the employees' own conduct during nonwork time and do not involve use of the employer's equipment. Being rightfully on the premises, however, confers no additional right on employees to use the employer's equipment for Section 7 purposes regardless of whether the employees are authorized to use that equipment for work purposes.[11]

The dissent contends that e-mail has revolutionized business and personal communications and that, by failing to carve out an exception for it to settled principles regarding use of employer property, we are failing to adapt the Act to the changing patterns of industrial life. The dissent attempts to distinguish use of e-mail from other communication equipment based on e-mail's interactive nature and its ability to process thousands of communications simultaneously.

We recognize that e-mail has, of course, had a substantial impact on how people communicate, both at and away from the workplace. Moreover, e-mail has some differences from as well as some similarities to other communications methods, such as telephone systems. For example, as the dissent points out, transmission of an e-mail message, unlike a telephone conversation, does not normally "tie up" the line and prevent the simultaneous transmission of messages by others. On the other hand, e-mail messages are similar to telephone calls in many ways. Both enable virtually instant communication regardless of distance, both are transmitted electronically, usually through wires (sometimes the very same fiber-optic cables) over complex networks, and both require specialized electronic devices for their transmission. Although the widespread use of telephone systems has greatly impacted business communications, the Board has never found that employees have a general right to use their employer's telephone system for Section 7 communications.

In any event, regardless of the extent to which communication by e-mail systems is similar to or different from communication using other devices or systems, it is clear that use of the Respondent's e-mail system has not eliminated face-to-face communication among the Respondent's employees or reduced such communication to an insignificant level. Indeed, there is no contention in this case that the Respondent's employees rarely or never see each other in person or that they communicate with each other solely by electronic means. Thus, unlike our dissenting colleagues, we find that use of e-mail has not changed the pattern of industrial life at the Respondent's facility to the extent that the forms of workplace communication sanctioned in *Republic Aviation* have been rendered useless and that employee use of the Respondent's e-mail system for Section 7 purposes must therefore be mandated. Consequently, we find no basis in this case to refrain from applying the settled principle that, absent discrimination, employees have no statutory right to use an employer's equipment or media for Section 7 communications.[12]

Accordingly, we hold that the Respondent may lawfully bar employees' nonwork-related use of its e-mail system, unless the Respondent acts in a manner that discriminates against Section 7 activity.[13] As the CSP on its face does not discriminate against Section 7 activity, we find that the Respondent did not violate Section 8(a)(1) by maintaining the CSP.

B. Alleged Discriminatory Enforcement of the CSP

The judge found that the Respondent violated Section 8(a)(1) by discriminatorily enforcing the CSP to prohibit Prozanski's union-related e-mails while allowing other nonwork-related e-mails. We affirm the violation as to

violated Sec. 8(a)(1) by maintaining a rule restricting the use of e-mail for nonbusiness purposes.

[9] In a later case, the Board held that employees may also engage in distribution on nonworking time in nonwork areas. *Stoddard-Quirk Mfg. Co.*, 138 NLRB 615 (1962). Because we find that e-mail use is governed by the decisions dealing with the use of an employer's equipment, and not by cases dealing with oral solicitation and distribution of literature, we need not address the arguments by some amici that e-mail is more analogous to distribution than to solicitation.

[10] The Board recently distinguished *Republic Aviation* in a case involving employee use of an employer's personal property. In *Johnson Technology, Inc.*, 345 NLRB 762, 763 (2005), the Board found that the respondent did not violate Sec. 8(a)(1) by prohibiting an employee from using the employer's scrap paper to prepare a union meeting notice. The Board emphasized that "it is not unlawful for an employer to caution employees to restrict the use of company property to business purposes." Rejecting the General Counsel's reliance on *Republic Aviation*, the Board further noted: "The issue in *Republic Aviation* was whether an employer's right to control the activities of employees lawfully on its premises was subject to limitations to accommodate the employees' Sec. 7 rights, such as to engage in prounion solicitations. Here, the question is whether an employee can take and use the employer's personalty, without its consent, to engage in a nonwork-related purpose such as a Sec. 7 activity." Id. at 763 fn. 8.

[11] Testimony in the record that sending or receiving a simple "text" e-mail does not impose any additional monetary cost on the Respondent is of no consequence to our inquiry here. The Respondent's property rights do not depend on monetary cost. Cf. *Johnson Technology,* supra at 763 ("[T]he issue is whether the [employees'] use of the property was protected, not how much the property is worth."). Moreover, although the dissent, noting that "the Respondent does not own cyberspace," seems to question the very existence of Respondent's property interest in its e-mail system, it is beyond doubt that the Respondent has a property interest in its servers that host its e-mail system and in the software on which it operates, as well as its computers on which the employees access e-mail.

[12] Contrary to the dissent, in reaching this conclusion, we are not applying an "alternative means of communication" test appropriate only for questions of nonemployee access. See *Lechmere, Inc. v. NLRB*, 502 U.S. 527 (1992). Rather, we are merely examining whether, as asserted by the dissent, e-mail has so changed workplace communication that the Board should depart from settled precedent and order that the Respondent must permit employees to use its e-mail system to communicate regarding Sec. 7 matters. Such an analysis necessarily requires examination of whether the face-to-face solicitation and distribution permitted under *Republic Aviation* no longer enable employees to communicate. As we find controlling here the principle that employees have no statutory right to use an employer's equipment or media for Sec. 7 communications, neither *Republic Aviation* nor *Lechmere* is applicable.

[13] We do not pass on circumstances, not present here, in which there are no means of communication among employees at work other than e-mail.

Prozanski's May 4 e-mail, but reverse and dismiss as to her August e-mails. In doing so, we modify Board law concerning discriminatory enforcement.[14]

1. The appropriate analysis for alleged discriminatory enforcement

In finding that the Respondent discriminatorily enforced the CSP, the judge relied on evidence that the Respondent had permitted employees to use e-mail for various personal messages. Specifically, the record shows that the Respondent permitted e-mails such as jokes, baby announcements, party invitations, and the occasional offer of sports tickets or request for services such as dog walking.[15] However, there is no evidence that the Respondent allowed employees (or anyone else) to use e-mail to solicit support for or participation in any outside cause or organization other than the United Way, for which the Respondent conducted a periodic charitable campaign.

Citing *Fleming Co.*, 336 NLRB 192 (2001), enf. denied 349 F.3d 968 (7th Cir. 2003), the judge found that "[i]f an employer allows employees to use its communications equipment for nonwork related purposes, it may not validly prohibit employee use of communications equipment for Section 7 purposes." We agree with the judge that the Board's decision in *Fleming* would support that proposition. However, having carefully examined current precedent, we find that the Board's approach in *Fleming* and other similar cases fails to adequately examine whether the employer's conduct discriminated against Section 7 activity.

In *Fleming*, the Board held that the employer violated Section 8(a)(1) by removing union literature from a bulletin board because the employer had allowed "a wide range of personal postings" including wedding announcements, birthday cards, and notices selling personal property such as cars and a television. There was no evidence that the employer had allowed postings for any outside clubs or organizations. Id. at 193–194.[16] Likewise, in *Guardian Industries*, 313 NLRB 1275 (1994), enf. denied 49 F.3d 317 (7th Cir. 1995), the Board found an 8(a)(1) violation where the employer allowed personal "swap and shop" postings but denied permission for union or other group postings, including those by the Red Cross and an employee credit union.

The Seventh Circuit denied enforcement in both cases. *Fleming*, supra, 349 F.3d at 968; *Guardian*, supra, 49 F.3d at 317. In *Guardian*, the court started from the proposition that employers may control the activities of their employees in the workplace, "both as a matter of property rights (the employer owns the building) and of contract (employees agree to abide by the employer's rules as a condition of employment)." Id. at 317. Although an employer, in enforcing its rules, may not discriminate against Section 7 activity, the court noted that the concept of discrimination involves the unequal treatment of equals. See id. at 319. The court emphasized that the employer had never allowed employees to post notices of organizational meetings. Rather, the nonwork-related postings permitted by the employer consisted almost entirely of "swap and shop" notices advertising personal items for sale. The court stated: "We must therefore ask in what sense it might be discriminatory to distinguish between for-sale notes and meeting announcements." Id. at 319. The court ultimately concluded that "[a] rule banning all organizational notices (those of the Red Cross along with meetings pro and con unions) is impossible to understand as disparate treatment of unions." Id. at 320.

In *Fleming*, the court reaffirmed its decision in *Guardian* and further stated:

> Just as we have recognized for-sale notices as a category of notices distinct from organizational notices (which would include union postings), we can now add the category of personal postings. The ALJ's factual finding that Fleming did not allow the posting of organizational material on its bulletin boards does not support the conclusion that Fleming violated Section 8(a)(1) by prohibiting the posting of union materials.

349 F.3d at 975.

We find that the Seventh Circuit's analysis, rather than existing Board precedent, better reflects the principle that discrimination means the unequal treatment of equals. Thus, in order to be unlawful, discrimination must be along Section 7 lines. In other words, unlawful discrimination consists of disparate treatment of activities or communications of a similar character because of their union or other Section 7-protected status. See, e.g., *Fleming*, supra, 349 F.3d at 975 ("[C]ourts should look for disparate treatment of union postings before finding that an employer violated Sec. 8(a)(1)."); *Lucile Salter Packard Children's Hospital at Stanford v. NLRB*, 97 F.3d 583, 587 (D.C. Cir. 1996) (charging party must demonstrate that "the employer treated nonunion solicitations differently than union solicitations").

For example, 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.[17] 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 noncharitable 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 nonbusiness-related use. In each of these examples, the fact that union solicitation would fall on the prohibited side of the line does not establish that the rule discriminates along Section 7 lines.[18] For example, a rule that permitted charitable solicitations but not noncharitable solicitations would permit solicitations for the Red Cross and the Salvation Army, but it would prohibit solicitations for Avon and the union.[19]

The dissent contends that our analysis is misplaced because, in 8(a)(1) cases, discrimination is not the essence of the violation. Rather, the dissent asserts that discrimination is relevant in 8(a)(1) cases merely because it weakens or exposes as pretextual the employer's business justification for its actions. In our view, the dissent overlooks the Supreme Court's inhospitable response to this theory and too readily writes off discrimination as the essential basis of many 8(a)(1) violations.

The dissent argues that denying employees access to the employer's e-mail system for union solicitations while permitting access for other types of messages undermines the employer's business justification and constitutes discrimination. This argument is at odds with Supreme Court precedent. In *NLRB v. Steelworkers*, 357 U.S. 357 (1958), the Court reviewed the Board's finding in *Avondale Mills*, 115 NLRB 840 (1956), that the employer violated Section 8(a)(1) when it denied employees worktime access to their coworkers for union solicitation while permitting supervisors to engage in antiunion solicitation on working time. Even though supervisors and employees were not similarly situated, the Board found the employer's rule discriminatory because it diminished the employees' ability to communicate their organizational message and the employer's exception for supervisors belied the working-time-is-for-work justification. Id. at 842. The Supreme Court disagreed. Although the Court left the Board free in future cases to proceed on a theory of actual discrimination, it rejected the notion that a difference in treatment between any two groups not similarly situated that undermines the employer's asserted business justification violates Section 8(a)(1). According to the Court, there could be no unfair labor practice finding in such circumstances unless, in view of the available alternate channels of communication, the employer had truly diminished the ability of the labor

[14] The Respondent contends that all allegations regarding enforcement of the CSP are time-barred by Sec. 10(b), which states in relevant part that "no complaint shall issue based upon any unfair labor practice occurring more than 6 months prior to the filing of the charge with the Board." The Respondent argues that the 10(b) period runs from 1996, when the CSP was promulgated. The Respondent further argues that it gave the Union clear and unequivocal notice in 1997 that the Respondent would invoke the CSP to prohibit union-related e-mails. The Respondent relies on a 1997 memo from a manager to the Union's then-president, Bill Bishop, stating: "I will take responsibility for opening the door to use e-mail for Company/Union communications . . . I am now closing that door: E-mail will no longer be used for Company/Union communications. This of course applies also to using e-mail for Union or any other non-Company solicitations between employees."

We find no merit in the Respondent's argument that the 10(b) period runs from the promulgation of the policy in 1996 or from the 1997 memo to Bishop. The Board considers each instance of disparate enforcement of a policy to be a separate and independent act for purposes of Sec. 10(b). *Norman King Electric*, 334 NLRB 154, 162 (2001). Moreover, even assuming the 1997 memo constituted notice to the Union that the Respondent would enforce the e-mail policy against union-related e-mails, the Respondent's later actions were inconsistent with that memo. The Respondent did not adhere to its own statement that it was "closing the door" to using e-mail for union communications. The Respondent and the Union continued to communicate with one another by e-mail on matters such as scheduling bargaining sessions, and employees and managers continued to use e-mail for personal messages until the Prozanski incidents in 2000. Thus, the Union reasonably would have believed the Respondent was not following the 1997 memo. Accordingly, we reject the Respondent's 10(b) defense.

[15] The judge's finding that Weight Watchers had access to the Respondent's e-mail system is not supported. The record shows that the Respondent distributed information on a Weight Watchers program through payroll stuffers, not e-mail.

[16] Chairman Hurtgen, dissenting, would have dismissed the allegation based on the absence of any evidence that the employer permitted postings of any outside organizations. Id. at 194–195.

[17] On the other hand, an employer may use its own equipment to send antiunion messages, and still deny employees the opportunity to use that equipment for prounion messages. As noted above, employees are not entitled to use a certain method of communication just because the employer is using it. See *Nutone*, supra at 363–364.

[18] Of course, if the evidence showed that the employer's motive for the line-drawing was antiunion, then the action would be unlawful. There is no such evidence here.

Member Kirsanow notes that in determining whether a facially Section 7-neutral line has been drawn with an antiunion motive, the employer's reasonable interest in drawing that particular line would be, for Member Kirsanow, a relevant consideration. That is, if the line drawn has the effect of prohibiting all Section 7 communications and is not based on any reasonable employer interest, Member Kirsanow would find an antiunion motive to be a permissible inference.

[19] Indeed, the Board has already recognized that allowing limited charitable solicitations does not necessarily require an employer to allow union solicitations. See *Hammary Mfg. Corp.*, 265 NLRB 57 (1982) (an employer will not violate Sec. 8(a)(1) by "permitting a small number of isolated 'beneficent acts'"—such as solicitation for a United Way campaign—as "narrow exceptions" to a no-solicitation rule, while prohibiting union solicitation).

organization involved to carry its message to the employees.

It is not surprising, therefore, that the dissent fails to acknowledge that many decisions require actual discrimination. For example, as the Board noted in *Salmon Run Shopping Center*, 348 NLRB No. 31 (2006), the Supreme Court has held that "an employer violates 8(a)(1) of the Act by prohibiting nonemployee distribution of union literature if its actions 'discriminate against the union by allowing other distribution.'" Id., slip op. at 1, quoting *NLRB v. Babcock & Wilcox Co.*, 351 U.S. 105, 112 (1956). After determining that the employer's decision to deny the union access was based "solely on the Union's status as a labor organization and its desire to engage in labor-related speech," the Board found in *Salmon Run* that "[s]uch discriminatory exclusion" violated Section 8(a)(1). *Salmon Run Shopping Center,* above, slip op. at 2.

Similarly, in *Enloe Medical Center*, 348 NLRB No. 63 (2006), the Board found that the employer violated Section 8(a)(1) by sending employees a message stating that "it is not appropriate for union literature to be . . . placed in our breakroom." The Board found that the message was discriminatory, and therefore unlawful, because it "barred only union literature, and no other, from being placed in the breakroom." Id., slip op. at 1.

To be sure, the cases on which the dissent relies include language suggesting that the employers' unlawful, discriminatory conduct tended to undermine their asserted business justifications.[20] However, the presence of such language in those cases does not negate the many cases that find discriminatory conduct violative of Section 8(a)(1) purely on the basis of the conduct's discriminatory nature.

We therefore adopt the position of the court in *Guardian* and *Fleming* 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, and we shall apply this view in the present case and in future cases.[21] Accordingly, in determining whether the Respondent discriminatorily enforced the CSP, we must examine the types of e-mails allowed by the Respondent and ask whether they show discrimination along Section 7 lines.[22]

2. Application of the standard

Prozanski's August 14 e-mail urged all employees to wear green to support the Union. Her August 18 e-mail urged employees to participate in the Union's entry in a local parade. Both messages called for employees to take action in support of the Union. The evidence shows that the Respondent tolerated personal employee e-mail messages concerning social gatherings, jokes, baby announcements, and the occasional offer of sports tickets or other similar personal items. Notably, however, there is no evidence that the Respondent permitted employees to use e-mail to solicit other employees to support any group or organization.[23] Thus, the Respondent's enforcement of the CSP with respect to the August 14 and 18 e-mails did not discriminate along Section 7 lines, and therefore did not violate Section 8(a)(1).[24]

Prozanski's May 4 e-mail, however, was not a solicitation. It did not call for action; it simply clarified the facts surrounding the Union's rally the day before. As noted above, the Respondent permitted a variety of nonwork-related e-mails other than solicitations. Indeed, the CSP itself prohibited only "non-job-related solicitations," not all non-job-related communications. The only difference between Prozanski's May e-mail and the e-mails permitted by the Respondent is that Prozanski's e-mail was union-related. Accordingly, we find that the Respondent's enforcement of the CSP with respect to the May 4 e-mail discriminated along Section 7 lines and therefore violated Section 8(a)(1).[25]

C. The 8(a)(3) Allegations

We agree with the judge that the May 5 warning to Prozanski violated Section 8(a)(3) and (1). Contrary to the judge, however, we find it unnecessary to engage in a *Wright Line*[26] analysis. *Wright Line* is appropriately used in cases "turning on employer motivation." 251 NLRB at 1089. A *Wright Line* analysis is not appropriate where the conduct for which the employer claims to have disciplined the employee was union or other protected activity. See *St. Joseph's Hospital*, 337 NLRB 94, 95 (2001) (warning for displaying union-related screen saver violated 8(a)(3) where employer allowed other nonwork-related screen savers), enfd. 55 Fed. Appx. 902 (11th Cir. 2002); *Saia Motor Freight Line, Inc.*, 333 NLRB 784, 785 (2001) (8(a)(3) violation found where employee was disciplined for "distributing union literature").

Here, the May 5 warning stated that Prozanski "used the company's e-mail system expressly for the purpose of conducting Guild business" and that this violated the CSP. Thus, it is clear from the warning itself that the Respondent disciplined Prozanski for sending a union-related e-mail. The issue is whether Prozanski lost the protection of the Act by using the Respondent's e-mail system to send the message. With respect to the May 4 e-mail, she did not. As explained above, although there is no Section 7 right to use an employer's e-mail system, there is a Section 7 right to be free from discriminatory treatment. See *St. Joseph's Hospital*, supra at 95. The Respondent acted discriminatorily in applying the CSP to Prozanski's May 4 e-mail. Accordingly, the May 5 warning to Prozanski for sending that e-mail violated Section 8(a)(3) and (1).

However, we reverse the judge and dismiss the allegation that the August 22 warning violated Section 8(a)(3) and (1). That warning was issued in response to Prozanski's August 14 and 18 e-mails. We have found above that the Respondent's application of the CSP to prohibit those e-mails did not discriminate along Section 7 lines. Prozanski's conduct was therefore unprotected, and the August 22 discipline was lawful.

D. The 8(a)(5) Allegation

The judge found that the Respondent violated Section 8(a)(5) and (1) by insisting on counterproposal 26, which the judge found was an unlawful bargaining proposal. We reverse. In doing so, we find it unnecessary to decide whether counterproposal 26 was unlawful on its face. Rather, we find the evidence insufficient to show that the Respondent insisted on the proposal.

A party violates its duty to bargain in good faith by insisting on an unlawful proposal. See, e.g., *Teamsters Local 20 (Seaway Food Town)*, 235 NLRB 1554, 1558 (1978); *Thill, Inc.*, 298 NLRB 669, 672 (1990), enfd. in rel. part 980 F.2d 1137 (7th Cir. 1992). However, a party does not necessarily violate the Act simply by proposing or bargaining about an unlawful subject. *Sheet Metal Workers Local 91 (Schebler Co.)*, 294 NLRB 766, 773 (1989), enfd. in part 905 F.2d 417 (D.C. Cir. 1990). Rather, what the Act prohibits is "the insistence, as a condition precedent of entering into a collective bargaining agreement," that the other party agree to an unlawful provision. *National Maritime Union (Texas Co.)*, 78 NLRB 971, 981–982 (1948), enfd. 175 F.2d 686 (2d Cir. 1949), cert. denied 338 U.S. 954 (1950).

Here, contrary to the dissent, we find no proof of such insistence. The Union filed a charge alleging that the Respondent had made an unlawful proposal in violation of Section 8(a)(5). The charge was administratively dismissed. Thereafter, on April 21, 2001, the Union told the Respondent that the Union was prepared "to bargain a proposal" and that the Union "neither accepted nor rejected" the Respondent's proposal. The Union also sought clarification of the proposal, and there is no allegation that such clarification was unlawfully withheld. Finally, there is no direct evidence that the Union asked that the proposal be removed from the table.[27] In these

[20] *Honeywell, Inc.*, 722 F.2d 405, 407 (8th Cir. 1983); *Sprint/United Management Co.*, 326 NLRB 397, 399 (1998); *Churchill's Supermarkets*, 285 NLRB 138, 156 (1987).

[21] Accordingly, we overrule the Board's decisions in *Fleming*, *Guardian*, and other similar cases to the extent they are inconsistent with our decision here.

We note, however, that our view of "discrimination" is broader than that of some courts. See, e.g., *Cleveland Real Estate Partners v. NLRB*, 95 F.3d 457, 465 (6th Cir. 1996) (in case involving nonemployee access to an employer's premises, court defined "discrimination" as "favoring one union over another or allowing employer-related information while barring similar union-related information").

[22] We also reject the dissent's assertion that our test, taken to its logical extreme, is a license for an employer to permit almost anything but union communication as long as the employer does not expressly say so. Indeed, the hypothetical postulated by the dissent shows the fallacy of this assertion. Thus, contrary to the dissent, a rule barring all nonwork-related solicitations by membership organizations certainly would not "permit employees to solicit on behalf of virtually anything except a union," given the vast number of membership organizations in which employees may participate.

[23] The sole exception is the limited use of e-mail in connection with the Respondent's United Way campaign, which does not establish discriminatory enforcement. *Hammary Mfg. Corp.*, 265 NLRB 57 (1982) (an employer does not violate 8(a)(1) "by permitting a small number of isolated 'beneficent acts' as narrow exceptions to a no-solicitation rule").

[24] The dissent asserts that there is no clear evidence that the Respondent ever enforced the CSP against anything other than union-related messages. However, there is no evidence that any employee had ever previously sent e-mails soliciting on behalf of *any* groups or organizations. Accordingly, given the absence of evidence that the Respondent permitted employees to use e-mail to solicit support for groups or organizations, we decline to find that the Respondent's barring of e-mail solicitation on behalf of the Union constituted disparate treatment of activities or communications of a similar character.

The dissent further argues that the Respondent's barring of e-mail solicitations on behalf of the Union was unlawful because the CSP barred all "non-job-related" solicitations, but the Respondent—in practice—permitted personal e-mail messages, such as jokes, baby announcements, party invitations, and the occasional offer of sports tickets or request for services such as dog walking. We note, however, that the court of appeals in *Fleming Co.*, above, similarly found lawful the employer's removal of union literature from a bulletin board even though the employer's rule barring posting of all noncompany material was not enforced and posting of personal notices was routinely allowed.

[25] The Respondent argues that in sending all three e-mails, Prozanski was acting as a nonemployee union agent, not as an employee, and that her conduct is therefore governed by *Lechmere, Inc. v. NLRB*, 502 U.S. 527 (1992). *Lechmere* holds that an employer may exclude nonemployee union agents from its property, except where the employer acts discriminatorily or where the union has no reasonable alternative means to communicate with the employees. Id. at 535, 538. Prozanski was the union president, and she sent the August 14 and 18 e-mails from the union office. However, we need not reach the issue of whether *Lechmere* applies because it would not change the result. There would still be a violation as to the May 4 e-mail under *Lechmere*'s discrimination exception. There would be no violation as to the August 14 and 18 e-mails because there was no discrimination, and there is no allegation that the Union lacked reasonable alternative means of access to employees.

[26] 251 NLRB 1083 (1980), enfd. 662 F.2d 899 (1st Cir. 1981), cert. denied 455 U.S. 989 (1982), approved in *NLRB v. Transportation Management Corp.*, 462 U.S. 393 (1983).

[27] Contrary to the dissent, we do not find that the Union's second filing of the charge in itself provided evidence establishing the violation alleged in the charge.

circumstances, especially given the initial dismissal of the Union's 8(a)(5) charge and the Union's subsequent statements that it was prepared "to bargain a proposal" and that it "neither accepted nor rejected" the Respondent's proposal, we find the evidence insufficient to establish that the Respondent insisted on the proposal as a condition of entering into an agreement, or that the proposal impeded negotiations on lawful subjects.[28] Accordingly, we find no 8(a)(5) violation.

AMENDED CONCLUSIONS OF LAW

1. Delete the words "and August 22" from the judge's Conclusion of Law 2.

2. Delete the judge's Conclusion of Law 3.

ORDER

The National Labor Relations Board orders that the Respondent, The Guard Publishing Company d/b/a The Register-Guard, Eugene, Oregon, its officers, agents, successors, and assigns, shall

1. Cease and desist from

(a) Discriminatorily prohibiting employees from using the Respondent's electronic communications systems to send union-related messages.

(b) Maintaining an overly broad rule that prohibits employees from wearing or displaying union insignia while working with customers.

(c) Issuing written warnings to, or otherwise discriminating against, any employee for supporting the Eugene Newspaper Guild, CWA Local 37194 or any other labor organization.

(d) In any like or related manner interfering with, restraining, or coercing employees in the exercise of the rights guaranteed them by Section 7 of the Act.

2. Take the following affirmative action necessary to effectuate the policies of the Act.

(a) Rescind the rule prohibiting circulation department employees from wearing or displaying union insignia while working with customers**.**

(b) Within 14 days from the date of this Order, rescind the unlawful warning issued to Suzi Prozanski on May 5, 2000, remove from its files any reference to the unlawful warning, and within 3 days thereafter notify Prozanski in writing that this has been done and that the warning will not be used against her in any way.

(c) Within 14 days after service by the Region, post at its facility in Eugene, Oregon, copies of the attached notice marked "Appendix."[29] Copies of the notice, on forms provided by the Regional Director for Region 19, after being signed by the Respondent's authorized representative, shall be posted by the Respondent and maintained for 60 consecutive days in conspicuous places, including all places where notices to employees are customarily posted. Reasonable steps shall be taken by the Respondent to ensure that the notices are not altered, defaced, or covered by any other material. In the event that, during the pendency of these proceedings, the Respondent has gone out of business or closed the facility involved in these proceedings, the Respondent shall duplicate and mail, at its own expense, a copy of the notice to all current employees and former employees employed by the Respondent at any time since May 5, 2000.

(d) Within 21 days after service by the Region, file with the Regional Director a sworn certification of a responsible official on a form provided by the Region attesting to the steps that the Respondent has taken to comply with this Order.

IT IS FURTHER ORDERED that the complaint is dismissed insofar as it alleges violations of the Act not specifically found.

Dated, Washington, D.C. December 16, 2007

Robert J. Battista, Chairman

Peter C. Schaumber, Member

Peter N. Kirsanow, Member

(SEAL) NATIONAL LABOR RELATIONS BOARD

MEMBERS LIEBMAN AND WALSH, dissenting in part.

Today's decision confirms that the NLRB has become the "Rip Van Winkle of administrative agencies." *NLRB v. Thill, Inc*., 980 F.2d 1137, 1142 (7th Cir. 1992). Only a Board that has been asleep for the past 20 years could fail to recognize that e-mail has revolutionized communication both within and outside the workplace. In 2007, one cannot reasonably contend, as the majority does, that an e-mail system is a piece of communications equipment to be treated just as the law treats bulletin boards, telephones, and pieces of scrap paper.

National labor policy must be responsive to the enormous technological changes that are taking place in our society. Where, as here, an employer has given employees access to e-mail for regular, routine use in their work, we would find that banning all nonwork-related "solicitations" is presumptively unlawful absent special circumstances. No special circumstances have been shown here. Accordingly, we dissent from the majority's holding that the Respondent's ban on using e-mail for "non-job-related solicitations" was lawful.

We also dissent, in the strongest possible terms, from the majority's overruling of bedrock Board precedent about the meaning of discrimination as applied to Section 8(a)(1). Under the majority's new test, an employer does not violate Section 8(a)(1) by allowing employees to use an employer's equipment or media for a broad range of nonwork-related communications but not for Section 7 communications. We disagree, and therefore would also affirm the judge's finding that the Respondent violated Section 8(a)(3) and (1) by issuing written warnings to employee Suzy Prozanski for sending union-related e-mails. Finally, we dissent from the majority's finding that the Respondent did not insist on a bargaining proposal that codified the Respondent's unlawful discriminatory practice of prohibiting union-related e-mails while allowing other nonwork-related e-mails.[1]

I. FACTS

A. The Respondent's Communications Systems Policy

Since 1997, the Respondent has provided computer and e-mail access to the vast majority of its 155 unit employees. Numerous employees testified that they spend large portions of their workday on the computer, that they use e-mail regularly, and that to some extent it has replaced in-person communication.[2]

The principal issues in this case revolve around a Communications Systems Policy (CSP) implemented by the Respondent. The CSP governs employee use of the Respondent's communications systems, including e-mail. It states in relevant part:

> Company communication systems and the equipment used to operate the communication system are owned and provided by the Company to assist in conducting the business of The Register-Guard. Communications systems are not to be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, *or other non-job-related solicitations*. [Emphasis supplied.]

Except with respect to union activity, however, the CSP was honored (and enforced) in the breach. In addition to using e-mail regularly for work-related matters, the Respondent's employees, with the Respondent's knowledge and tacit approval, also used e-mail to send and receive nonwork-related messages. For example, the record contains hard copies of e-mails such as baby announcements, party invitations, a request for a dog walker, and offers of sports tickets. Employees also testified that they used e-mail for such matters as making lunch plans, disseminating jokes, keeping in touch with friends and relatives, and organizing a poker group.

B. The Respondent's Discipline of Suzi Prozanski for Sending Union-Related E-mails

Suzi Prozanski is a unit employee and the Union's president. On May 4, 2000, she composed an e-mail message on her breaktime and sent it to unit employees from her work station. The message, entitled "setting it straight," clarified facts surrounding a union rally on May 1.[3] On May 5, the Respondent issued Prozanski a written warning for violating the CSP by using e-mail for "conducting Guild business." The warning stated in part: "Employees who see that e-mail message are likely to assume that it's OK to use the company's e-mail for purposes other than company business. And, of course, that's not true."

On August 14 and 18, Prozanski sent two more e-mails to unit employees at their Register-Guard e-mail addresses. However, she composed and sent these messages from the Union's office, off the Respondent's premises. The August 14 e-mail asked employees to wear green to support the Union's position in negotiations. The August 18 e-mail asked employees to participate in the Union's entry in an upcoming town parade. The Respondent issued Prozanski another written warning on August 22, stating that Prozanski had violated the CSP by using the Respondent's communications system for Guild activities. The warning instructed Prozanski to "stop using the system for dissemination of union information."

Other than the warnings to Prozanski and a warning to one other employee, Bill Bishop, there is no clear evidence that the CSP was enforced against any other employees. Managing Editor Dave Baker, Prozanski's supervisor, testified that he had received numerous nonwork-related e-mails from employees but had never disciplined anyone other than Prozanski and Bishop.[4]

[28] Under these circumstances, we find it unnecessary to pass on whether the proposal itself was unlawful.

[29] If this Order is enforced by a judgment of a United States court of appeals, the words in the notice reading "Posted by Order of the National Labor Relations Board" shall read "Posted Pursuant to a Judgment of the United States Court of Appeals Enforcing an Order of the National Labor Relations Board."

[1] We join the majority in rejecting the Respondent's 10(b) defenses and in holding that the Respondent violated Sec. 8(a)(1) by maintaining an overly broad rule prohibiting employees from wearing or displaying union insignia while working with the public.

[2] The record in this case closed in 2001. Although not necessary, it is safe to assume that, in the interim, employee use of computers and e-mail has only increased.

[3] The circumstances leading up to Prozanski's message are described more fully in the majority decision.

[4] As discussed more fully in sec. II,B,1 of the majority decision, Bishop's discipline, too, was for a union-related e-mail. That discipline is not alleged to be unlawful.

C. The Respondent's Bargaining Proposal to Prohibit Using the Respondent's Communications Systems for "Union Business"

The parties' collective-bargaining agreement expired on April 30, 1999. In January 1999, they began negotiating for a successor agreement. Negotiations continued through the time of the 2001 hearing.

On October 25, 2000, at the end of a bargaining session, the Respondent presented the Union with "counterproposal 26," which proposed the following contract language:

> The electronic communications systems are the property of the Employer and are provided for business use only. They may not be used for union business.

There was no discussion of the proposal that day. The parties met again the next day, but did not discuss counterproposal 26. On November 15, around the time of their next bargaining session, the Respondent clarified in writing that counterproposal 26 "only prohibits use of the systems *for union business*" [emphasis in original]. The Respondent stated that its existing CSP "will govern the use of systems in situations 'other than' union business."

On November 16, the Union responded to counterproposal 26 in writing. The response stated that, on the advice of counsel, "we will not respond to this proposal at this time because it illegally restricts individuals' rights to concerted activity in the workplace." On November 30, the Union filed an unfair labor practice charge alleging that the Respondent violated Section 8(a)(5) by proposing counterproposal 26. The Region dismissed the charge on March 31, 2001. There is no evidence that the parties discussed the proposal between the filing and dismissal of the charge.

On April 9, 2001, the Union made a written request for information regarding the scope of counterproposal 26. The request noted that "the Guild asserted at the bargaining table that the company's proposal sought an illegal waiver of employee statutory rights and requested that the employer withdraw the proposal. The company refused." The Union then requested "immediate clarification as to the intent behind Company Counterproposal No. 26," including the types of union-related discussions it would prohibit. The Union stated: "Absent clarification from the employer as to a contrary intent, the Guild will assume that its original understanding regarding the intent of Counterproposal No. 26 was and is correct."

The Respondent provided a written response on April 21. The response stated in part: "It is unfortunate that you have decided to create a legal workshop on this issue. Until your unfair labor practice charge was dismissed you refused to even discuss our proposal." The response further stated that, "as a general rule," the proposal would apply to "all union business" and to all unit employees as well as union officers. It stated that the Respondent was not asking the union to waive employees' rights to decertify the Union. However, the proposal would bar an employee e-mail discussing the merits of a proposed union dues increase. With regard to other questions raised by the Union, the Respondent stated that it could not "try to prejudge all possible hypothetical acts and circumstances." The response also referred to Prozanski's discipline and stated that counterproposal 26 was intended to "make it clear" that its systems were not to be used for similar communications.

That same day, the parties held a bargaining session at which the Respondent's intended scope of counterproposal 26 was discussed further. The Union did not accept or reject any part of the proposal or offer any counterproposal. Rather, the Union's lead negotiator, Lance Robertson, continued to press for additional clarification of the proposal, specifically what the Respondent meant by "union business." In response, the Respondent's negotiator complained that Robertson was not bargaining, but simply "tak[ing] notes for your appeal to the process." He also noted the Union's prior position, that "it might be illegal for [the Union] to agree with the proposal." Robertson told the Respondent that he was "here to bargain a proposal," but he also stated: "In order to bargain it, we need to know how it would work." The Respondent's negotiator said that he would take Robertson's questions under advisement.

After the April 21 session, there is no evidence that the Respondent provided the Union with any further clarification. On April 24, the Union filed a new 8(a)(5) charge alleging that the Respondent had proposed and "refus[ed] to withdraw" counterproposal 26. On August 13, 2001, the Region revoked its dismissal of the previous charge. The parties stipulated that counterproposal 26 has been the Respondent's position since October 25, 2000.

II. DISCUSSION

A. Maintenance of the CSP

1. Legal framework governing Section 7 communications by employees in the workplace

The General Counsel contends that the CSP's prohibition on "non-job-related solicitations" is unlawfully overbroad and violates Section 8(a)(1). The judge dismissed that allegation, and the majority affirms the dismissal. We dissent.

The issue in an 8(a)(1) case is whether the employer's conduct interferes with Section 7 rights. If so, the employer must demonstrate a legitimate business reason

that outweighs the interference. See, e.g., *Caesar's Palace*, 336 NLRB 271, 272 fn. 6 (2001); *Jeannette Corp.*, 532 F.2d 916, 918 (3d Cir. 1976).

It is intuitively obvious that the workplace is "uniquely appropriate" for Section 7 activity. *NLRB v. Magnavox Co. of Tennessee*, 415 U.S. 322 (1974). In cases involving employee communications at work, the Board's task is to balance the employees' Section 7 right to communicate with the employer's right to protect its business interests. *Beth Israel Hospital v. NLRB*, 437 U.S. 483, 494 (1978). Limitations on communication should not be "more restrictive than necessary" to protect the employer's interests. Id. at 502–503.

Republic Aviation Corp. v. NLRB, 324 U.S. 793 (1945), is the seminal case balancing those interests with respect to oral solicitation in the workplace. The employer in *Republic Aviation* maintained a rule prohibiting solicitation anywhere on company property and discharged an employee for soliciting for the union during nonworking time. The Board adopted a presumption that restricting oral solicitation on nonworking time was unlawful, absent special circumstances. The Supreme Court affirmed the Board's finding that the employer's rule and its enforcement violated Section 8(a)(1). Although the solicitation occurred on the employer's property, the Court found that an insufficient justification to allow the employer to prohibit it. Rather, the Court endorsed the Board's reasoning that "[i]t is not every interference with property rights that is within the Fifth Amendment. . . . Inconvenience or even some dislocation of property rights, may be necessary in order to safeguard the right to collective bargaining." 324 U.S. at 802 fn. 8. Although an employer may make and enforce "reasonable rules" covering the conduct of employees on working time, "time outside working hours . . . is an employee's time to use as he wishes without unreasonable restraint, *although the employee is on company property*." Id. at 803 fn. 10 (emphasis supplied). The Court upheld the Board's presumption that a rule banning solicitation during nonworking time is "an unreasonable impediment to self-organization . . . in the absence of evidence that special circumstances make the rule necessary in order to maintain production or discipline." Id. at 803 fn. 10.

Thus, the presumption adopted in *Republic Aviation* vindicates the right of employees to communicate in the workplace regarding Section 7 matters, subject to the employer's right to maintain production and discipline. Although the majority correctly notes that the rule in *Republic Aviation* itself involved a complete ban on solicitation on the employer's premises, the Board and courts have long since applied *Republic Aviation*'s principles to lesser restrictions on employee speech. See, e.g., *Beth Israel,* 437 U.S. at 492 (rule prohibiting solicitation and distribution in the hospital's patient-care and public areas; employer permitted those activities in employee locker rooms and restrooms); *Times Publishing Co.*, 240 NLRB 1158 (1979) (rule prohibiting solicitation in "public areas" of the building), affd. 605 F.2d 847 (5th Cir. 1979); *Bankers Club, Inc.*, 218 NLRB 22, 27 (1975) (rule banning solicitation in "customer areas" of the respondent's restaurant).

The Supreme Court struck quite a different balance in cases involving nonemployees seeking to communicate with employees on the employer's premises. In a case involving distribution of union literature on an employer's property by nonemployee union organizers, the Court emphasized that "[a]ccommodation" between Section 7 rights and employer property rights "must be obtained with as little destruction of one as is consistent with the maintenance of the other." *NLRB v. Babcock & Wilcox*, 351 U.S. 105, 112 (1956). The Court held that an employer "may validly post his property against *nonemployee* distribution of union literature if reasonable efforts by the union through other available channels of communication will enable it to reach the employees with its message and if the employer's notice or order does not discriminate against the union by allowing other distribution." Id. (emphasis supplied). Distinguishing *Republic Aviation* on the basis that it involved communications by employees, the Court emphasized that "[t]he distinction [between employees and nonemployees] is one of substance. No restriction may be placed on the employees' right to discuss self-organization among themselves, unless the employer can demonstrate that a restriction is necessary to maintain production or discipline. But no such obligation is owed nonemployee organizers." Id. at 113; see also *Hudgens v. NLRB*, 424 U.S. 507, 521 fn. 10 (1976) ("A wholly different balance [is] struck when the organizational activity was carried on by employees already rightfully on the employer's property, since the employer's management interests rather than his property interests were there involved.").

In short, the Board and courts have long protected employees' rights to engage in Section 7 communications at the workplace, even though the employees are on the employer's "property."

2. The Respondent's prohibition on all "non-job-related solicitations" violated Section 8(a)(1)

Applying the foregoing principles, the General Counsel contends that employer rules restricting employee e-mail use must be evaluated under *Republic Aviation*, and that broad bans on employee e-mail use should be presumptively unlawful. The General Counsel emphasizes

that e-mail has become the "natural gathering place" for employees to communicate in the workplace,[5] and that e-mail sent and received on computers issued to employees for their use is not analogous to employer "equipment" such as bulletin boards, photocopiers, and public address systems.

The majority, however, finds the *Republic Aviation* framework inapplicable. Emphasizing the employer's "property" interest in its e-mail system, the majority reasons that, absent discriminatory treatment, employees have no Section 7 right to use employer personal property such as bulletin boards, television sets, and telephones. According to the majority, *Republic Aviation* ensures only that employees will not be "entirely deprived" of the ability to engage in any Section 7 communications in the workplace, but otherwise does not entitle employees to use their employer's equipment. Here, the majority asserts, the employees had other means of communication available.

We disagree. Indeed, we find that the General Counsel's approach is manifestly better suited to the role of e-mail in the modern workplace. "The responsibility to adapt the Act to changing patterns of industrial life is entrusted to the Board." *NLRB v. J. Weingarten*, 420 U.S. 251, 266 (1975). The majority's approach is flawed on several levels. First, it fails to recognize that e-mail has revolutionized business and personal communications, and that cases involving static pieces of "equipment" such as telephones and bulletin boards are easily distinguishable. Second, the majority's approach is based on an erroneous assumption that the Respondent's ownership of the computers gives it a "property" interest that is sufficient on its own to exclude Section 7 e-mails. Third, the majority's assertion that *Republic Aviation* created a "reasonable alternative means" test, even regarding employees who are already rightfully on the employer's property, is untenable.[6]

E-mail has dramatically changed, and is continuing to change, how people communicate at work. According to a 2004 survey of 840 U.S. businesses, more than 81 percent of employees spent at least an hour on e-mail on a typical workday; about 10 percent spent more than 4 hours.[7] About 86 percent of employees send and receive at least some nonbusiness-related e-mail at work.[8] Those percentages, no doubt, are continuing to increase. "Even employees who report to fixed work locations every day have seen their work environments evolve to a point where they interact to an ever-increasing degree electronically, rather than face-to-face. The discussion by the water cooler is in the process of being replaced by the discussion via e-mail."[9]

Given the unique characteristics of e-mail and the way it has transformed modern communication, it is simply absurd to find an e-mail system analogous to a telephone, a television set, a bulletin board, or a slip of scrap paper. Nevertheless, that is what the majority does, relying on the Board's statements in prior cases that an employer may place nondiscriminatory restrictions on the nonwork-related use of such equipment and property.[10] None of those "equipment" cases, however, involved sophisticated networks designed to accommodate thousands of multiple, simultaneous, interactive exchanges. Rather, they involved far more limited and finite resources. For example, if a union notice is posted on a bulletin board, the amount of space available for the employer to post its messages is reduced. See, e.g., *Sprint/United Management Co.*, 326 NLRB 397, 399 (1998) (employer "may have a legitimate interest in ensuring that its postings can easily be seen and read and that they are not obscured or diminished in prominence by other notices posted by employees"). If an employee is using a telephone for Section 7 or other nonwork-related purposes, that telephone line is unavailable for others to use. Indeed, in *Churchill's Supermarkets*, 285 NLRB 138, 147 (1987), enfd. 857 F.2d 1471 (6th Cir. 1988), cert. denied 490 U.S. 1046 (1989), cited by the majority, the judge noted that the employer's "overriding consideration has always been that an employee should not tie up the phone lines" for personal use.[11] Here, in

[5] See *Beth Israel*, supra at 490 (noting that the employer recognized the cafeteria as a "natural gathering place" for employees, because the employer had used and permitted use of the cafeteria for other types of solicitation and distribution).

[6] We also disagree with the majority's characterization of our approach as "carv[ing] out an exception" to precedent. Our analysis is hardly novel. Rather, as explained below, we apply the decades-old principles that employees have a right to communicate in the workplace, that the Board must balance that right with the employer's right to protect its business interests, and that interference with employees' Section 7 rights is unlawful unless outweighed by a legitimate business interest. *Republic Aviation*, supra, 324 U.S. at 803 fn. 10; *Beth Israel*, supra, 437 U.S. at 494; *Jeannette Corp.*, supra, 532 F.2d at 918.

[7] American Management Association, 2004 Workplace E-Mail and Instant Messaging Survey (2004). (www.amanet.org/research/pdfs/IM_2004_summary.pdf).

[8] Id.

[9] Martin H. Malin & Henry H. Perritt Jr., "The National Labor Relations Act in Cyberspace: Union Organizing in Electronic Workplaces," 49 U. Kan. L. Rev. 1, 17 (Nov. 2000).

[10] See sec. V,A of the majority decision.

[11] In any event, the statements in *Churchill's,* supra, and *Union Carbide Corp.*, 259 NLRB 974, 980 (1981), enfd. in rel. part 714 F.2d 657 (6th Cir. 1983), that an employer may bar all personal use of its telephones were dicta. In both of those cases, the Board found that the employer had discriminatorily prohibited union-related telephone calls while allowing other personal calls. Therefore, the Board was not faced with the issue of whether a nondiscriminatory ban on personal use was lawful.

contrast, the Respondent concedes that text e-mails impose no additional cost on the Respondent. At the time of the hearing in 2000, the Respondent's system was receiving as many as 4000 e-mail messages per day. One or more employees using the e-mail system would not preclude or interfere with simultaneous use by management or other employees. Furthermore, unlike a telephone, e-mail's versatility permits the sender of a message to reach a single recipient or multiple recipients simultaneously; allows the recipients to glimpse the subject matter of the message before deciding whether to read the message, delete it without reading it, or save it for later; and, once opened, allows the recipient to reply to the sender and/or other recipients, to engage in a real-time "conversation" with them, to forward the message to others, or to do nothing. Neither the telephone nor any other form of "equipment" addressed in the Board's prior cases shares these multidimensional characteristics.

The majority relies on the employer's ownership of the computer system as furnishing a "basic property right" to regulate e-mail use. But ownership, simpliciter, does not supply the Respondent with an absolute right to exclude Section 7 e-mails. The Respondent has already provided the computers and the e-mail capability to employees for regular and routine use to communicate at work.[12] Thus, the employees are not only "rightfully" on the Respondent's real property, the building itself; they are rightfully on (using) the computer system. See *Hudgens,* supra at 521 (when activity is "carried on by employees already rightfully on the employer's property . . . the employer's management interests rather than his property interests" are involved). Moreover, an e-mail system and the messages traveling through it are not simply "equipment"; the Respondent does not own cyberspace. See *Reno v. ACLU*, 521 U.S. 844, 850 (1997) (e-mail, the "World Wide Web," and mail listing services "constitute a unique medium—known to its users as 'cyberspace'—located in no particular geographic location but available to anyone, anywhere in the world, with access to the Internet.").

As the discussion above demonstrates, the existence of a "property right" does not end the inquiry—rather, it only begins it. The Respondent has not demonstrated how allowing employee e-mails on Section 7 matters interferes with its alleged property interest. To repeat, the Respondent already allows the employees to use the computers and e-mail system for work—and, for that matter, for personal messages. Additional text e-mails do not impose any additional costs on the Respondent. And e-mail systems, unlike older communications media, accommodate multiple, simultaneous users.

Common law involving computer "trespass," on which the Respondent relies, harms its case rather than helping it. Trespass cases illustrate that the mere use of a computer system to send e-mails does not interfere with the owner's property interest, absent some showing of harm to the system. The Restatement (Second) of Torts states in part: "The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor." See Section 218, cmt. e. Where courts have allowed tort actions to go forward based on trespass to a computer system, they have relied on specific allegations of harm.[13] Courts have dismissed claims where there was no such evidence.[14]

As stated, the majority also reasons, based on the particular facts of *Republic Aviation*, that the Respondent need not yield its "property interests" here, because employees have alternative means to communicate in the workplace, such as oral in-person communication. In

The majority states that the Board "reaffirmed" *Union Carbide* in *Mid-Mountain Foods*, 332 NLRB 229 (2000), enfd. 269 F.3d 1075 (D.C. Cir. 2001), by citing *Union Carbide* for the principle that employees have no statutory right to use an employer's telephone for nonbusiness purposes. The majority in *Mid-Mountain* did cite *Union Carbide* in passing for that principle, but did not engage in any analysis specific to the use of an employer's telephone system. *Mid-Mountain* involved the use of an employer's television set, not its telephone system. In any event, Member Liebman dissented on that issue in *Mid-Mountain*, and Member Walsh did not participate in the case.

[12] Cf. *Sprint/United Management Co.*, 326 NLRB 397, 399 (1998) (drawing a distinction between a bulletin board and the locker space that the respondent had "already ceded . . . to the personal use of the employees to whom the lockers are assigned").

[13] See, e.g., *Compuserve Incorporated v. Cyber Promotions, Inc.*, 962 F.Supp. 1015, 1022–1023 (S.D. Ohio 1997) (injunction granted to internet service provider against spam advertiser; handling the enormous volume of mass mailings burdened plaintiff's equipment, and many subscribers terminated their accounts because of the spam); *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 404 (2d Cir. 2004) (use of computer "robots" to obtain data through multiple queries of plaintiff's database consumed a significant portion of the system's capacity, and if the practice were permitted to continue, it was "highly probable" that others would devise similar programs, leading to overtaxing of the system).

[14] See, e.g., *Pearl Investments, LLC v. Standard I/O, Inc.*, 257 F.Supp. 326, 354 (D. Me. 2003) (even if defendant accessed the network without authorization, "there is no evidence that in doing so he impaired its condition, quality or value"); *Intel Corp. v. Hamidi*, 71 P.3d 296, 304, 308 (Cal. 2003) (no liability where evidence did not show that ex-employee's multiple e-mails criticizing the company "used the system in any manner in which it was not intended to function or impaired the system in any way"; "Whatever interest Intel may have in preventing its employees from receiving disruptive communications, it is not an interest in personal property. . . .").

2007, however, that train has already left the station: that is not how the courts and the Board have applied *Republic Aviation*, and the availability of alternative means is not relevant when dealing with employee-to-employee communications**.** See, e.g., *Babcock & Wilcox*, supra at 112–113; *Helton v. NLRB*, 656 F.2d 883, 896–897 (D.C. Cir. 1981) (collecting cases). The alternative-means test applies only to activity by *nonemployees* on the employer's property. See *Babcock & Wilcox*, supra at 112; *Lechmere, Inc. v. NLRB*, 502 U.S. 527 (1992). The distinction between employee and nonemployee activity is "one of substance." *Babcock & Wilcox*, supra at 113. If the absence of alternative means to communicate in the workplace were a prerequisite to employees' right to engage in Section 7 activity on employer property, presumably an employer could ban oral solicitation by employees in "work areas," or even everywhere except an employee breakroom, without any showing of special circumstances, because the employer would not have "entirely deprived" employees of the right to communicate on the premises. Of course, neither the Board nor the Supreme Court has ever placed such limits on Section 7 communication.[15]

For all of the foregoing reasons, we reject the majority's conclusion that e-mail is just another piece of employer "equipment." Where, as here, the employer has given employees access to e-mail in the workplace for their regular use, we would find that banning all nonwork-related "solicitations" is presumptively unlawful absent special circumstances. This presumption recognizes employees' rights to discuss Section 7 matters using a resource that has been made available to them for routine workplace communication. Because the presumption is rebuttable, it also recognizes that an employer may have interests that justify a ban. For example, an employer might show that its server capacity is so limited that even text e-mails would interfere with its operation.[16] An employer might also justify more limited restrictions on nonwork-related e-mails—such as prohibiting large attachments or audio/video segments—by demonstrating that such messages would interfere with the efficient functioning of the system. In addition, rules limiting nonwork-related e-mails to nonworking time would be presumptively lawful, just as with oral solicitations.[17]

Here, the Respondent has shown no special circumstances for its ban on "non-job-related solicitations," which on its face would prohibit even solicitations on nonworking time, without regard to the size of the message or its attachments, or whether the message would actually interfere with production or discipline. Accordingly, we would reverse the judge and find that the Respondent violated Section 8(a)(1) by maintaining the portion of the CSP that prohibits employees from using e-mail for "non-job-related solicitations."

B. The Respondent's Enforcement of the CSP

Even assuming the maintenance of the CSP were lawful, the judge correctly found that the Respondent violated Section 8(a)(1) by discriminatorily enforcing it. The majority does not dispute that this result was correct under Board precedent. Instead, the majority overrules that precedent and announces a new, more limited conception of "discrimination," based on two decisions from the Seventh Circuit.[18]

As explained below, we respectfully but emphatically disagree with the Seventh Circuit's analysis.[19] But even assuming we did not, the majority's application of its new test is flawed. Accordingly, we would affirm the judge's conclusion that the Respondent violated Section

[15] See, e.g., *Stoddard-Quirk Mfg. Co*., 138 NLRB 615, 621 (1962) ("the right of employees to [orally] solicit on plant premises must be afforded subject only to the restriction that it be on nonworking time"; in contrast, distribution of flyers and other printed material may be limited to nonworking time and nonworking areas).

[16] We would, however, require specific evidence to support such an assertion. "'Suffer the servers' is among the most chronically overused and under-substantiated interests asserted by parties . . . involved in Internet litigation. . . ." *White Buffalo Ventures v. University of Texas at Austin*, 420 F.3d 366, 375 (5th Cir. 2005), cert. denied 546 U.S. 1091 (2006).

[17] As with oral solicitations, however, if an employer has no rule in place that limits nonwork-related e-mails to nonworking time, the employer must show an actual interference with production or discipline in order to discipline employees for e-mails sent on working time. See, e.g., *Union Carbide*, supra at 979.

The Respondent and various amici argue that because of the nature of e-mail, enforcement of a "working time" restriction would be difficult. But similar difficulties exist even with oral solicitation rules. For example, where employees self-regulate their breaks, where a supervisor is not constantly present, or where the nature of the employees' work requires them to move around the workplace rather than stay at a particular workstation, an employer may have difficulty enforcing an oral solicitation rule. That difficulty, however, has never been held to be a special circumstance justifying an outright ban on employee-to-employee communications.

[18] *Fleming Co. v. NLRB*, 349 F.3d 968 (7th Cir. 2003); *Guardian Industries Corp. v. NLRB*, 49 F.3d 317 (7th Cir. 1995).

[19] As the Seventh Circuit itself has observed, it is not the obligation of the Board to "knuckle under to the first court of appeals (or the second, or even the twelfth) to rule adversely to the Board. The Supreme Court, not this circuit . . . is the supreme arbiter of the meaning of the laws enforced by the Board . . . ." *Nielsen Lithographing Co. v. NLRB*, 854 F.2d 1063, 1066 (1988). Rather, the court continued, the duty of the Board when faced with adverse circuit precedent is "to take a stance, to explain which decisions it agree[s] with and why, and to explore the possibility of intermediate solutions. . . . We do not follow stare decisis inflexibly; if the Board gives us a good reason to do so, we shall be happy to reexamine [our decisions]."

8(a)(1) by discriminatorily enforcing the CSP to all three of Prozanski's union-related e-mails.

1. The Respondent violated Section 8(a)(1) under longstanding precedent

Section 7 grants employees the right "to engage in . . . concerted activities for the purpose of collective bargaining or other mutual aid or protection. . . ." An employer violates Section 8(a)(1) by "interfer[ing] with, restrain[ing], or coerc[ing] employees" in the exercise of that right. In particular, and in accord with the decades-old understanding of discrimination within the meaning of the National Labor Relations Act, the Board has long held that an employer violates that section by allowing employees to use an employer's equipment or other resources for nonwork-related purposes while prohibiting Section 7-related uses. See, e.g., *Vons Grocery Co.*, 320 NLRB 53, 55 (1995) (bulletin board); *Honeywell, Inc.*, 262 NLRB 1402 (1982), enfd. 722 F.2d 405 (8th Cir. 1983) (bulletin board); *Union Carbide*, supra at 980 (telephone). As recently as 2005, the Board applied this principle to employee use of e-mail. See *Richmond Times-Dispatch*, 346 NLRB No. 11, slip op. at 3 (2005) (employer violated Sec. 8(a)(1) by permitting a "wide variety of e-mail messages unrelated to the Respondent's business" but prohibiting union-related messages), enfd. 225 Fed. Appx. 144 (4th Cir. 2007), cert. denied 128 S.Ct. 492 (2007); see also *E. I. du Pont de Nemours & Co.*, 311 NLRB 893, 919 (1993) (employer violated Sec. 8(a)(1) by permitting the "routine use" of e-mail by employees "to distribute a wide variety of material that has little if any relevance to the Company's business," but prohibiting the use of e-mail to distribute union literature).

Here, the record makes plain that the Respondent allowed employees to use e-mail for a broad range of nonwork-related messages, including e-mails requesting employees to participate in nonwork-related events. For example, employees and supervisors used e-mail to circulate jokes, baby announcements, and party invitations; to offer sports tickets; to seek a dog walker; to organize a poker group; and to make lunch plans. Yet, the Respondent enforced the CSP against Prozanski for sending three union-related messages. This is a clear 8(a)(1) violation under longstanding precedent.

2. The majority's standard

The majority defines "unlawful discrimination" as "disparate treatment of activities or communications of a similar character because of their union or other Section 7-protected status." According to the majority, the employer "may draw a line between charitable solicitations and non-charitable solicitations, between solicitations of a personal nature . . . and solicitations for the commercial sale of a product . . ., 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." Applying that standard to the record here, the majority finds that the Respondent permitted nonwork-related e-mails other than solicitations, but had never permitted solicitations to support any group or organization. Therefore, the majority concludes, the Respondent discriminated along Section 7 lines in applying the CSP to Prozanski's May 4 e-mail about the union rally (which was not a solicitation), but did not discriminate in applying the CSP to Prozanski's August 14 and 18 e-mails (which the majority finds were solicitations).

a. The Fleming and Guardian decisions

The majority decision is based on two Seventh Circuit cases: *Fleming Co. v. NLRB*, 349 F.3d 968 (7th Cir. 2003), denying enf. to 336 NLRB 192 (2001), and *Guardian Industries Corp. v. NLRB*, 49 F.3d 317 (7th Cir. 1995), denying enf. to 313 NLRB 1275 (1994). In *Guardian*, the Board found an 8(a)(1) violation where the employer allowed personal "swap and shop" postings advertising items for sale, but denied permission for union or other group postings, including those by the Red Cross and an employee credit union. In *Fleming*, the Board held that the employer violated Section 8(a)(1) by removing union literature from a bulletin board. Although the employee handbook stated that the bulletin boards were "for company business purposes only," the employer had allowed "a wide range of personal postings," including wedding announcements, birthday cards, and notices selling personal property such as cars and a television. There was no evidence that the employer had allowed postings for any outside clubs or organizations. 336 NLRB at 193–194. According to the credited testimony, an employee had asked permission to post a church announcement, which the employer denied. Id. at 202–203. Thus, the employer had affirmatively excluded at least one "organizational" posting other than union postings.

The Seventh Circuit denied enforcement in both cases. In *Guardian*, the court stated that discrimination "is a form of inequality" and that a person claiming discrimination "must identify another case that has been treated differently and explain why that case is 'the same' in the respects the law deems relevant or permissible as grounds of action." See id. at 319. Reasoning that "labor law is only one of many bodies implementing an antidiscrimination principle," id., the court posed several hypotheticals about whether other statutes or constitutional provisions, such as the Age Discrimination in Em-

ployment Act (ADEA) or the First Amendment, would be violated by allowing certain personal notices to be posted in the workplace, but not allowing postings by political groups or senior citizens' groups. The court found that such practices would not be discriminatory. The court also relied on *Perry Education Assn. v. Perry Local Educators' Assn.*, 460 U.S. 37 (1983), in which the Supreme Court held that a school system did not violate the First Amendment by allowing the collective-bargaining representative and certain other groups, but not a rival union, to use the school's internal mailboxes. Turning back to the facts of the case before it, the *Guardian* court noted that the employer had never allowed employees to post notices of organizational meetings. The court acknowledged that a practice of tolerating notices for anything but unions would be "antiunion discrimination by anyone's definition," id. at 321, but "[a] rule banning all organizational notices (those of the Red Cross along with meetings pro and con unions) is impossible to understand as disparate treatment of unions." Id. at 320. Accordingly, the court found that the employer's refusal to post union notices was not unlawful. Id. at 322.

In *Fleming,* the court reaffirmed *Guardian.* 349 F.3d at 975. The court noted that Fleming did not enforce its written "company use only" policy, but that "Fleming consistently excluded any posting of group or organizational notices." Id. at 974. Therefore, the court reasoned, "Fleming's *actual* practice of permitting personal postings, but not organizational ones, was consistently enforced." Id. at 975. The court then held: "Just as we have recognized for-sale notices as a category of notices distinct from organizational notices (which would include union postings), we can now add the category of personal postings." Id.[20]

b. The Seventh Circuit's analysis is inappropriate in the context of the NLRA

In analyzing whether union postings were "equal to" "swap and shop" notices, the *Guardian* court relied on case law and hypotheticals involving the First and Fourteenth Amendments and ADEA. See 49 F.3d at 320. Thus, the court implicitly assumed that the "discriminatory" enforcement of a rule in violation of Section 8(a)(1) is analogous to "discrimination" in other contexts. Cf. Rebecca Hanner White, Modern Discrimination Theory and the National Labor Relations Act, 39 Wm. & Mary L. Rev. 99, 115 (Oct. 1997) (the *Guardian* court "mistakenly . . . imported Title VII's disparate treatment approach into Section 8(a)(1)").

The hypotheticals posed by the court, however, are not analogous to an 8(a)(1) analysis. Unlike antidiscrimination statutes, the Act does not merely give employees the right to be free from discrimination based on union activity. It gives them the *affirmative* right to engage in concerted *group* action for mutual benefit and protection. Nor are employees' Section 7 rights dependent on a "public forum" analysis, as in *Perry*. Rather, in evaluating whether an employer's conduct violates Section 8(a)(1), the Board examines whether the conduct reasonably tended to interfere with those affirmative Section 7 rights. If so, the burden is on the employer to demonstrate a legitimate and substantial business justification for its conduct. *Caesar's Palace*, 336 NLRB 271, 272 fn. 6 (2001); *Jeannette Corp.*, 532 F.2d 916, 918 (3d Cir. 1976). Motive is not part of the analysis. Section 8(a)(3) separately prohibits discrimination with the motive to encourage or discourage union support.[21]

Therefore, by focusing on what types of activities are "equal" to Section 7 activities, the majority misses the point. In 8(a)(1) cases, the essence of the violation is not "discrimination." Rather, it is interference with employees' Section 7 rights. The Board's existing precedent on discriminatory enforcement—that an employer violates Section 8(a)(1) by allowing nonwork-related uses of its equipment while prohibiting Section 7 uses—is merely one application of Section 8(a)(1)'s core principles: that employees have a right to engage in Section 7 activity, and that interference with that right is unlawful unless the employer shows a business justification that outweighs the infringement. Discrimination, when it is present, is relevant simply because it weakens or exposes as pretextual the employer's business justification.[22]

[20] But see *J. C. Penney Co. v. NLRB*, 123 F.3d 988 (7th Cir. 1997) (cited in *Fleming*, supra at 974–975) (employer violated 8(a)(1) by removing union postings from bulletin boards and union bumper stickers from work carts while allowing other postings and stickers; court emphasized that the employer's enforcement of its bulletin board policy was "spotty" and rejected an argument that the stickers permitted on the work carts were "not similar in character" to union stickers, because they were personal).

[21] On that basis alone, we would have to reject the majority's definition of 8(a)(1) discriminatory enforcement as "disparate treatment of activities or communications of a similar character *because of* their union or other Section 7-protected status" (emphasis supplied). This improperly suggests that discriminatory motive is required—something even the Seventh Circuit does not propose.

[22] See, e.g., *Honeywell*, 722 F.2d at 407 (an employer's decision to allow other bulletin board postings "minimize[d] its managerial concerns"); *Sprint/United Management Co.*, supra, 326 NLRB at 399 (1998) (where the employer had "already ceded the locker space to the personal use of the employees to whom the lockers are assigned," the employer "has clearly already assumed the risk" that the presence of other materials in the lockers could cause notices the employer places there to be overlooked; "[t]hus, the [employer] cannot legitimately claim that concern as a reason for refusing to allow employees to put union literature into the lockers"); *Churchill's*, 285 NLRB at 156

Contrary to the majority's contention, this principle is not at odds with *NLRB v. Steelworkers (Nutone)*, 357 U.S. 357 (1958). In that case, the Court addressed the "very narrow and almost abstract question" of whether an employer violates the Act by enforcing a facially valid no-solicitation rule against employees when the *employer* has engaged in antiunion solicitation. Id. at 362. Thus, the case involved the employer's own communications—through its supervisors—in a campaign against the union. In declining to adopt a per se rule that an employer may never enforce a no-solicitation rule if the employer itself is engaging in antiunion solicitation, the Court noted that the employer had made exceptions to its no-solicitation rule in the past for charitable solicitation, and that there was no evidence that the union or employees had requested such an exception for their own activities. The Court then found no evidence that the rule diminished the ability of the unions to carry their message to the employees. Having previously noted that an employer's right to engage in noncoercive antiunion solicitation "is protected by the so-called 'employer free speech' provision of Section 8(c) of the Act,"[23] the Court reasoned that where the union's opportunities for reaching the employees with its pro-union message were "at least as great as the employer's ability *to promote the legally authorized expression of his antiunion views*, there is no basis for invalidating [the employer's] 'otherwise valid' rules." Id. at 364 (emphasis supplied). Thus, *Nutone* reflects the need to consider an employer's free speech right to express its views on unionization—a consideration not applicable when determining whether an employer has violated Section 8(a)(1) by allowing *employees* to communicate on some nonwork-related matters, but not on Section 7 matters. The *Nutone* Court never discussed the latter issue, which was not before it. Thus, the majority grossly overstates the scope of *Nutone* by contending that the Court "rejected" the general notion that disparate treatment of two groups "not similarly situated" undermines the employer's business justification and therefore violates Section 8(a)(1). No such discussion appears in the Court's decision, and *Nutone* has little, if any, relevance here.[24]

Rather, under the basic Section 8(a)(1) principles discussed above, if an employer wants to "draw a line" between permitted and prohibited e-mails—or, for that matter, between permitted and prohibited bulletin board postings, telephone calls, or other uses of employer equipment or media—based on whether the employees are urging support for "groups" or "organizations," the employer must show some legitimate business reason for drawing that particular line, and that business justification must outweigh the interference with Section 7 rights. Otherwise, the employer's rule is completely antithetical to Section 7's protection of concerted activity.[25] The Seventh Circuit and majority fail to engage in this analysis. In any event, the Respondent has not offered any such justification here.

Taken to its logical extreme, the majority's holding that an employer need only avoid "drawing a line on a Section 7 basis" is a license to permit almost anything but union communications, so long as the employer does not expressly say so.[26] It is no answer to say that a rule

("When an employer singles out union activity as its only restriction on the private use of company phones, it is not acting to preserve use of the phones for company business. It is interfering with union activity . . . ."); White, supra at 111 ("Under a [S]ection 8(a)(1) balancing approach, an employer that permits solicitation by employees during working time for nonunion activities is hard-pressed to stand on its managerial interests in production and discipline when the working time solicitation is on behalf of the union.") (citations omitted).

[23] Id. at 362. Sec. 8(c) states: "The expressing of any views, argument, or opinion, or the dissemination thereof, whether in written, printed, graphic, or visual form, shall not constitute or be evidence of an unfair labor practice under any of the provisions of this Act, if such expression contains no threat of reprisal or force or promise of benefit."

[24] The Board decisions cited by the majority are also inapposite. In *Salmon Run Shopping Center*, 348 NLRB No. 31 (2006), the Board found that the employer's exclusion of nonemployee union organizers from the premises was discriminatorily motivated. Because *Salmon Run* involved access by nonemployees, it implicated the employer's property interests, not just its managerial interests. See id., slip op. at 1. Even aside from that distinction, the fact that the employer in *Salmon Run* had a discriminatory motive for excluding the union does not mean that proof of such a motive is *required* in order to find a violation.

Enloe Medical Center, 348 NLRB No. 63 (2006), involved a facially discriminatory rule (barring union literature, but nothing else, from the breakroom), not a facially neutral rule that was discriminatorily applied. In any event, the fact that a rule will violate Sec. 8(a)(1) if it expressly singles out union activity does not establish that an express "singling out" is required in order to find a violation. In short, *Salmon Run* and *Enloe* are examples of particularly clear-cut and obvious violations, but nothing in those decisions suggests that they limit the circumstances under which a violation may be found, redefine "discrimination," or otherwise modify the Board's longstanding precedent.

[25] For similar reasons, we reject as utterly meritless the Respondent's argument that, because employee Suzi Prozanski sent her e-mails in her capacity as union president, her right of access to the computer system must be evaluated under the *Lechmere* standard governing nonemployee access to an employer's premises. Prozanski was an employee as well as the union president. To contend that an employee who engages in activity on behalf of her union no longer has the Section 7 rights of an employee, but only the "derivative" rights of a nonemployee, is nonsensical. When employees communicate with one another about union or other Section 7 matters, whether or not they act "for" their union, they are exercising their own, nonderivative Section 7 rights. See *Nashville Plastic Products*, 313 NLRB 462, 463 (1993) ("the rule enunciated in *Lechmere* does not apply to employees").

[26] For example, an employer might prohibit all nonwork-related solicitations by membership organizations. Such a rule would extend privileges to employee solicitations on behalf of any commercial enterprise and many charities and other activities, but not to employee solici-

prohibiting all noncharitable solicitations or all solicitations for a group or organizations is not discriminatory because it would also prohibit selling Avon or Amway products. The Act does not protect against interference with those activities; it does protect against interference with Section 7 activity. Accordingly, we would adhere to precedent, which properly reflects that principle.

3. The Respondent violated Section 8(a)(1) even under the majority's standard

In any event, even under the majority's standard, the Respondent's enforcement of the CSP was unlawful with respect to all three of Prozanski's e-mails: the May 4 e-mail "setting the record straight" about the union rally, the August 14 e-mail urging employees to wear green to support the Union, and the August 18 e-mail urging participation in the Union's entry in a town parade.

First, assuming that Prozanski's August 14 and 18 e-mails were "solicitations" and that the Respondent could lawfully draw a line between "solicitations to support any group or organization" and other messages, as the majority contends, that is not the line the CSP drew. By its terms, the CSP barred all "non-job-related solicitations," whether or not they urge support for a "group or organization." Yet, the Respondent allowed other personal "solicitations"—which violated the terms of the CSP—while disallowing Prozanski's union-related "solicitations."

Second, even the Seventh Circuit recognized that if an employer allowed notices for anything except unions, "that is anti-union discrimination by anyone's definition." *Guardian*, supra at 321. In *Fleming*, the employer had denied an employee's request to post a church announcement. 336 NLRB at 202–203. In *Guardian*, the employer routinely excluded all "organizational" requests. Here, there is no clear evidence that the Respondent ever enforced the CSP against *anything other than* union-related messages. That is unlawful discrimination "by anyone's definition." *Guardian*, supra at 321.

tations on behalf of the union representing the employees—the entity through which the employees have chosen to vindicate their Sec. 7 right to engage in concerted activity. In other words, the rule would permit employees to solicit on behalf of virtually anything *except* a union. Yet, on its face, this policy would not "draw the line" on Sec. 7 grounds, and would therefore be lawful. Such a result stands labor law on its head.

The majority notes that a line drawn out of antiunion motive will still be unlawful. As noted above, however, motive is not an element of this type of 8(a)(1) violation.

B. The Respondent's Discipline of Prozanski Violated Section 8(a)(3) and (1)

Applying *Wright Line*,[27] the judge found that the Respondent violated Section 8(a)(3) and (1) by issuing written warnings to Prozanski on May 5 and August 22 for sending union-related e-mails. The majority, finding *Wright Line* inapplicable here, affirms the violation as to the May 5 discipline, but reverses as to the August 22 warning.

We agree with the majority that a *Wright Line* analysis is inappropriate. However, for the reasons stated below, we would find both warnings unlawful.

First, we would find that the CSP's prohibition on using e-mail for any "non-job-related solicitations" was unlawful on its face. Therefore, the discipline of Prozanski on May 5 and August 22 pursuant to that policy was unlawful. *Saia Motor Freight Line*, 333 NLRB 784, 785 (2001) (discipline pursuant to overbroad no-solicitation/no-distribution rule violated Sec. 8(a)(3) and (1) without consideration of *Wright Line*).

Alternatively, even assuming the policy was lawful, we agree with the majority that it was discriminatorily enforced with respect to the May 4 e-mail. Therefore, the Respondent's May 5 discipline of Prozanski for sending that e-mail violated Section 8(a)(3) and (1). As explained above, we would also find that the CSP was discriminatorily enforced with respect to the August 14 and 18 e-mails. Accordingly, the second, August 22 warning for sending those e-mails also violated Section 8(a)(3) and (1). See *St. Joseph's Hospital*, 337 NLRB 94, 95 (2002) (warning for displaying union-related screen saver violated Sec. 8(a)(3) where employer allowed other nonwork-related screen savers), enfd. 55 Fed. Appx. 902 (11th Cir. 2002).

D. The Respondent's Insistence on an Illegal Bargaining Proposal

The judge found that the Respondent violated Section 8(a)(5) and (1) by insisting on the proposal known as counterproposal 26, which stated that the Respondent's electronic communication systems could not be used for "union business." The majority reverses the judge, finding that the evidence fails to show "insistence" on the proposal. The majority finds it unnecessary to pass on whether the proposal was unlawful. We dissent.

First, we agree with the judge that counterproposal 26 was an illegal codification of the Respondent's discriminatory practice of allowing e-mail use for a broad range of nonwork-related messages, but not for union-related

[27] 251 NLRB 1083 (1980), enfd. 662 F.2d 899 (1st Cir. 1981), cert. denied 455 U.S. 989 (1982), approved in *NLRB v. Transportation Management Corp.*, 462 U.S. 393 (1983).

messages. Second, for the reasons stated below, we disagree with the majority's finding of no "insistence."[28]

A party may not continue to insist on a nonmandatory proposal in the face of the other party's "clear and express refusal" to bargain over it. *Laredo Packing Co.*, 254 NLRB 1, 19 (1981). Here, the Union responded to the proposal by stating that it would not respond, because the proposal illegally restricted Section 7 rights. The Union also filed an 8(a)(5) charge. After that charge was dismissed, the Union sought clarification regarding the scope of the proposal, but still expressed concern that it was illegal. The majority notes that at an April 21 bargaining session, the Union's lead negotiator stated that "I'm here to bargain a proposal." However, he also stated at various points during the discussion that "it makes it very difficult to bargain this issue if we don't know what would be allowed and what wouldn't be allowed. . . . In order to bargain it, we need to know how it would work." Indeed, at the April 21 session, the Respondent accused the Union of failing to bargain over the proposal and instead simply "taking notes" to appeal the dismissal of the first 8(a)(5) charge.

The evidence as a whole, including bargaining notes from the April 21 session, indicates that the parties had not begun substantive bargaining over the proposal; rather, the Union was still seeking clarification of what the proposal meant. Furthermore, on April 24, 2001, the Union filed a new 8(a)(5) charge alleging that the Respondent had proposed and "refused to withdraw" counterproposal 26. If the Respondent had any doubt about the Union's position after the April 21 bargaining session, the filing and service of the charge put it on notice that the Union did not want to discuss counterproposal 26. Nevertheless, the Respondent still did not withdraw the proposal.

Under the above circumstances, we find that the Union communicated a "clear and express refusal" to bargain over counterproposal 26, and that the Respondent nevertheless continued to insist on the proposal. Accordingly, we would adopt the 8(a)(5) violation.

III. CONCLUSION

The majority decision, particularly those portions addressing the maintenance and enforcement of the CSP, does damage to employee Section 7 rights on multiple levels. First, the majority fails to heed the Supreme Court's instruction that the Board must "adapt the Act to changing patterns of industrial life"[29]—here, the explosion of electronic mail as a primary means of workplace communication. Second, the majority erroneously treats the employer's asserted "property interest" in e-mail—a questionable interest here, in any event—as paramount, and fails to give due consideration to employee rights and the appropriate balancing of the parties' legitimate interests. Third, the majority blurs the "distinction of substance" between the rights of employees and those of nonemployees.[30] Finally, the majority discards the Board's longstanding test for discriminatory enforcement of a rule, replacing it with a standard that allows the employer virtually unlimited discretion to exclude Section 7 communications, so long as the employer couches its rule in facially neutral terms. Accordingly, we dissent.

Dated, Washington, D.C. December 16, 2007

Wilma B. Liebman, Member

Dennis P. Walsh, Member

NATIONAL LABOR RELATIONS BOARD

APPENDIX

NOTICE TO EMPLOYEES
POSTED BY ORDER OF THE
NATIONAL LABOR RELATIONS BOARD
An Agency of the United States Government

The National Labor Relations Board has found that we violated Federal labor law and has ordered us to post and obey this notice.

FEDERAL LAW GIVES YOU THE RIGHT TO

Form, join, or assist a union

Choose representatives to bargain with us on your behalf

Act together with other employees for your benefit and protection

Choose not to engage in any of these protected activities.

WE WILL NOT discriminatorily prohibit employees from using our electronic communications system to send union-related messages.

WE WILL NOT maintain an overly broad rule prohibiting employees from wearing or displaying union insignia while working with customers.

WE WILL NOT issue written warnings to, or otherwise discriminate against, any employee for supporting the

[28] We do not rely on *California Pie Co.*, 329 NLRB 968, 974 (1999), cited by the judge to support his finding of insistence. In that case, there were no exceptions to the finding that the respondent insisted on an illegal subject.

[29] *NLRB v. J. Weingarten*, 420 U.S. 251, 266 (1975).

[30] *Babcock & Wilcox*, supra at 113.

Eugene Newspaper Guild, CWA Local 37194 or any other labor organization.

WE WILL NOT in any like or related manner interfere with, restrain, or coerce employees in the exercise of the rights set forth above.

WE WILL rescind the rule prohibiting circulation department employees from wearing or displaying union insignia while working with customers.

WE WILL, within 14 days from the date of the Board's Order, rescind the unlawful warning issued to Suzi Prozanski on May 5, 2000, remove from our files any reference to the unlawful warning, and within 3 days thereafter notify Prozanski in writing that this has been done and that the warning will not be used against her in any way.

THE GUARD PUBLISHING COMPANY D/B/A THE REGISTER-GUARD

Jill Wrigley, Esq., for the Charging Party.
L. Michael Zinser, Esq., of Nashville, Tennessee, for the Respondent.

DECISION

STATEMENT OF THE CASE

JOHN J. MCCARRICK, Administrative Law Judge. This case was tried in Eugene, Oregon, on November 14–16, 2001, upon the General Counsel's second consolidated complaint (complaint) alleging that The Guard Publishing Company d/b/a The Register-Guard (Respondent) violated Section 8(a)(1), (3), and (5) of the Act by maintaining, promulgating and enforcing an overly broad no-solicitation policy, by promulgating and maintaining an insignia policy prohibiting display of union insignia or signs, by discriminatorily enforcing its no-solicitation policy by warning Suzi Prozanski (Prozanski)[1] on May 5 and August 22, 2000,[2] and by proposing an illegal subject during collective bargaining with Eugene Newspaper Guild, CWA Local 37194 (Union). Respondent filed a timely answer to the complaint and denied any wrongdoing. On the entire record,[3] including my observation of the demeanor of the witnesses, and after considering the briefs filed by the parties, I make the following

FINDINGS OF FACT

I. JURISDICTION

The Respondent, an Oregon corporation, publishes a newspaper at its Eugene, Oregon facility, where it annually had gross sales of goods and services valued in excess of $200,000 and held membership in or subscribed to interstate news services, published nationally syndicated features and advertised nationally sold products. The Respondent admits and I find that it is an employer engaged in commerce within the meaning of Section 2(2), (6), and (7) of the Act and that the Union is a labor organization within the meaning of Section 2(5) of the Act.

II. ALLEGED UNFAIR LABOR PRACTICES

A. The Issues

1. Does Respondent's communications policy constitute an overly broad no-solicitation rule in violation of Section 8(a)(1) of the Act?

2. Has Respondent enforced its communications policy in a discriminatory manner in violation of Section 8(a)(1) of the Act?

3. Has Respondent implemented and maintained an overly broad rule prohibiting the wearing of union insignia or the display of signs soliciting support for the union in violation of Section 8(a)(1) of the Act?

4. Did Respondent's May 5 and August 22 warnings to Prozanski for violating Respondent's communications policy violate Section 8(a)(1) and (3) of the Act?

5. Did Respondent's October 25 counterproposal 26 prohibiting use of Respondent's e-mail systems for union business, constitute an illegal subject of bargaining which violated Section 8(a)(5) of the Act?

B. The Facts

1. Background

Respondent publishes The Register-Guard, a daily newspaper with circulation in the Eugene, Oregon area. The Union represents about 150 of Respondent's employees in the editorial, circulation, business office, display and classified advertising, human relations, promotion and information systems departments. These departments include, inter alia, reporters, photographers, copy editors, secretaries, clerks, advertising department employees and district managers in the circulation department. The last collective-bargaining agreement between Respondent and the Union was for the period October 16, 1996 to April 30, 1999. Respondent and the Union have been negotiating for a new agreement but have not yet entered into a successor contract.

Respondent began installing a computer and information system at its Eugene facility in March 1996 and had fully implemented the system, with internet and electronic mail (e-mail) capability in the summer of 1997. All of Respondent's employees with the exception of 15 district managers have access to e-mail. While most employees have their own computer terminal, a few employees, such as the 12 outside salespersons, share a terminal and have e-mail access.

On October 4, 1996, Respondent promulgated a written Company communications policy that applies to the use of Respondent's communications systems including telephones, message machines, computers, fax machines and photocopy machines. Under the heading "general guidelines" the policy provides, "Communications systems are not to be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations." The general guidelines further state that "Improper use of Company communication systems will result in discipline, up to and including termination." The initial draft of the communications policy was issued on September 4, 1996. On September 12, 1996, the Union requested bargaining over the use of the electronic communications system. However, there is no evidence that the parties executed a written agreement reflecting an accord regarding the communications policy.

2. May 5 and August 22 warnings to Prozanski

Respondent has employed Prozanski for about 17 years. She currently works as a copy editor in the newsroom features department. Prozanski is a member of the Union and has served as union president since January 2000. In her capacity as copy editor, Prozanski has her own desk and computer with internet and e-mail functions. Prozanski uses e-mail for both work and nonwork purposes. In her work Prozanski uses e-mail to make story lists, compile photographs, review stories and to send memos to coworkers regarding work topics. She also sends and receives e-mails on a regular basis for nonwork purposes. For example, Prozanski sends and receives e-mail about union business or to advise fellow workers she is going on a break.

On May 4, Prozanski, in her capacity as union president, sent e-mail from her computer at work to about 50 coworkers at their work e-mail addresses. The e-mail dealt with a rally that took place on May 1. Prozanski told Respondent's managing editor, Dave Baker, she was going to send the e-mail and he replied, "OK, I understand." About 5 minutes later, Baker returned and told Prozanski she should not send the e-mail. On May 5, Baker issued Prozanski a written warning for violating the Respondent's communications policy for sending a union-related e-mail on May 4.

On August 14, Prozanski sent e-mail from the union office to Respondent's employees at their work e-mail addresses advising them to wear green in support of union efforts to gain a raise for employees and a contract. On August 18, Prozanski sent another e-mail from the union office to Respondent's employees at their work e-mail addresses urging them to participate in the Union's entry in the Eugene celebration parade. On August 22, Cynthia Walden, Respondent's director of human relations, issued a written warning to Prozanski for sending the August 14 and 18 Guild-related e-mails to employee workstations in violation of Respondent's communications policy.

Respondent's employees testified without contradiction that both they and their managers used e-mail at work for nonbusiness purposes without reprimand. In addition to Prozanski, Respondent's reporters Lance Robertson (Robertson), Randi Bjornstad (Bjornstad), William Bishop (Bishop), and Kimber Williams (Williams) sent and received e-mail at work from employees and managers regarding parties, jokes, breaks, community events, sporting events, births, meeting for lunch, and poker games. Respondent's general manager, Dave Baker (Baker) admitted that he has received personal e-mail from other employees and has not disciplined them. Numerous e-mails were offered into evidence that reflect employees, supervisors and managers have sent and received personal e-mail at work without discipline. The following e-mails were sent by managers or supervisors: On March 18, city editor, Margaret Haberman, e-mailed an unspecified group of employees that she was throwing a party in honor of her 40th birthday. On September 1, assistant city editor, Scott McFetridge, sent e-mail to over 20 employees announcing a going away party. On March 30, assistant city editor, Lloyd Paseman, e-mailed employees, managers and supervisors seeking someone to walk a reporter's dog. On March 14, assistant news editor, Paul Yarbrough, sent e-mail to employees and supervisors that he had basketball tickets available. On November 8, deputy managing editor, Carl Davaz, sent e-mail to all employees listing among other business related items, a birth announcement. On July 28, graphics editor, R. Romig, announced a party to numerous employees by e-mail. On October 8 and 10, managing editor, Baker, sent e-mail to all employees announcing the United Way Campaign and soliciting assistance from employees in the campaign.

3. December 12—Kangail's armband and placard

Ronald Kangail (Kangail) worked for Respondent as a district manager since 1977. He is a member of the Union and is part of the bargaining unit. As a district manager Kangail deals with newspaper carriers, subscribers and businesses in his district and also in his office. While in the field, Kangail drives his own vehicle. Neither Kangail nor any of the other district managers are required to wear a uniform when dealing with the public. In his office at Respondent's facility, Kangail has union material displayed that he has not been required to remove.

In November Kangail began to wear a green armband to show support for the Union and to demonstrate the Union did not have a contract with Respondent. At the same time he displayed a green placard in the window of his vehicle while working in the field. The placard was 8-1/2 by 11 inches in size and stated:

WORKERS AT THE
REGISTER-GUARD
DESERVE A FAIR CONTRACT!
SUPPORT THE
EUGENE NEWSPAPER GUILD.
Want to help? Call 343-8625.

[1] In its answer, Respondent contends that this allegation is not encompassed by the underlying unfair labor practice charges and is timebarred by Section 10(b) of the Act. A complaint is not restricted to the precise allegations of the charge. As long as there is a timely charge, the complaint may allege any matter sufficiently related to or growing out of the charged conduct. *NLRB v. Fant Milling Co.*, 360 U.S. 301, 309 (1959). The test that applies for adding related uncharged allegations is stated in *Redd-I, Inc.*, 290 NLRB 1115, 1115–1116 (1988). In applying the closely related test set forth in *Redd-I*, the Board looks at three factors. Whether the untimely allegation involves the same legal theory as the timely charge. Whether the untimely allegation arises from the same factual circumstances or sequence of events as the timely charge. Whether the respondent would raise the same or similar defenses to both allegations. I find that the allegation in the complaint is closely related to the timely charge in Case 36–CA–8743.

[2] All dates are in 2000, unless otherwise indicated.

[3] At the end of the trial counsel for the General Counsel without objection requested leave to submit official Board documents to explain the status of Case 36–CA–8075. On November 20, 2001, counsel for the General Counsel submitted the order consolidating cases, consolidated complaint and notice of hearing dated February 29, 2000 in Case 36–CA–8075. There being no objection to its introduction into the record, this document will be received as GC Exh. 63.

On December 12, Kangails' supervisor, Zone Manager Steve Hunt (Hunt) told Kangail to remove the armband from his arm and the placard from his car when he was in the field. Kangail complied with the directive. Other district managers wore insignia while in the field including hats with the logos of football teams and the Marine Corps and shirts displaying college names. Respondent has no written policy or rules concerning the display of insignia or signs at work. There was contradictory testimony from Advertising Director Michael Raz (Raz) and Circulation Director Charles Downing (Downing) concerning exactly what Respondent's policy was concerning wearing insignia when dealing with the public. Raz said the policy was that, ". . . employees could not wear or exhibit indicia that are controversial in nature, or partisan or political, or in—otherwise represent the company in a negative context." Downing testified that the policy was, "That while in the execution of their duties in the field, they're not to wear anything that is not appropriate to the business."

4. October 26—Respondent proposes contract language prohibiting unit employees from using Respondent's electronics communications systems for union matters

On about October 25, during the course of bargaining for a new collective-bargaining agreement, Respondent proposed the following contract language:

Company Counterproposal No. 26
October 25, 2000

Article XVII

Section 8. Electronic Communications Systems—The electronic communications systems are the property of the Employer and are provided for business use only. They may not be used for union business.

On November 15, Respondent clarified its position with respect to Company counterproposal 26. In a statement of position Respondent reaffirmed that it's "contract proposal only prohibits use of the systems for union business." The position statement added, "Attached to this statement of position is the Company's current Communication's [sic] Policy. It is our intention that this attached policy will govern the use of systems in situations 'other than' union business." On November 16, the Union responded that it would not reply to Company counterproposal 26 since it illegally restricted employees' rights to concerted activity in the workplace. Two weeks later the Union filed a charge in Case 36–CA–8789 on November 30, 2001, alleging that Respondent violated Section 8(a)(5) of the Act by making Company counterproposal 26. The Region dismissed the charge on March 30, 2001, and the Union filed an appeal to the General Counsel. On August 13, 2001, the Region revoked the dismissed charge in Case 36–CA–8789. Meanwhile the Union asked Respondent for further clarification of Company counterproposal 26. In a letter dated April 9, 2001, the Union asked Respondent to address four questions. The letter asks in pertinent part:

1. Does the e-mail ban apply to bargaining unit members who are discussing "union business" or solely to elected officers and representatives of the Guild?

2. Does "union business" include the expression of ideas and opinions by bargaining unit members regarding the Guild in its representative role? Would it ban employee use of e-mail to critique the course of ongoing contract negotiations or the terms of the collective bargaining agreement? To discuss the Guild's position in bargaining? To discuss the Guild's handling of employee grievances? To discuss the status of an unfair labor practice charge or an arbitration matter being pursued by the Guild on behalf of the bargaining unit?

3. Does the e-mail ban cover workplace discussion by co-workers of candidates for Guild office? The expression of employee opinion to co-workers on the quality of representation being offered by the Guild? Could a Register-Guard worker properly communicate by company e-mail to a co-worker criticism or opinion regarding Guild action as bargaining representative of the actions of its elected officers?

4. Could a Register-Guard employee use the company e-mail to discuss the merits of a proposed Guild dues increase?

Respondent replied in writing on April 21, 2001. This response stated in pertinent part:

We will now attempt to answer your questions in the order asked:

1. The proposal applies to all employee[s] covered by the contract as well as officers and representatives.

2. As a general rule the proposal will apply to all union business. We are not going to, in advance, try to prejudge all possible hypothetical acts and circumstances. See final paragraph below.

3. Same as answer number 2.

4. No.

By agreeing to this proposal we are not asking the union to waive any rights employees may hypothetically have regarding the selection of a new union and/or to decertify Guild Local 194. This proposal is intended to cover the conduct of union business and the employees represented by this union under this contract while it represents them. We express, with this proposal, no position with respect to use of our systems in that circumstance because we are not bargaining about that circumstance. Whatever our position is in that regard we will make that decision at the time that the circumstances present itself, but independent of Company Counterproposal No. 26.

Also on August 21, 2001, a bargaining session took place between the Union and Respondent. Attorney L. Michael Zinser and Director of Human Relations Cynthia Walden represented Respondent. Lance Robertson represented the Union. Union member Randi Bjornstad contemporaneously recorded bargaining notes of this session. The notes reflect that Zinser advised that counterproposal 26 applied to all members of the bargaining unit who were discussing any union business. Zinser further said that counterproposal 26 would not address the issue of employee attempts to decertify the Union. To date Respondent has not withdrawn counterproposal 26. After all witnesses had been called, Zinser took the stand and testified over the objection of the General Counsel and Charging Party. Zinser denied that on August 21, 2001, he said Respondent's e-mail system could be used to decertify the Union.

C. The Analysis

1. Respondent's communications policy

The General Counsel and the Union contend that Respondent's maintenance of its communications policy is an overbroad prohibition on employees' rights to make solicitations regarding Section 7 subjects. Both the General Counsel and the Union argue that the employer's computers and computer systems, including e-mail, constitute a work area within the meaning of *Republic Aviation Corp.*[4] Since the communications policy ban on nonbusiness use of e-mail includes solicitation and is not limited to working time, it is presumptively unlawful. Respondent argues that it has a right to prohibit the use of its personal property for nonbusiness purposes and that the Union agreed to the communications policy.

a. The law

The Board has generally found that an employer may validly limit employee use of its communications equipment. The Board has held that employees have no statutory right to use an employer's equipment or media. *Mid Mountain Foods, Inc.,* 332 NLRB 229, 230 (2000). Thus the Board has found no violation in nondiscriminatory limits on the use of employer bulletin boards,[5] telephones,[6] public address systems,[7] video equipment,[8] and e-mail.[9]

b. The analysis

While the General Counsel and Charging Party argue that Respondent's e-mail system amounts to a workplace and that employee solicitation cannot be totally banned without justification, I find the argument misplaced. The Board has yet to hold that an e-mail system owned by an employer constitutes a workplace where an employer is prohibited from limiting all employee Section 7 solicitation. Rather, the Board has consistently found that employers may nondiscriminatorily limit the use of their communications equipment without infringing on employees' rights to solicit for Section 7 purposes. I find that Respondent's communications policy is not a facially overbroad no-solicitation/no-distribution rule but rather a valid limit on the use of its communications equipment. I will dismiss this portion of the complaint.

2. The May 5 and August 22 discipline of Prozanski

Both the General Counsel and Charging Party argue that Respondent's communications policy was applied to Prozanski in a discriminatory fashion. Thus they contend that the implementation of the policy itself violated Section 8(a)(1) of the Act. Since Respondent applied the communications policy to Prozanski due to her activities on behalf of the Union, the General Counsel and Charging Party take the position Respondent violated Section 8(a)(3) of the Act. Respondent contends that it applied its communications policy in a uniform manner that limited all use of its e-mail system by third party organizations. Thus, its discipline of Prozanski was neither a violation of Section 8(a)(1) or (3) of the Act.

a. The law

While an employer may limit the personal use of its property by employees, it may not do so in a manner that discriminates against employees' Section 7 rights. In a case involving the use of an employer's e-mail system, the Board in *E. I. du Pont de Nemours & Co.*, 311 NLRB 893, 919 (1993), found that the employer violated Section 8(a)(1) of the Act by allowing use of its e-mail system by employees for a wide variety of personal subjects but prohibited employees from using e-mail to distribute any union material.

Section 8(a)(3) of the Act prohibits employers from discriminating in regard to an employee's "tenure of employment . . . to encourage or discourage membership in any labor organization."[10]

In 8(a)(3) cases the employer's motivation is frequently in issue, therefore the Board applies a causation test to resolve such questions. *Wright Line*, 251 NLRB 1083, 1088 (1980). The *Wright Line* test requires the General Counsel to make a prima facie showing sufficient to support an inference that the employee's protected conduct motivated the employer's adverse action. "The critical elements of discrimination cases are protected activity known to the employer and hostility toward the protected activity." *Western Plant Services*, 322 NLRB 183, 194 (1996). Although not conclusive, timing is usually a significant element in finding a prima facie case of discrimination. Id. at 194.

If the General Counsel successfully presents a prima facie case of discrimination, the burden then shifts to the employer to persuade the trier of fact that the same adverse action would have occurred even in the absence of the employee's protected activity. *Western Plant,* supra. To meet this burden, "an employer cannot simply present a legitimate reason for its action but must persuade by a preponderance of the evidence that the same action would have taken place even in the absence of the protected conduct." *Roure Bertrand Dupont, Inc.,* 271 NLRB 443 (1984).

b. The analysis

The record is replete with evidence of personal use of Respondent's e-mail system by its employees and managers both before and after Respondent disciplined Prozanski. Respondent's argument that it limited all e-mail use by third party

[4] 51 NLRB 1186 (1943), enfd. 142 F.2d 193 (2d Cir. 1944), affd. 324 U.S. 793 (1945).

[5] *Honeywell, Inc.*, 262 NLRB 1402 (1982), enfd. 722 F.2d 405 (8th Cir. 1983).

[6] *Union Carbide Corp.*, 259 NLRB 974, 980 (1981), enfd. in relevant part 714 F.2d 657, 663–664 (6th Cir. 1983).

[7] *The Heath Co.*, 196 NLRB 134 (1972).

[8] *Mid Mountain Foods, Inc.*, supra.

[9] *Adtranz AAB Daimler-Benz Transportation NA, Inc.*, 331 NLRB 291 (2000). In affirming the ALJ's decision, the Board noted that no exceptions were filed to the judge's finding that Respondent's ban on nonbusiness use of its e-mail system did not violate Sec. 8(a)(1) of the Act.

[10] 29 U.S.C. Sec. 158(a)(3).

organizations, including the Union, misses the mark. First, there is evidence that Respondent permitted third party organizations such as Weight Watchers and United Way access to e-mail; second, the Board has drawn no distinction between nonbusiness use of communications equipment by third party organizations as opposed to personal use by employees. If an employer allows employees to use its communications equipment for nonwork related purposes, it may not validly prohibit employee use of communications equipment for Section 7 purposes. *Fleming Co.,* 336 NLRB 192, 194 (2001). The evidence reflects Respondent has failed to enforce its communications policy. It has permitted personal use of e-mail for a wide variety of nonbusiness purposes. Having permitted a plethora of nonbusiness uses of e-mail, Respondent cannot validly prohibit e-mail dealing with Section 7 subjects. Respondent's argument that Prozanski's use of e-mail was a more egregious violation of the communications policy since they were sent to multiple persons (spam) is without merit. First, the practice of sending e-mail to multiple recipients was common practice by both employees and managers. Second, there has been no evidence that sending e-mail to many addressees has any adverse impact on discipline or production. I find Respondent's enforcement of its communications policy in the May 5 and August 22 discipline of Prozanski violated Section 8(a)(1) of the Act.

It is clear that Prozanski was engaged in union activity at the time she sent her e-mail messages on May 4, August 14 and 18. She sent the e-mail to union members on behalf of the Union. Moreover, there is no dispute that Respondent was aware of Prozanski's union activity. Respondent noted in the disciplinary letters of May 5 and August 22 that Prozanski was engaged in Guild activity when she sent the e-mail. Respondent stated in both disciplinary letters that Prozanski was being disciplined for sending the union-related e-mail in violation of its communications policy. The General Counsel has established each prima facie element of its case establishing Respondent disciplined Prozanski in violation of Section 8(a)(3) of the Act. The burden shifts to Respondent to prove that it would have disciplined Prozanski even in the absence of her union activity.

Respondent's defense is based upon a faulty premise. It assumes that the communications policy was enforced in a consistent, nondiscriminatory fashion. As noted above, the communications policy was observed in the breach not the enforcement. Having permitted a wide variety of nonbusiness use of its e-mail, Respondent cannot rely on this policy to establish it would have disciplined Prozanski in the absence of her union activity. I find Respondent's May 5 and August 22 discipline of Prozanski violated Section 8(a)(3) of the Act.

3. Respondent's insignia policy

The General Counsel and Charging Party contend that Respondent violated Section 8(a)(1) of the Act by enforcing an unwritten insignia policy that prohibited employee Ronald Kangail from wearing union insignia and displaying a union placard at work. Respondent argues that it had the right to prohibit employees from wearing and displaying union insignia when dealing with the public.

a. The law

While working, an employee's right to wear and display union insignia is protected by Section 7 of the Act. *Republic Aviation Inc. v. NLRB*, 324 U.S. 793 (1945); *Albertson's Inc*., 319 NLRB 93, 102 (1995). This right is balanced against an employer's right to operate its business. An employee's right to wear insignia can be limited or prohibited only if the employer can show such a ban on Section 7 rights is mandated by "special circumstances." *Mack's Supermarket*, 288 NLRB 1082, 1098 (1988). Such special circumstances include employee safety, protecting the employer's product or image, and ensuring harmonious employee relations. *Nordstrom, Inc.,* 264 NLRB 698, 700 (1982). Mere exposure of customers to union insignia does not constitute a special circumstance. *Flamingo Hilton-Laughlin,* 330 NLRB 287 (1999).

b. The analysis

There is no dispute that Kangail was wearing union insignia and displaying a union placard in his car while working for Respondent and dealing with the public. Nor is there any controversy that Respondent directed Kangail to refrain from wearing his armband or from displaying his placard when dealing with the public. While Kangail's display of union insignia was protected by Section 7 of the Act, Respondent has failed to show any special circumstance that would justify its ban on Kangail's armband and placard in his auto while dealing with the public. Thus, no probative evidence was adduced that Kangail's display adversely affected Respondent's business, employee safety, or employee discipline. Moreover, Respondent's vague, unwritten insignia policy has not been enforced in a wide variety of other situations. District managers wore insignia, including baseball caps and shirts with various logos, while dealing with the public. I find that by promulgating and enforcing its unwritten insignia rule prohibiting the display of union insignia in December 2000, Respondent violated Section 8(a)(1) of the Act.

4. The October 25 counterproposal 26

The General Counsel and Charging Party argue that Respondent's counterproposal is an illegal subject of bargaining. It is argued that Respondent's continued insistence on counterproposal 26 in collective bargaining violated Section 8(a)(5) of the Act. Respondent contends that counterproposal 26 is a mandatory subject of bargaining. Consequently, there is no violation of Section 8(a)(5) of the Act.

a. The law

Neither party may require the other to agree to contract provisions that are unlawful under the Act. *National Maritime Union (Texas Co.),* 78 NLRB 971, 981–982 (1948), enfd. 175 F.2d 686 (2d Cir. 1949). However, merely proposing or bargaining about an illegal subject does not necessarily violate the Act. A violation occurs when the opposing party has rejected the illegal proposal and the proponent continues to insist on the illegal subject. In *California Pie Co.,* 329 NLRB 968, 974 (1999), the Board found insistence on an illegal proposal violated Section 8(a)(5) of the Act.

b. The analysis

Respondent contends that counterproposal 26 must be read in conjunction with the entire communications policy that applies to all employees. Its argument seems to be that the union ban on use of communications equipment in counterproposal 26 is part and parcel of the companywide ban on all nonbusiness use of communications equipment. This argument might hold water but for the fact that there was no enforcement of the communications policy on nonbusiness use, other than union use, of communications equipment. Consequently, Respondent's counterproposal 26 is an unlawful codification of a discriminatory policy and constitutes an illegal subject of bargaining.[11] The Union repeatedly objected to this counter proposal and filed an unfair labor practice charge with the Board. The Region dismissed this charge and later revoked the dismissal. Respondent's refusal to withdraw its illegal proposal violated Section 8(a)(5) of the Act.

CONCLUSIONS OF LAW

1. By maintaining a rule which prohibits employees from wearing of union insignia and by discriminatorily maintaining and enforcing a rule which prohibits use of communications equipment for union purposes Respondent has engaged in unfair labor practices affecting commerce within the meaning of Section 8(a)(1) and Section 2(6) and (7) of the Act.

2. By warning Suzi Prozanski on May 5 and August 22 Respondent violated Section 8(a)(1) and (3) and Section 2(6) and (7) of the Act.

3. By proposing, insisting upon and refusing to withdraw counterproposal 26 during collective bargaining, Respondent violated Section 8(a)(1) and (5) and Section 2(6) and (7) of the Act.

REMEDY

Having found that the Respondent has engaged in certain unfair labor practices, I find that it must be ordered to cease and desist and to take certain affirmative action designed to effectuate the policies of the Act.

On these findings of fact and conclusions of law and on the entire record, I issue the following recommended[12]

ORDER

The Respondent, Guard Publishing Company d/b/a The Register-Guard, Eugene, Oregon, its officers, agents, successors, and assigns, shall

1. Cease and desist from

(a) Discriminatorily maintaining a rule that prohibits its employees from using its electronic communications systems for union purposes.

(b) Maintaining rules that prohibit a display of union insignia.

(c) Issuing written warnings to employees to discourage their activities on behalf of the Union.

(d) Refusing to bargain in good faith with Eugene Newspaper Guild, CWA Local 37194 (Union) as the exclusive collective-bargaining representative of employees in the following appropriate unit:

> All employees described in the collective-bargaining agreement between Respondent and the Union, effective from October 16, 1996 to April 30, 1999.

(e) In any like or related manner interfering with, restraining or coercing employees in the exercise of the rights guaranteed them by Section 7 of the Act.

2. Take the following affirmative action necessary to effectuate the policies of the Act.

(a) Withdraw counterproposal 26 in any future negotiations with the Union over terms of a collective-bargaining agreement.

(b) Rescind the rule prohibiting the display of union insignia.

(c) Within 14 days from the date of this Order, remove from its files any reference to the unlawful warnings to Suzi Prozanski, and within 3 days thereafter notify Prozanski in writing that this has been done and that the warnings will not be used against her in any way.

(d) Within 14 days after service by the Region, post at its facility in Eugene, Oregon, copies of the attached notice marked "Appendix."[13] Copies of the notice, on forms provided by the Regional Director for Region 19, after being signed by the Respondent's authorized representative, shall be posted by the Respondent immediately upon receipt and maintained for 60 consecutive days in conspicuous places including all places where notices to employees are customarily posted. Reasonable steps shall be taken by the Respondent to ensure that the notices are not altered, defaced, or covered by any other material. In the event that, during the pendency of these proceedings, the Respondent has gone out of business or closed the facility involved in these proceedings, the Respondent shall duplicate and mail, at its own expense, a copy of the notice to all current employees and former employees employed by the Respondent at any time since March 7, 2000.

(e) Within 21 days after service by the Region, file with the Regional Director a sworn certification of a responsible official on a form provided by the Region attesting to the steps that the Respondent has taken to comply.

(f) IT IS FURTHER ORDERED that the complaint is dismissed insofar as it alleges violations of the Act not specifically found.

Dated, San Francisco, California February 21, 2002

[11] Respondent's reliance on Board cases that find computer access policy and the use of other communications equipment mandatory subjects of bargaining is inapposite. The issue here is not whether the communications policy was a mandatory subject of bargaining but whether counterproposal 26 was an illegal subject of bargaining.

[12] If no exceptions are filed as provided by Sec. 102.46 of the Board's Rules and Regulations, the findings, conclusions, and recommended Order shall, as provided in Sec. 102.48 of the Rules, be adopted by the Board and all objections to them shall be deemed waived for all purposes.

[13] If this Order is enforced by a Judgment of the United States Court of Appeals, the words in the notice reading "Posted By Order Of The National Labor Relations Board" shall read "Posted Pursuant To A Judgment Of The United States Court Of Appeals Enforcing An Order Of The National Labor Relations Board."

APPENDIX

NOTICE TO EMPLOYEES
POSTED BY ORDER OF THE
NATIONAL LABOR RELATIONS BOARD
An Agency of the United States Government

The National Labor Relations Board has found that we violated Federal labor law and has ordered us to post and obey this notice.

FEDERAL LAW GIVES YOU THE RIGHT TO

Form, join, or assist a union

Choose representatives to bargain with us on your behalf

Act together with other employees for your benefit and protection

Choose not to engage in any of these protected activities.

WE WILL NOT discriminatorily maintain or enforce a rule that prohibits employees from using electronic communications systems for union purposes.

WE WILL NOT maintain rules that prohibit a display of union insignia.

WE WILL NOT issue written warnings to employees to discourage their activities on behalf of the Union.

WE WILL NOT refuse to bargain in good faith with Eugene Newspaper Guild, CWA Local 37194 (Union) as the exclusive collective-bargaining representative of employees in the following appropriate unit:

All employees described in the collective-bargaining agreement between Respondent and the Union, effective from October 16, 1996 to April 30, 1999.

WE WILL NOT in any like or related manner interfere with, restrain, or coerce you in the exercise of the rights guaranteed you by Section 7 of the Act.

WE WILL withdraw counterproposal 26 in any future negotiations with the Union over terms of a collective-bargaining agreement.

WE WILL rescind the rule prohibiting the display of union insignia.

WE WILL within 14 days from the date of this Order, remove from its files any reference to the unlawful wamings to Suzi Prozanski, and within 3 days thereafter notify Prozanski in writing that this has been done and that the warnings will not be used against her in any way.

THE GUARD PUBLISHING COMPANY D/B/A THE REGISTER-GUARD

P Send

DOCKETED ON CM
AUG 2 4 2007
BY 085

FILED
CLERK, U S DISTRICT COURT
AUG 2 4 2007
CENTRAL DISTRICT OF CALIFORNIA
BY DEPUTY

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

COLUMBIA PICTURES, INC., et al.,

Plaintiffs,

vs.

JUSTIN BUNNELL, et al.,

Defendants.

2: 06-cv-01093 FMC-JCx

ORDER DENYING DEFENDANTS' MOTION FOR REVIEW

#254

This matter is before the Court on Defendants' Objections to and Motion for Review of Order Regarding Server Log Data (docket no. 194), filed June 12, 2007. The Court has read and considered the moving, opposition, and reply documents submitted in connection with this motion. The matter was heard on August 20, 2007, at which time the parties were in receipt of the Court's Tentative Order. For the reasons and in the manner set forth below, the Court hereby **DENIES** Defendants' Motion.

//

//

//

//

FACTUAL BACKGROUND AND PROCEDURAL HISTORY

Plaintiffs are motion picture studios that own copyrights or exclusive reproduction and distribution rights to numerous movies and television programs. Defendants operate a website that serves as a search engine that enables users to locate and download dot-torrent files. Using dot-torrent files and an independent computer software program, a "BitTorrent" client, users join a peer-to-peer network that facilitates the copying and distribution of the files that were the subject of the users' search. Defendants' website thereby allegedly permits Internet users to locate and download, view, store, and distribute unauthorized copies of Plaintiffs' copyrighted motion pictures and television shows. In this way, Plaintiffs allege Defendants knowingly enable, encourage, induce, and profit from the online piracy of Plaintiffs' copyrighted works.

On February 23, 2006, Plaintiffs filed a Complaint asserting a claim for copyright infringement. Numerous discovery disputes have arisen between the parties, and Defendants have repeatedly moved this Court to review and reconsider the rulings of Magistrate Judge Chooljian. On June 12, 2007, Defendants filed their latest challenge, against the Magistrate Judge's May 29, 2007, Order (1) Granting in Part and Denying in Part Plaintiffs' Motion to Require Defendants to Preserve and Produce Server Log Data and for Evidentiary Sanctions and (2) Denying Defendants' Request for Attorneys' Fees and Costs (the May 29 Order), on June 12, 2007.

STANDARD OF LAW

A district court will not modify or set aside a magistrate judge's order unless it is "found to be clearly erroneous or contrary to law." Fed. R. Civ. P. 72(a).[1] The clearly erroneous standard applies to the magistrate judge's factual

[1] In addition, the Local Rules require that a party objecting to a Magistrate Judge's ruling on a nondispositive matter must "designat[e] the specific portions of the ruling objected to and stat[e] the grounds for the objection." Local Rule 72-2.1.

findings while the contrary to law standard applies to the magistrate judge's legal conclusions, which are reviewed de novo. *See Wolpin v. Philip Morris, Inc.*, 189 F.R.D. 418, 422 (C.D. Cal. 1999); *see also Center for Biological Diversity v. Federal Highway Admin.*, 290 F. Supp. 2d 1175, 1199-1200 (S.D. Cal. 2003) (quoting *Weeks v. Samsung Heavy Indus. Co., Ltd.*, 126 F.3d 926, 943 (7th Cir. 1997), for the proposition that "discretionary orders and will be overturned 'only if the district court is left with the definite and firm conviction that a mistake has been made'").

When reviewing discovery disputes, however, "the Magistrate is afforded broad discretion, which will be overruled only if abused." *Wright v. FBI*, 385 F. Supp. 2d 1038, 1041 (C.D. Cal. 2005); *Geophysical Sys. Corp. v. Raytheon Co., Inc.*, 117 F.R.D. 646, 647 (C.D. Cal. 1987) (Tashima, J.) (questions of relevance in discovery context are reviewed under "the clearly implicit standard of abuse of discretion.").

DISCUSSION

I. The Scope of Federal Rule of Civil Procedure 34

At the heart of Defendants' Motion for Review is the following question of first impression: is the information held in a computer's random access memory (RAM) "electronically stored information" under Federal Rule of Civil Procedure 34?

Defendants and *amici* seek to engraft on the definition of "stored" an additional requirement, that the information be not just stored, but stored "for later retrieval." They argue that "electronically stored information" cannot

include information held in RAM because the period of storage, which may be as much as six hours, is too temporary. The Court finds this interpretation of "stored" unsupported by the text of the Rule, the accompanying commentary of its drafters, or Ninth Circuit precedent involving RAM. The Court holds that data stored in RAM, however temporarily, is electronically stored information subject to discovery under the circumstances of the instant case.

First, even the definition *amici* supplied fails to support their argument that information written to and held in random access memory is not "stored." As *amici* explain, according to the Merriam-Webster Collegiate Dictionary, to store means "to lay away, to accumulate or to place or leave in a location (as a warehouse, library, or *computer memory*) for preservation *or later use or disposal*." *Merriam-Webster's Collegiate Dictionary* (Frederick C. Mish et al. eds., 10th ed. 1993) (emphasis added). It is undisputed that RAM is computer memory and that information held in RAM is held there for later use by the computer (e.g., to be used in tasks performed by software or written to a hard drive, flash drive, DVD, or other more permanent medium) or disposal (e.g., to be erased when the computer is turned off or when the data is overwritten with new information as part of the regular computing process).

The definition of "to store" from the Random House Dictionary of the English Language specific to the context of computers further undermines Defendants' argument that RAM does not store data: "13. *Computers.* to put *or* retain (data) in a memory unit." Random House dictionary of the English Language (Stuart B. Flexner et al. eds., 2d ed. 1987) (emphasis added). Under this definition, the information need not even be subsequently accessed or used; simply placing the data in the RAM module is sufficient for it to constitute electronically stored information.

In addition, RAM itself is *defined* as a storage unit, and, due to its speed relative to hard disk drives, is typically used as the computer's primary storage:

"Random Access Memory (RAM): A read/write, nonsequential-access memory used for the *storage* of instructions and data. Note 1: RAM access time is essentially the same for all storage locations. Note 2: RAM is characterized by a shorter access time than disk or tape storage." National Communications System, *Federal Standard 1037C: Telecommunications: Glossary of Telecommunication Terms* (Gen. Servs. Admin., 4th ed. 1996) (emphasis added). Accordingly, information held in RAM is "stored" under the plain meaning of the unambiguous language of Rule 34.

Second, the Notes of the Advisory Committee to the 2006 Amendments to Rule 34, which amended the Rule to make explicit that it authorized discovery of information stored electronically,[2] indicate that the definition was intended to be read expansively to include all current and future electronic storage mediums:

> The wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition of electronically stored information. Rule 34(a)(1) is *expansive* and includes *any type of information that is stored electronically*. A common example often sought in discovery is electronic communications, such as e-mail. The rule covers--either as documents or as electronically stored information--information "stored in any medium," to encompass future developments in computer technology. Rule 34(a)(1) is intended to be *broad enough to cover all current types of computer-based information*, and flexible enough to encompass future changes and developments.

Fed. R. Civ. P. 34(a)(1) (2006 amendments) advisory committee's note. Such

---

[2] Rule 34(a) states, in part, that "[a]ny party may serve on any other party a request . . . to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample *any* designated documents or *electronically stored information*--including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored *in any medium from which information can be obtained*--translated, if necessary, by the respondent into reasonably usable form, or to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served." Fed. R. Civ. P. 34(a) (emphasis added).

clear evidence that Rule 34(a)'s scope was intended to be as broad as possible, and cover data stored "in any medium from which information can be obtained," leaves no room to interpret the Rule to categorically exclude information written in a particular medium simply because that medium stores information only temporarily. Information in the RAM of Defendants' computers "can be obtained" by Defendant. It is undisputed that the Server Log Data[3] Plaintiffs seek can be copied from RAM in Defendants' computers and produced to Plaintiffs. Rule 34 requires no greater degree of permanency from a medium than that which makes obtaining the data possible. As information can be obtained from RAM, it is within the scope of Rule 34 and subject to discovery under the appropriate circumstances.

Finally, as discussed in the Magistrate Judge's May 29 Order, *amici* and Defendants' argument that data in RAM is too ephemeral to satisfy Rule 34's storage requirement is foreclosed by the Ninth Circuit's decision in *Mai Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993). To determine if the plaintiff could prevail on a claim of copyright infringement, the court in *Mai Systems Corp.* confronted the question of whether a program in RAM was "fixed in a tangible medium of expression," which the applicable statute defined as "sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." *Id.* at 517-518; 17 U.S.C. § 101. Despite the Copyright Act's explicit requirement that the medium store information with a degree of permanence and for "more than transitory duration," the court held that a computer's copying of software into

[3] Server Log Data, as defined in the May 29 Order, includes (1) the anonymous (masked or encrypted) Internet Protocol (IP) address of users of Defendants' website who request dot-torrent files, (2) the identity of the dot-torrent files requested, and (3) the dates and times of such requests. (May 29 Order, 3:16-4:1.)

RAM was sufficient to meet the statutory prerequisites for liability and affirmed the district court's grant of summary judgment and issuance of a permanent injunction. *Id.* at 519.

In light of the Ninth Circuit's holding that RAM is a tangible medium, sufficiently permanent to permit reproduction, *amici* and Defendants' argument that RAM holds data for such a short duration that it is not stored subject to later access and retrieval simply has no merit. Defendants have therefore failed to establish that the Magistrate Judge's legal conclusion that data held in the RAM of computers under Defendants' control is within the scope of discoverable information under Federal Rule of Civil Procedure 34 was contrary to law.

In response to *amici*'s concerns over the potentially devastating impact of this decision on the record-keeping obligations of businesses and individuals, the Court notes that this decision does not impose an additional burden on any website operator or party outside of this case. It simply requires that the defendants in this case, as part of this litigation, *after* the issuance of a court order, and following a careful evaluation of the burden to these defendants of preserving and producing the specific information requested in light of its relevance and the lack of other available means to obtain it, begin preserving and subsequently produce a particular subset of the data in RAM under Defendants' control.

II. The Magistrate Judge's Authority to Order the Requested Discovery

In an attempt to resist complying with the Magistrate Judge's May 29 Order, Defendants have raised a number of creative legal challenges, the first of which is that the Magistrate Judge exceeded her authority by issuing an injunction and disposing of ultimate issues in the case. The Federal Magistrates Act provides that a magistrate judge may "hear and determine any pretrial matter pending before the court, except a motion for injunctive relief," and seven other enumerated motions. 28 U.S.C. § 636(b)(1)(A). The Ninth Circuit has held that

the list of excluded motions is not exhaustive, and courts must "look to the effect of the motion, in order to determine whether it is properly characterized as dispositive or non-dispositive of a claim or defense of a party." *United States v. Rivera-Guerrero*, 377 F.3d 1064, 1068 (9th Cir. 2004). If it is a final order, dispositive of a claim or defense, it is outside of the magistrate's statutorily granted jurisdiction. *Id.* at 1069.

Plaintiffs' Motion to Require Defendants to Preserve and Produce Server Log Data and for Evidentiary Sanctions was neither a motion for injunctive relief nor its functional equivalent, and the May 29 Order granting the motion did not dispose of any of Defendants' claims or defenses. The May 29 Order is a quotidian discovery order, resolving disputes over relevance, burden, and the proper scope of discovery, that is well within the Magistrate Judge's authority and substantial specialized expertise. Magistrate judges regularly compel production of documents and, although courts in other jurisdictions have interpreted orders to preserve evidence as injunctions, the Ninth Circuit has held that all parties are under a duty not to intentionally dispose of evidence they know is relevant. *Idaho Potato Comm'n v. G&T Terminal Packaging, Inc.*, 425 F.3d 708, 720 (9th Cir. 2005); *Pueblo of Laguna v. United States*, 60 Fed. Cl. 133, 138 (2004) (holding that "a document preservation order is no more an injunction than an order requiring a party to identify witnesses or to produce documents in discovery.") (citing *Mercer v. Magnant*, 40 F.3d 893, 896 (7th Cir. 1994); *cf. Madden v. Wyeth*, No. 3-03-CV-0167-R, 2003 U.S. Dist. LEXIS 6427, at *1 (N.D. Tex. Apr. 16, 2003) ("A motion to preserve evidence is an injunctive remedy and should issue only upon an adequate showing that equitable relief is warranted.").

Moreover, contrary to Defendants' contentions, the May 29 Order does not dispose of any of Defendants' potential First Amendment or other defenses to Plaintiffs' claim for copyright infringement. The May 29 Order addresses only

Defendants' arguments in opposition to the requested discovery, not whether the First Amendment or the Electronic Communications Privacy Act (ECPA) might factor into a final, permanent injunction prohibiting Defendants from engaging in any form of copyright infringement. That the creation of a server log might be a predicate step in fashioning effective hypothetical final relief does not alter the fact that such final disposition of any of the parties' claims or defenses remains a future event. As the May 29 Order is not dispositive of any claims or defenses, it was within the Magistrate Judge's jurisdiction, and the Court overrules Defendants' objection.

III. The Fifth Amendment

Defendants argue that the Magistrate Judge violated their Fifth Amendment due process rights by (1) finding that they voluntarily consented to the disclosure of the Server Log Data and (2) ruling against Defendants based on their failure to demonstrate that there are alternative means of acquiring the requested information after denying Defendants' discovery requests that would have led to the production of data Defendants could use to demonstrate such means. Defendants have not provided any authority for the proposition that a magistrate's order could violate a defendants' Fifth Amendment rights or that a motion for review would be the proper venue for obtaining relief for such a hypothetical constitutional injury. Nevertheless, the Court will briefly address Defendants' arguments, construing them as arguments that the Magistrate Judge's factual findings were clearly erroneous and that her legal conclusions were contrary to law, the applicable legal standard.

Defendants contend that production of their Server Log Data would violate the Stored Communications Act (SCA), the Wiretap Act, and the Pen Register Statute. The SCA prohibits unlawful access to stored communications, which is defined as either "(1) intentionally access[ing] without authorization a facility through which an electronic communication service is provided; or (2)

intentionally exceed[ing] an authorization to access that facility; and thereby obtain[ing] . . . authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ." The May 29 Order, however, contemplates no *unauthorized* access. Defendants are not ordered to access the facility of a third party and obtain stored communications, such as e-mails stored on a remote server. Defendants are also not custodians of private communications, as an Internet Service Provider would be of e-mails sent through its servers (where neither the sender nor the recipient would be parties to the litigation), ordered to disclose the contents of those communications. *Cf. Theofel v. Farey-Jones*, 341 F.3d 978, 985 (9th Cir. 2003). Rather, Defendants are the intended recipients of the information contained in the Server Log Data. When users access Defendants' website and request information (such as dot-torrent files), they voluntarily supply their IP addresses and a packet of information containing their request. That information is received and processed in Defendants' RAM on their servers, for their use (which, in addition to the contemporaneous fulfillment of the request, the record reveals has thus far consisted primarily of disclosure to advertisers to generate revenue). (May 29 Order 22:1-3; Reporter's Transcript of the April 3, 2007, Discovery Hearing (RT) 90-97).) Defendants' access to Defendants' information on servers under Defendants' control does not constitute unauthorized access to a "facility through which an electronic communication service is provided" or "to a wire or electronic communication while it is in electronic storage in such system." Production of the Server Log Data would therefore not violate the SCA.

The Wiretap Act makes it an offense to "intentionally intercept[] . . . any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). The Wiretap Act and the SCA are both part of the ECPA, and play complementary roles in Congress's regulatory scheme. Under the ECPA, an electronic communication may either be intercepted and actionable under the Wiretap Act or acquired while

in electronic storage and actionable under the SCA, but not both. *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 877 (9th Cir.2002). As such, an electronic communication may not simultaneously be actionable under both the Wiretap Act and the SCA. *Id.* The Ninth Circuit has held that the Wiretap Act applies only to "acquisition contemporaneous with transmission," and that "Congress did not intend for 'intercept' to apply to electronic communications when those communications are in 'electronic storage.'" *Theofel,* 359 F.3d at 1077-78, quoting *Konop.* 302 F.3d at 877. Communications are in "electronic storage" under the SCA, and outside the scope of the Wiretap Act, even where the storage is transitory and lasts for only a few seconds. *Quon v. Arch Wireless Operating Co.*, 445 F. Supp. 2d 1116, 1135-36 (C.D. Cal. 2006) (citing *Konop*, 302 F.3d at 878 n.6). As discussed above, the Server Log Data exists in electronic storage. The Wiretap Act is therefore inapplicable and does not pose any barrier to Defendants' compliance with the May 29 Order.

The Pen Register Statute is similarly inapplicable to the ordered discovery, as Defendants' own Motion makes clear. After discussing why the exemption the to the Pen Register Statute's prohibitions on use of pen registers and tap and trace devices that the Magistrate Judge relied upon does not apply in these circumstances, Defendants argued that the Court could not authorize production of the Server Log Data under the Pen Register Statute because the Server Log Data contains "contents" of communications, such as the identity of the dot-torrent files requested. As Defendants note, pen registers and trap and trace devices, by definition, do not record "the contents of any communication." 18 U.S.C. § 3127(3)–(4); *see also In re United States for an Order Authorizing the Use of a Pen Register & Trap*, 396 F. Supp. 2d 45, 50 (D. Mass. 2005) (interpreting "contents of communications" to include "application commands, search queries, requested file names, and file paths"). Because the May 29 Order requires the production of the contents of communications, Defendants have not

been ordered to install a pen register or trap and trace device, and the Pen Register Statute does not bar the ordered discovery. Accordingly, the Magistrate Judge's decision that production of the Server Log Data would not violate the SCA, the Wiretap Act, or the Pen Register Statute was not contrary to law.[4]

Defendants argue that the Magistrate Judge improperly based a number of key rulings on their failure to "prove facts where they could not obtain the needed evidence" because of the Magistrate Judge's prior rulings, and the orders of this Court, which concluded that the discovery Defendants were requesting would not lead to relevant or admissible evidence.

For example, Defendants note that the Magistrate Judge concluded that "preservation and production of the Server Log Data is appropriate in light of the conclusory and speculative nature of the evidence presented regarding the loss of good will and business, the key relevance and unique nature of the Server Log Data in this action, the lack of a reasonable alternative means to obtain such data, and the limitation imposed by the court regarding the masking of IP addresses." Defendants argue they were not able to present evidence of "alternative means to obtain such data" because "the evidence needed for such proof has been concealed by Plaintiffs in an institutional citadel of privilege." (Mot. 41:1-2.)

First, contrary to Defendants' arguments that "the Magistrate Judge's Order implicitly casts the burden of proof onto Defendants," in each instance Defendants cite, the decision is based on the Magistrate Judge's factual findings after a review of the full record that there were no "reasonable alternative means to obtain such data," not on Defendants' "failure to prove" the availability of any alternative means. Second, with respect to two of three challenged findings (the Magistrate Judge's determination that the requested production would not be

[4] As the Court's holding rests on independent legal grounds, it is unnecessary to review the Magistrate Judge's determination that Defendants' website constitutes an "electronic communications service."

unduly burdensome and that international law did not prohibit the requested discovery), the burden *was* properly on Defendants to demonstrate why they should be relieved from producing relevant information.

Finally, as discussed in this Court's prior orders, the information that was the subject of Defendants' denied discovery requests was irrelevant. Even if Defendants were able to show, as they allege, that Plaintiffs operate "honeypots" and participate in BitTorrent "swarms," thereby acquiring the IP addresses of individual copyright infringers, such evidence would not help them to demonstrate that "reasonable alternative means to obtain" the Server Log Data were available. Although Plaintiffs may have other means of discovering the IP addresses of individual direct infringers, in order to prevail in this action, Plaintiffs will need to establish that *Defendants* were in some way responsible for the direct infringement of others. The Server Log Data will show that individuals access Defendants' website and request and download dot-torrent files, which can be used to obtain Plaintiffs' copyrighted works without permission. This link in the causal chain is essential to proving Defendants' responsibility for copyright infringement under theories of contributory infringement, vicarious infringement, and inducement. Accordingly, the Magistrate Judge's finding of a "lack of a reasonable alternative means to obtain" the Server Log Data was not clearly erroneous or contrary to law.

IV. The First Amendment

Defendants argue that the Magistrate Judge's rejection of Defendants' First Amendment objections to the requested discovery was contrary to law because Plaintiffs failed to demonstrate a need for the Server Log Data and because the Magistrate Judge failed to perform a proper balancing test. The Court has already discussed why the Magistrate Judge's finding that Plaintiffs had a need for the Server Log Data was not clearly erroneous or contrary to law. The Court also agrees with the Magistrate Judge that "the preservation and disclosure of the

Server Log Data does not encroach or substantially encroach" upon the limited First Amendment protection to which the users of Defendants' website are entitled, "particularly in light of the fact that such data does not identify the users of Defendants' website and that the IP addresses of such users have been ordered to be masked." (May 29 Order 23:3-7.)

Defendants argue that, under *Adolph Coors Co. v. Wallace*, 570 F. Supp. 202, 208 (N.D. Cal. 1983), the Magistrate Judge was required to employ a formal three-part balancing test in determining whether to order the requested discovery. *Adolph Coors Co.*, in addition to not constituting binding precedent, proposed only that "any tribunal confronted with facts and arguments similar to those presented here undertake a sensitive evaluation in three steps." *Id.* In *Adolph Coors Co.*, the defendant Solidarity was a political organization comprised exclusively of gay men and lesbian women who sought to exert pressure on the plaintiff brewing company through a boycott in an effort to modify the plaintiff's political positions. *Id.* at 204. The plaintiff requested a list of the names of Solidarity's members and its sources of financial support. *Id.* Solidarity argued that revealing the group's members and donors would chill its associational privacy and freedom of political expression. *Id.*

In the instant case, Plaintiffs have sought data that would demonstrate that anonymous individuals accessed Defendants' website and requested dot-torrent files. Plaintiffs are not requesting the names or other identifying information, as the plaintiff sought in *Adolph Coors Co.*, and the May 29 Order ensures that such identifying information will not be disclosed. In addition, in contrast to the strong First Amendment protections for the freedom of association and right to engage in political speech, the privacy interests of Defendants' users are, at best, limited. To the extent the users are engaged in copyright infringement, the First Amendment affords them no protection whatsoever. *Harper & Row, Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 559, 105 S. Ct. 2218; 85 L. Ed. 2d 588

(1985) ("The essential thrust of the First Amendment is to prohibit improper restraints on the *voluntary* public expression of ideas; it shields the man who wants to speak or publish when others wish him to be quiet. There is necessarily, and within suitably defined areas, a concomitant freedom *not* to speak publicly, one which serves the same ultimate end as freedom of speech in its affirmative aspect.") (emphasis in original) (internal quotations omitted)); *A&M Records v. Napster, Inc.*, 239 F.3d 1004, 1028 (9th Cir. 2001) (holding that the First Amendment does not protect use of a peer-to-peer file sharing network that constitutes copyright infringement). Even if the users are engaged in *legal* file sharing, they have little to no expectation of privacy because they are broadcasting their identifying information to everyone in the BitTorrent "swarm" as they download the file. *See, e.g., In re Verizon Internet Servs.*, 257 F. Supp. 2d 244, 267 (D.D.C. 2003) (finding that "if an individual subscriber opens his computer to permit others, through peer-to-peer file-sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world."). Similarly, because users openly disclose their IP addresses as part of the BitTorrent file transfer process, the Court is not persuaded by Defendants' argument that the retention of the IP addresses of users who obtain dot-torrent files from Defendants' website will "chill" their speech. Accordingly, the Court is satisfied that the Magistrate Judge properly weighed Defendants' First Amendment concerns against the need for the requested discovery, and that her resolution of the matter was not contrary to law.

V. Impact of International Law

Defendants insist that the Magistrate Judge erred in rejecting their argument that the law of the Netherlands, where Defendants have placed their servers, prohibits the courts of the United States from ordering the requested discovery in this action. First, the Magistrate Judge properly found that

Defendants had failed to meet their burden in establishing that Netherlands law would prohibit retention of the Server Log Data or production of an encrypted, anonymous version of that data to Plaintiffs. *See United States v. Vetco, Inc.*, 691 F.2d 1281, 1289 (9th Cir. 1981) ("The party relying on foreign law has the burden of showing that such law bars production."). Defendants argue the Magistrate Judge erred, citing a recent opinion of the Amsterdam District Court that held as follows:

> A service provider may, in certain circumstances, be obliged to provide rights holders (or their representatives) with the information asked for. For this, the Court must first of all be satisfied that there have been (unlawful) infringement activities by the subscribers concerned and, secondly, that it is beyond reasonable doubt that those whose identifying information is made available are also actually those who have been guilty of the relevant activities.

BREIN Foundation v. UPC Nederland B.V., Fabrizio Decl. Ex. 28. As the quoted text makes evident, however, *BREIN Foundation* does not support Defendants' argument. It places restrictions only on the production of "identifying information." As the Server Log Data Defendants must produce is anonymous, *BREIN Foundation*, even if it were the applicable legal standard, would not prohibit its production.

Second, as the Supreme Court has stated, "[i]t is well settled that [foreign] statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute." *Societe Nationale Industrielle Aerospatiale v. United States Dist. Court for S. Dist.*, 482 U.S. 522, 544 n.29, 107 S. Ct. 2542, 96 L. Ed 2d 461 (1987); *see also Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468, 1474 (9th Cir. 1992); *United States v. Vetco, Inc.*, 691 F.2d 1281, 1287 (9th Cir. 1981); May 29 Order 29:14-17. Assuming, *arguendo*, that Netherlands law would prohibit the discovery ordered, the Magistrate Judge analyzed the issue under the applicable legal standard, considered the relevant, non-exhaustive list of factors enumerated in *Richmark Corp.*, and determined that the factors

weighed in favor of permitting the ordered discovery. Although Defendants disagree with the Magistrate Judge's ultimate decision, they have failed to establish that her factual findings were clearly erroneous or that her legal conclusions were contrary to law.

VI. Defendants' Control of the Routing of Server Log Data

Defendants' final objection is a cryptic argument that the Magistrate Judge's factual finding that "Defendants have the ability to manipulate at will how the Server Log Data is routed" is clearly erroneous because it was based on insufficient evidence. In support of this contention, Defendants state that "Panther," the third-party service Defendants recently began using that prevents requests being received in the RAM of Defendants' servers, "never logged." However, as Defendants' representative testified during the Magistrate Judge's evidentiary hearing, Defendants "could disengage and resume the functions currently performed by Panther if directed to log the Server Log Data in issue." (May 29 Order 10:27-28 (citing RT 72, 103-04).)

The Magistrate Judge's factual findings were based on a full day of testimony, including testimony by expert witnesses called by both parties, as well as hundreds of pages of briefing, technical declarations, and even multiple rounds of supplemental briefing. Her finding that the "data in issue which is currently routed to a third party entity under contract to defendants and received in said entity's RAM . . . is within defendants' possession, custody or control by virtue of defendants' ability to manipulate at will how the data in issue is routed" was founded on her "consideration of the extensive arguments and evidence presented" and "the court's assessment of the credibility of the declarants and witnesses." (May 29 Order 1:25-2:8.) Moreover, the Magistrate Judge's decision with respect to Defendants' ability to route the Server Log Data to themselves or through Panther at will was also based on "the change in the method of operation" from routing the data to Defendants' servers to employing Panther

"and the timing thereof," as Defendants engaged Panthers' services just one month prior to the Magistrate Judge's evidentiary hearing. (*Id.* at 8:24-10:28.) As the record reflects that Defendants have the ability to reroute the Server Log Data through their own servers, should it prove impracticable for Defendants to acquire the information from Panther, the Court finds that the Magistrate Judge's finding that Defendants' control the routing of the Server Log Data was not clearly erroneous.

CONCLUSION

For the foregoing reasons, the Court hereby **DENIES** Defendants' Motion for Review (docket no. 194).

IT IS SO ORDERED.

Dated: August 24, 2007

FLORENCE-MARIE COOPER, JUDGE
UNITED STATES DISTRICT COURT

Today We Talk About . . .

- The factual background of *Quon v. Arch Wireless.*
- The Ninth Circuit's *Quon* decision of June 18, 2008.
- Implications of *Quon* under the Stored Communications Act.
- Implications of *Quon* under constitutional law (California and federal).
- Post-*Quon* pointers for employers.

Factual Background: Bikers, Texting and Internal "Affairs" at the Ontario PD

Quon begins with a lawsuit by Ontario, California PD employees Jeff Quon, Jerilyn Quon, April Florio, Doreen Klein, and Steve Trujillo against:

- The City of Ontario
- The Ontario Police Department
- Lloyd Scharf, Ontario Police Chief
- Debbie Glenn, Sergeant, Ontario PD
- Arch Wireless, text messaging vendor to the City of Ontario

Bikers, Texting and Internal "Affairs" (cont.)

1. Ontario PD officers issued alphanumeric pagers pursuant to Arch Wireless contract.
2. The Hell's Angels scandal.
3. Excessive pager use by certain employees.

Bikers, Texting and Internal "Affairs" (cont.)

- All Ontario PD employees had read and signed a strong "Computer Usage, Internet and E-mail Policy" that waived any expectation of privacy.
- As to pagers, there was evidence of a lieutenant's "unwritten policy" of not auditing usage so long as employees paid their overage charges.

Bikers, Texting and Internal "Affairs" (cont.)

- Stored messages could only be obtained from Arch Wireless.
- Department asked Arch Wireless to furnish transcripts of text messages. Arch Wireless complied.
- Messages of Quon, who was having an extra-marital affair with Florio, a Department dispatcher, "were, to say the least, sexually explicit in nature."

Quon in the Trial Court

Plaintiffs brought claims under, among other theories: the (federal) Stored Communications Act; the Fourth Amendment; the California constitution; and a California anti-eavesdropping statute.

The trial court disposed of principal claims as follows:

Quon in the Trial Court (cont.)

- As to the Stored Communications Act (18 USC 2701 *et seq.*):
  - Court finds that governmental defendants are not service providers.
  - Court finds that Arch Wireless is a remote computing service, which can divulge contents of stored communications with the consent of a "subscriber."

Quon in the Trial Court continued

- As to California Penal Code sec. 629.86:
  - Prohibits the interception, disclosure and use of wire, electronic pager or electronic cellular telephone communications.
  - Court finds that sec. 629.86 does not apply to communications acquired from electronic storage.

Quon in the Trial Court (cont.)

- As to the Fourth Amendment:
  - Quon had a reasonable expectation of privacy because of lieutenant's decision not to enforce the Department's written policy in the case of pager text messages.
  - However, trial court found that search was reasonable (no less restrictive method of assessing efficacy of 25,000-character limit).

Quon in the Ninth Circuit

- Ninth Circuit reversed the trial court's principal findings on Stored Communications Act and Fourth Amendment.
- As to the Stored Communications Act:
  - Ninth Circuit found that Arch Wireless provided an electronic communication service (ECS) to the public, rather than a remote computing service (RCS).
  - As an ECS, Arch Wireless could divulge the contents of a stored communication with the lawful consent of an originator, addressee or intended recipient of the communication, but not with the consent of a mere "subscriber" (e.g., the City of Ontario).

Quon in the Ninth Circuit (cont.)

- An electronic communication service is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 USC sec. 2510(15).
- A remote computing service is "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 USC sec. 2711(2).

Implications of *Quon*

- For employers: employees' messages stored by a vendor may not be accessible to employers without employees' consent.
- Previous decisions permit employers to read employees' stored communications for any purpose. *See Bohach v. City of Reno*, 932 F.Supp.1232, 1234-35 (D. Nev. 1996).
- Stored Communications Act restrictions do not apply when stored communications are accessed "by the person or entity providing a wire or electronic communication service." 18 USC 2701(c)(1).

Quon in the Ninth Circuit (cont.)

- Fourth Amendment:
  - Lieutenant's unwritten policy of *not reviewing the contents of employees' messages so long as overages were paid superseded, for "reasonable expectation of privacy" purposes, the written policy that Department personnel had read and signed.*
  - Search and seizure was not reasonable under the circumstances.

Implications of *Quon* (cont.)

- Where the employer is not the service provider, access to stored messages maintained by the vendor ordinarily requires the consent of the employee or another party (originator, addressee or recipient) to the communication.

Implications of *Quon* (cont.)

- After *Quon*, employers should consider noting in their personnel manuals or technology-use policies that the employer may request a consent from the employee to obtain stored messages from third-party vendors."
- *Quon* also argues for providing communication services "in house" where feasible.

Implications of *Quon* (cont.)

- Even for private employers, the Ninth Circuit's finding that the City's surveillance policy was effectively waived for "reasonable expectation" purposes is important.
- After *Quon,* employers' written policies should clearly state that the employers' right to monitor employee communications cannot be waived or varied by the oral representations of any supervisor or other employee.

Implications of *Quon* (cont.)

- For employers that also are governmental agencies: Fourth Amendment constraints apply.
- Employees' reasonable expectation of privacy can be revived by supervisors' apparent waivers of, or failures to enforce, the policy.
- Search and seizure of employees' communications will be upheld where there is a close fit between the search's purpose and its extent.

Implications of *Quon* (cont.)

- For electronic communication services:
  - *Quon* reminds us that such entities have unique obligations to users – not just customers – under the Electronic Communications Privacy Act, Stored Communications Act and other statutes.
  - Consent from the entity that pays for your service might not be enough.

Court Limits Right of Employers to Obtain Stored Text Messages from Vendors' Servers

By Charles Kennedy

In a decision entered on June 18, 2008, the United States Court of Appeals for the Ninth Circuit made important findings concerning the right of employers to obtain and read employees' text messages sent over employer-provided services. This Legal Update discusses the decision in detail and recommends that employers review their workplace surveillance practices to ensure their continuing compliance with state and federal law.

THE NINTH CIRCUIT'S DECISION

The decision in *Quon et al. v. Arch Wireless et al.* has its origins in an internal affairs investigation into text messages sent by members of the City of Ontario, California, Police Department.[1] Sergeant Jeff Quon had sent a number of messages to other persons, including Sergeant Steve Trujillo, Dispatcher April Florio, and Quon's wife, Jerilyn Quon, using an alphanumeric pager issued by the Department. The volume of messages sent from Quon's pager exceeded the service provider's limit of 25,000 characters per pager per month, causing the city to incur overage charges. The City of Ontario billed those charges to Quon and other individual employees who had exceeded the character limit.

In response to a complaint from the police lieutenant in charge of collecting overages, the Ontario police chief ordered an audit of Department members' pager usage to determine if the overages were incurred for official business. The contents of employees' text messages were stored on the server of the City's vendor, Arch Wireless. Pursuant to an email request from the City, Arch Wireless turned over transcripts of the text messages sent by certain employees, including Sergeant Quon, to the City. The internal affairs review of the transcripts disclosed that many of the messages were non-work-related, including messages that were "personal in nature and were often sexually explicit."[2]

Sergeant Quon, his wife, and two Department members with whom Quon exchanged messages brought a complaint against the City, Arch Wireless, the Chief of Police, the Department, and Sergeant Debbie Glenn, a member of Internal Affairs who had been involved in the investigation. Among other claims, the complaint alleged that the City and the Department had violated the plaintiffs' rights under the United States and California Constitutions when they obtained and read the stored text messages, and that Arch Wireless had violated the Stored Communications Act when it voluntarily surrendered the contents of the plaintiffs' text messages to the City.

The trial court (the United States District Court for the Central District of California) held that Arch Wireless did not violate the Stored Communications Act and that the governmental defendants did not violate the Fourth Amendment to the United States Constitution, which prohibits unreasonable searches and seizures.[3] The plaintiffs appealed those decisions to the Ninth Circuit.

The Ninth Circuit's Reading of the Stored Communications Act

The Stored Communications Act ("SCA") defines the circumstances under which persons may gain access to emails and other electronic communications that are stored on a service provider's facilities.[4] The SCA also governs a service provider's disclosure of those communications to others.[5]

In motions filed with the trial court, the plaintiffs had argued that as an electronic communication service provider to the public, Arch Wireless was prohibited by the SCA from "knowingly divulg[ing] to any person the contents of a communication while in electronic storage by that service."[6] The trial court disagreed, finding that Arch Wireless was a not an electronic communication service provider but a "remote computing service," which is permitted by the SCA to disclose the contents of stored communications on its server to its subscriber (in this case, the City of Ontario).[7]

The Ninth Circuit reversed the lower court on this point, finding that Arch Wireless's text-messaging pager service was not a remote computing service, which is defined in the SCA as "the provision to the public of computer storage or processing services,"[8] but an electronic communication service, which is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[9] The Ninth Circuit based its conclusion on the statutory definitions, the SCA's legislative history, and the court's own 2004 decision in *Theofel v. Farey-Jones*, which characterized an email service provider's storage of messages after delivery as archival storage for backup protection by an electronic communication service provider.[10]

The Stored Communications Act ("SCA") defines the circumstances under which persons may gain access to emails and other electronic communications that are stored on a service provider's facilities.

As a provider of electronic communication services, Arch Wireless was not permitted to release the contents of messages stored on its service to a mere "subscriber," such as the City of Ontario, but could divulge those messages only to "an addressee or intended recipient" of those messages.[11] Accordingly, the

Ninth Circuit found as a matter of law that Arch Wireless's unauthorized disclosure of the contents of plaintiffs' text messages to the City was unlawful under the SCA.

The Constitutional Claims

The plaintiffs had also argued in the district court that the City, the Police Department and the Chief of Police had violated their rights under the Fourth Amendment to the U.S. Constitution, and that all of the defendants, including Sergeant Glenn, had violated their right to privacy under the California Constitution.

These claims, which were based upon the defendants' constitutional obligations as governmental bodies and agents, would not be available against private employers and will be discussed only briefly here.

The Fourth Amendment claim (and the California constitutional claim as well, to the extent that it was based upon a theory of unreasonable search and seizure) could succeed only if the plaintiffs had a reasonable expectation of privacy in the contents of their text messages and if the search or seizure was unreasonable.

The *Quon* case contains lessons for employers and communications service providers alike.

On the first question, the district court had found that the plaintiffs *did* have a reasonable expectation of privacy in the contents of the text messages, notwithstanding a formal Department policy that disclaimed any such expectation, because of a superior officer's stated informal policy (apparently relied upon by Sergeant Quon) of not auditing pager usage so long as overages were paid. The Ninth Circuit agreed with this finding.[12]

However, the Ninth Circuit rejected the lower court's finding, pursuant to a jury verdict, that the seizure of plaintiffs' messages was reasonable. Although the Ninth Circuit accepted the jury's conclusion that the search was intended to "determine the efficacy of the 25,000 character limit," the court also found that the Department could have achieved that purpose by less intrusive means, rendering the seizure and reading of the text messages unreasonable. Accordingly, the Ninth Circuit found that the search violated the plaintiffs' Fourth Amendment rights and the plaintiffs' privacy rights under the California Constitution.[13]

IMPLICATIONS OF THE NINTH CIRCUIT'S DECISION

The *Quon* case contains lessons for employers and communications service providers alike.

For employers, *Quon* is a reminder of the importance of obtaining comprehensive, effective consent from their employees to monitor their communications over employer-provided facilities, and of avoiding statements and actions that might be construed as a weakening or outright waiver of those surveillance rights.

Notably, the record in *Quon* showed that Department employees were, in fact, subject to a "Computer Usage, Internet and E-mail Policy" stating that "[u]sers should have no expectation of privacy or confidentiality when using [Department-provided] resources."[14] Sergeant Quon had signed this written policy, and the

SAMPLE
NOTICE AND CONSENT TO
TELEPHONE MONITORING AND RECORDING

[Company name] is committed to providing quality service to its customers. It is also committed to providing a safe and respectful work place. Consistent with the [Company] Code of Business Practices and Ethics and its Vision and Values, [Company] respects an environment that encourages participation and emphasizes the importance of communicating clearly and partnering for the customers' benefit.

To ensure that we achieve and maintain the above commitments, Call Center staff will establish objective standards and measurements of the quality of call handling. In order to evaluate whether these criteria have been met, the Call Center staff, internal business partners, and/or selected vendors shall record all incoming phone calls and may, as silent observers, randomly monitor and observe phone calls consistent with [Company] policy.

The following guidelines will be strictly adhered to:

1. All incoming calls into the Contact Center will be recorded. Calls that are transferred out of the Call Center will cease being recorded.
2. Call Center employees are hereby notified that silent monitoring and recording will occur on a regular basis. A pre-defined number of calls will be identified for evaluation regarding each employee providing telephone service to our customers.
3. Employees subject to call recording or monitoring are strongly encouraged to use a telephone that is not subject to recording or monitoring for personal calls. Employees should make every effort to confine their personal use of telephones to scheduled break times or the meal break.
4. In addition to the foregoing, calls may also be monitored, recorded, or observed for the purpose of analyzing existing telephonic systems and applications and not for the evaluation of individual employees.
5. The evaluation of calls will be strictly adhered to as published leveraging the [insert company model name] model of service interaction and workflow guidelines/expectations.
6. Only calls in which [Company] has a business or legal interest will be evaluated. A recording of a call that generates a legal or human resources issue for [Company] including but not limited to a call in which a Call Center employee uses offensive language or engages in inappropriate conduct may be reviewed by his or her manager as well as a member of the Human Resources department and that employee may become subject to performance management or other disciplinary action.
7. Training or developmental needs will be addressed and opportunities for improvement will be discussed.

Please note that the recording party shall keep confidential all claimant or customer information that is exposed to as part of the monitoring.

If you have any questions regarding the above, please contact and discuss with your manager prior to signing below.

By signing and dating in the space provided below, you are confirming that you have read, understand and hereby consent to the terms of this Notice and Consent to Telephone Monitoring and Recording.

_____
SIGNATURE

_____
DATE

CC: Employee Personnel File

Draft

Standard for the creation, use, storage and retention of Audio Recordings

Purpose

Audio Recordings present unique challenges to compliance efforts due to their specialized storage requirements and their inability to be full text indexed or reviewed except in real time. [Company] personnel should follow these standards with regards to the creation, use, storage, and retention of Audio Recordings unless such standard is superseded by an approved enterprise policy.

Standard

With the exception of those Audio Recordings that are specifically excluded from this standard, UnumProvident does not regard any Audio Recordings as official records of the corporation and they should not be retained once the information they contain has been extracted and the recording has ceased to have any legitimate business use. Additionally, notification that the conversation may be recorded is provided in any setting where [Company] employs recording technology.

Temporary Audio Recordings

Audio Recordings may be created and utilized at [Company] for only the following purposes.

1. The temporary recording and retention of Audio information from random external or internal sources for the purpose of training employees in customer service and quality assurance protocol. These recordings should be deleted once their value as training material has ended.

2. The temporary recording and retention of external customer communications if specifically required by contract. These Audio Recordings are made at the request of external customers and are temporarily retained for the exclusive use of the customer.

3. The temporary recording and retention of voicemail for the sake of customer convenience by providing extended service hours and improving customer service. After review and required entry of data, these recordings are automatically deleted by the voicemail recording system.

4. The temporary recording and retention of various Audio Recordings and data as part of programs testing new technology or developing data for the purpose of evaluating and improving customer service.

5. The temporary transmission or dissemination of training materials. [Company] uses a combination of technologies to provide remotely accessible training materials. However, [Company] does not consider the audio portions of these Recordings as official records of the corporation. [Company] recognizes only the distributed hardcopy information portion of training materials as official records and any incidental statements in an Audio Recording that may be construed to contradict the hardcopy portion of training materials is automatically superseded by the text of the hardcopy materials.

6. Statements made by officers of the corporation that were broadcasted or made available as Audio Recordings to the employees of the corporation.

Excluded from Standard

The following audio recordings are specifically excluded from this Standard and are retained according to the [Company] Retention Schedule:

- [Insert here any audio recordings that are actual business records]
- [Insert here any audio recordings that are subject to antispoliation requirements or record hold orders.]

System Approval

Any system or procedure that results in the creation, use and retention of any Audio Recording must be reviewed and approved by a member of the Law and Regulatory Affairs Department, the head of telephony operations, Information Security Architecture (ISA), and Information and Records Management (IRM) due to the special requirements they present for compliance, security, and retention.

M E M O R A N D U M

Re: Call Recording

Background:

Your company may receive customer requests to record telephone calls relating to service provided by company. The requests may range from wanting to record all calls with customer employees to just calls made to a Call Center or customer intake areas. Although each customer may articulate a slightly different rationale for its request, it appears that verifying tone and service as well as content are the predominant reasons that recording is requested.

Technology Options

In-house counsel advising on recording and monitoring solutions should work closely with their telephony areas to understand the technology used by the company. Generally, the two "locations" for connecting recording technology are trunk side (where the telephone line comes in to the company) and station side (on an individual telephone).

Applicable Considerations:

It is useful to consider these requests for recording, retaining, retrieving, and producing in three separate stages of the process:

1. Recording and Monitoring, which evoke wiretap and privacy considerations;
2. Retention and Retrieval, which evoke ERISA, preservation order, and discovery considerations; and
3. Production, which evokes privacy considerations.

1. Recording and Monitoring

Wiretap statutes: There are a number of federal and state laws governing the interception, monitoring, and recording of calls. The Omnibus Crime Control and Safe Streets Act, also known as the Electronic Communications and Privacy Act of 1986 (ECPA), and the Federal Communications Act both prohibit surreptitious recording of telephone calls. The FCC has specific requirements in connection with recording; there is also the Data Protection Act of 1998 which requires us to secure consent forms if we are going to monitor conversations. This memorandum focuses on ECPA.

ECPA makes it illegal to intercept, use, and disclose protected wire communications. It also prohibits procuring another (such as an ASO provider) to intercept, disclose or use such communication. This is a criminal statute that also has some civil remedies, including monetary damages.

There are two primary exceptions to ECPA:

1. The business extension exclusion allows an employer to intercept electronic communications using telephone equipment that is "being used by the subscriber or user in the ordinary course of business."

The first part of this exception relates to whether a communication is intercepted with "an electronic, mechanical or other device," which would be illegal. The exception exists if the interception is made instead by any "telephone or telegraph instrument, equipment or facility, or any component thereof." If your company uses a system which is an add-on digital recording system wired into the telephone, this may put you outside the business extension exception. The Circuits are split on whether systems wired into our telephone system allows us to use the business exception. If the recordings are stored on a server off your system, you are even less able to argue that it is your system. You then have Stored Communications Act considerations.

The second part is whether the recording is made in the ordinary course of business. There are two different analyses used by different jurisdictions to determine whether the business extension exclusion applies:

- The content approach focuses not on the employer's business justification for monitoring but on whether the nature of the monitored communication is business or personal.
- The context approach focuses on the employer's motive for the monitoring, such as quality control.

There are some weaknesses in an argument that a company is recording in the ordinary course of business if you capture every single call with a given customer to achieve the goal of quality or of content. The proportionality of the extent a company records compared to the extent of what is needed to secure appropriate quality would be considered and potentially found lacking. Further, the ordinary course of business exception may be lost if the company cannot clearly articulate what the business rationale is for recording.

2. The consent exclusion allows an employer to intercept the communications if the intended recipient or sender of the communication has given prior express or implied (not constructive) consent. Implied consent can be inferred from an employee's awareness of the monitoring. Federal law requires only one of the participants on the call to consent.

If we do not have the ordinary course of business exception, we look only to consent. In twelve states, the consent of all parties to a conversation is required (California, Massachusetts, Connecticut, Florida, Illinois, Maryland, Michigan, Montana, Nevada, New Hampshire, Pennsylvania and Washington). You will sometimes hear these referred to inaccurately as "two-party consent" laws; if there are more than two people involved in the conversation, all must consent to the taping. California has indicated that it will enforce its law against surreptitious recording of calls originating from or being placed to CA regardless of where the recording actually takes place.

Accordingly, companies which record all calls are at risk under the consent exception if the company makes or receives calls from multiple states unless that they can ensure that each call, outgoing as well as incoming, receives notification that the call is being recorded. The script of the message should reflect the actual recording policy so that the inferred consent is knowing and accurate. One possible script is, "Incoming and outgoing calls with [Company] are recorded for quality and verification purposes."

Because this script may generate some interest in litigation involving the company, you should consider whether business needs are met with recording of incoming calls only.

If a customer agreed to recording only incoming calls, the consent is easily managed by a recorded greeting. If your company were to try to capture all calls, on outgoing calls you would have to either implement a recording to preface outgoing calls before yoru representative comes on in person or train people to reliable announce that a call is being recorded at the beginning of a call. A comparable message should be left on voicemail as well. You would also have to have an alternative way of providing service if the customer objects to being recorded.

It would evidence of inferred consent if your company made multiple communications to customers regarding the recording practice. A company could provide written notice of the recording policy, perhaps in the contract or in our first mailing to the customer or potential callers. That would work for the caller but not necessarily for his or her dependents (considering the nature of your business).

Certain state laws provide more stringent protections than ECPA. For example, Washington state law requires that the consent actually be recorded. California law requires consent of everyone on the line. There is no "ordinary course of business" exception under CA law. CA law applies to calls placed both into and out of the state; CA courts have claimed jurisdiction even if the recording is not taking place in CA.

Technology and Implications: Technology can assist companies in reducing some of the risks of wiretap violations:

- Determine whether your vendor can provide technology that allows for cradle to grave recording (from when the call comes in to the company through any required transfers) across sites so long as the station side telephones are licensed and wired. Have a reliable solution for any remote employees who work from their homes.
- The technology exists where a company employee can engage and disengage the recording device (toggle on and off) regardless of whether we are using station side or trunk side locations. Failing to toggling on has customer service implications; failing to toggle off has wiretap/criminal implications.
- Determine what retrieval system your vendor can offer to assist in retrieving calls. Some vendors have key terms or fields in it that can lead to retrieval of calls. Make sure any RFPs for vendors have sophisticated retrieval systems.

If your company stays with station side recording, it must purchase licenses for each telephone subject to recordings. The risk of human error is largest with station side recording since it is a more manual operation than trunk side.

The longer term option is the trunk side recording which would allow all incoming customer calls to be recorded when they come in to the company. It could be programmed to capture only incoming calls, not outgoing ones. The company would have to license each user as well.

For both stations side and trunk side recording, you must obtain your employee's consent, ensuring that current consent forms are signed as employees transition into and out of jobs that require recording calls.

Penalties for Violation: The federal statutes provide criminal penalties for unlawful interception of telephone conversations, including up to five years' imprisonment or a maximum of $10,000 in fines. They also allow for civil remedies, by which private parties are entitled to recover actual and punitive damages, together with fees and costs.

Know your state laws for criminal wiretap of the states where you do business. For example:

California: California requires all parties to calls consent to recording. A violation is punishable by a fine of up to $2,500 imprisonment for not more than one year, or both. A civil plaintiff may recover the greater of $5,000 or three times the amount of any actual damages sustained. Cal. Penal Code § 637.2(a). It is also a crime to disclose information obtained from such an interception in California. A first offense is punishable by a fine of up to $2,500 and imprisonment for no more than one year. Subsequent offenses carry a maximum fine of $10,000 and jail sentence of up to one year. A civil action for invasion of privacy also may be brought against the person who committed the violation. Cal. Penal Code § 637.2.

Maine: Maine is a one party consent state. Interception of wire and oral communications is a "Class C" crime which carries with it a penalty of imprisonment for up to five years and a fine of up to $5,000. Under the statute, an interceptor is someone other than the sender or receiver of a communication who is not in the range of "normal unaided hearing" and has not been given the authority to hear or record the communication by a sender or receiver. 15 M.R.S.A. §709. Disclosure of the contents of intercepted communications, knowing the information was obtained by interception, is a violation of the criminal code as well. 15 M.R.S.A. §710. Anyone whose communications have been intercepted can sue for civil damages and recover the greater of $100 a day for each day of violation or actual damages, and also attorney fees and litigation costs. 15 M.R.S.A. §711.

Tennessee: Tennessee is a one party consent state. A person who is a party to a wire, oral or electronic communication, or who has obtained the consent of at least one party, can lawfully record a communication and divulge the contents of the recorded communication unless he has a criminal or tortious purpose for doing so. Violations are punishable as felonies with jail sentences of between two and twelve years and fines not exceeding $5,000. Tenn. Code Ann. §§ 39-13-602, 40-35-111.

Anyone whose communications have been unlawfully intercepted can sue to recover the greater of actual damages, $100 per day of violation or $10,000, along with punitive damages, attorney fees and litigation costs. Tenn. Code Ann. § 39-13-603.

Recording or disseminating a communication carried out through a cellular or cordless telephone, or disseminating the contents with knowledge of their illegal origin, without the consent of at least one party, can be punished as a felony with a potential prison sentence of between one and six years and a fine not to exceed $3,000. Tenn. Code Ann. §§ 39-13-604, 40-35-111

Massachusetts: Massachusetts requires all parties to calls consent to recording. It is a crime to record any conversation, whether oral or wire, without the consent of all parties in Massachusetts. The penalty for violating the law is a fine of up to $10,000 and a jail sentence of up to five years. Mass. Ann. Laws ch. 272 , § 99.

Disclosure of the contents of an illegally recorded conversation, when accompanied by the knowledge that it was obtained illegally, is a misdemeanor that can be punished with a fine of up to $5,000 and imprisonment for up to two years. Civil damages are expressly authorized for the greater of actual damages, $100 for each day of violation or $1,000. Punitive damages and attorney fees also are recoverable.

2. Retention and Retrieval

Industry Specific Laws: Different industries are governed by industry specific laws. For example, the insurance industry is governed by ERISA, the Employee Retirement Income Security Act, enforced by the Department of Labor. The DOL requires that "anything generated in the course of claims handling" be considered part of the claims file, and produced upon request. If there were recording of claims handling activities, such recordings would arguably need to produce them to the extent that they are considered part of the file. Consider the laws that are applicable to your industry as part of your analysis.

Preservation Order Concerns: If your company has preservation orders in effect that arguably require the retention of telephone recordings related to claims, you must preserve and be able to retrieve such recordings.

Record Management Concerns: From a records management perspective, companies may develop a standard or guideline on how to handle audio recordings. By adding "records" to your retention schedule, you may be questioned regarding any inconsistent practices of recording and retaining calls for one customer and not all customers.

An additional consistency concern would be if you record communications as business records and want to retain them only for 60 or 90 days. If your retention schedule identifies customer correspondence with a three year retention, it would be difficult from a records management perspective to differentiate between written and oral correspondence/calls. Also, for consistency, you would have to consider instituting a retention requirement for all customers if you determine such recordings are a business record.

In addition, voice recordings would need to be added to your policy, and then you would need to consider how to differentiate these from regular voice mail.

This retention topic cannot be taken lightly and should be discussed by yoru records management steering committee or the law department before a final decision is reached.

Discovery Concerns: In the context of our normal litigation, Rule 34 of the Federal Rules of Civil Procedure defines the term "document" to include phone records. Generally, much of the discovery undertaken in our claim litigation is pursued under the terms of this rule. The change in the federal rules makes it clear that electronic documents are included under the rule. Therefore, you will likely have to produce recordings of telephone conversations that you retain if it is the proper subject of inquiry in the litigation.

To be in compliance with Rule 34, you must develop, implement and monitor procedures that ensure that you company properly retains business record telephone recordings and has the ability to search and produce them in response to requests for claim files in discovery requests in litigated matters.

The failure for properly producing discoverable information can result in a wide range of penalties. Companies that knowingly fail to produce requested information are exposed to penalties as severe as a default judgment. An extreme example is found in Coleman Holdings, Inc. v. Morgan Stanley, Inc., 2005 WL 674885. The Opinion is lengthy but worth the read to understand the level of scrutiny and judicial skepticism that many attach to discovery in corporate America. The substantive claims at issue in the case were weak. Yet the sanction imposed, a default judgment, was quite draconian, as the claimed damages were about $700,000,000 and $2,000.000 in punitive damages. Significantly, no evidence was actually lost or destroyed, and the court entered these sanctions without finding that the omitted discovery would have affected the outcome of the case. This case focused on E-discovery, but one could see a similar outcome for similar failures in the context of telephone recordings. Another reason for appropriate technology is the discovery requirement for producing responsive recordings within 30 days of receiving a request.

You will need complete confidence from your vendor and your IT resources that you can accomplish these steps consistently and accurately before your company makes a commitment to undertake this effort. Finally, you can anticipate many additional costs associated with “searching and producing” data from telephony systems.

3. Production

Privacy Concerns: The Gramm-Leach-Bliley Act prohibits the release of any non-public financial and (often) non-public health information; HIPAA has limitations on how to store and limit disclosure of personal health information; and the Insurance Information and Privacy Protection Act (known as the 1982 Act, adopted in some form in approximately 17 states) prohibits the sharing of personal information, with some limited exceptions.

Based on the above, your company may not be able to legally provide actual copies of the recordings so your customer may or may not have its needs met if it is concerned with the tone of the call. However, most privacy concerns would be satisfied with an authorization signed by the participant agreeing to the disclosure of his or her private information. The alternative of de-identifying calls can be time consuming and thereforer not an attractive solution.

Conclusion:

Recording and Monitoring: Companies must invest in the technology that would sufficiently minimize legal risks of violating wiretap laws and preservation orders. Likewise, the technology purchased must have sufficient capacity to assist in meeting standards in record retention and for discovery concerns.

Trunk side recording is the most reliable for securing consent on incoming calls only. Alter recorded greetings and obtain revised consent forms from your employees. Provide an alternative means of doing business if a caller does not consent. Station side recording has the most risk since it would involve constant toggling on and off of recording. Any toggling on and off is fraught with human error and provides exposure to criminal violations.

The risks are most reduced if your company agrees to record only incoming calls to a limited area of the business (e.g. an intake area or a call center) if you have trunk side recording of those calls. Alter the recorded greeting to get inferred consent and tailor internal employee consent forms to apply the broadest protection possible for the company.

Retention and Retrieval: Your company would need to work out a process for cataloguing, holding, and retrieving recordings that are certainly discoverable in the claims arena if you record for business records.

For audio recordings that are business records, you would need to set up appropriate processes, auditing and enforcing compliance with those; you would need to comply with any retention requirements; any you should deal with legal issues that arise (such as whether such recordings should be "housed" with a specific file and produced when the file is produced. In the context of litigation, your deponents will need to be prepared to testify about what is recorded and why and explain retention procedures. You should also budget for the costs of reproduction, etc. The very same concerns relating to email preservation apply to telephone call recordings and vice verse. Should a recording be discarded inappropriately or lost, the spoliation consequences can be substantial.

The discoverability and preservations order issues are of a magnitude that many litigators do not support the customer requests for broad call recording.

Production: This is a privacy concern. Your business may be involved in handling very sensitive personal information regarding customer financial or health information. If protected information is present and incapable of being de-identified, you cannot provide copies, electronic or otherwise, to the customer. Screening the calls for production would be labor intensive.

Additionally, your customers may benefit from having you explain the down-side to them of getting recorded information, particularly private health information. Specifically, they would have to put into place certain safeguards regarding privacy, and they are disadvantaged in the context of disability discrimination and the ADA if they know about their employees’ specific health problems. Additionally, customers may not appreciate that the privacy limitations that you have in place are for the benefit of their employees and their dependents.

Of course, if you get authorizations from the individual caller, you can release information private to them.

Attachments: Chart with Tape Recording Laws at a Glance

Tape-recording laws at a glance

	Is consent of all parties required?	Are there criminal penalties?	Does the statute allow for civil suits?	Is there a specific hidden camera law?	Are there additional penalties for disclosing or publishing information?
Federal		☑	☑		☑
Alabama		☑		☑	☑
Alaska		☑		☑	☑
Arizona		☑		☑	
Arkansas		☑		☑	
California	☑	☑	☑	☑	☑
Colorado		☑			☑
Connecticut	☑	☑	☑		
Delaware		☑	☑	☑	☑
D.C.		☑	☑		☑
Florida	☑	☑	☑		
Georgia		☑	☑	☑	
Hawaii		☑	☑	☑	☑
Idaho		☑	☑		☑
Illinois	☑	☑	☑	☑	☑
Indiana		☑	☑		☑
Iowa		☑			☑
Kansas		☑		☑	☑
Kentucky		☑			☑
Louisiana		☑	☑	☑	☑
Maine		☑	☑	☑	☑
Maryland	☑	☑	☑	☑	☑
Massachusetts	☑	☑	☑		☑
Michigan	☑	☑	☑	☑	☑
Minnesota		☑	☑	☑	☑
Mississippi		☑	☑		☑
Missouri		☑	☑	☑	☑
Montana	☑	☑			☑
Nebraska		☑	☑		☑
Nevada	☑	☑	☑		☑
New Hampshire	☑	☑	☑	☑	☑
New Jersey		☑	☑		☑
New Mexico		☑	☑		☑
New York		☑			☑
North Carolina		☑	☑		☑
North Dakota		☑			☑
Ohio		☑	☑	☑	☑
Oklahoma		☑			☑
Oregon		☑		☑	
Pennsylvania	☑	☑	☑	☑	☑
Rhode Island		☑	☑		☑
South Carolina		☑	☑	☑	
South Dakota		☑		☑	
Tennessee		☑	☑	☑	☑
Texas		☑	☑		☑
Utah		☑	☑	☑	☑
Vermont					
Virginia		☑	☑		☑

Washington	☑	☑	☑		
West Virginia		☑	☑		☑
Wisconsin		☑	☑		☑
Wyoming		☑	☑		☑

SAMPLE

Guidelines - Telephone, Fax, Voice Mail & E-Mail Monitoring

Telephone Monitoring - Listening

Listening to both sides of a telephone conversation is permissible if it is done in the ordinary course of business. "Ordinary course of business" may include a variety of matters in which [Company] has a business or legal interest, such as quality assurance, customer satisfaction, or performance management or disciplinary concerns. It may include but is not limited to such matters as training, measuring job performance, and measuring customer service and satisfaction, or ensuring compliance with company polices.

[Company] guidelines are:

- Employees in business units, e.g. Customer Contact Centers, Producer Compensation, Group Customer Service, etc., whose conversations typically are monitored must be notified in advance of the practice, why it is being done, and how it will be done;
- [Company] employees having telephone contact with [Company] business units subject to monitoring are on notice that their contact with employees in those business units may be monitored in accordance with these guidelines;
- Employees are strongly encouraged to make personal calls in conference rooms or using telephones where calls are not recorded or monitored;
- Monitoring shall not take place during scheduled breaks or lunch periods when employees are more likely to make personal calls;
- Only calls in which [Company] has a clear business or legal interest will be monitored; as soon as it is clear that a call is of a purely personal nature, monitoring shall cease;
- Information learned while determining if the call is of a personal or business nature may not be used against the employee if the information does not constitute a clear violation of public policy or hold a clear legal or business interest for the Company. Personal information may be considered in cases where the employee's personal use of the telephone has been previously prohibited or restricted by his/her management;
- Listening may be done only by employees whose job responsibilities include the monitoring of calls or enforcement of company policies; in most cases, this means supervisors, persons monitoring for training purposes, human resource representatives, or legal personnel;
- Only employees with monitoring responsibilities may have access to or activate the monitoring capability of a telephone.

Telephone Monitoring – Recording

Recording telephone conversations is permitted for valid business reasons, and certain conditions must be met. [Company]'s guidelines are:

- The employees who are subject to recording for quality or other business purposes must be informed in advance that the conversation will be recorded and consent to the recording;
- [Company] employees having telephone contact with [Company] business units subject to monitoring are on notice that their contact with employees in those business units could lead to the recording of their calls consistent with these guidelines;
- Parties calling in on the 800 or 877 lines shall be notified that all calls to [Company] Corporation may be recorded for quality purposes unless advised otherwise. Employees must also leave a notification on their voicemail message that calls to [Company] may be recorded for quality purposes.
- If any party to a conversation that is being recorded changes his/her mind and objects to the recording, the manager or lead person in charge of recording must be notified and, upon such notice, cease any recording immediately;
- A copy of a recorded conversation must be made available upon written request of the employee if received within 60 days of the call;

- Only calls in which [Company] has a business or legal interest may be recorded.

E-Mail Monitoring
E-mail sent from or stored on [Company] assets are the property of [Company]. Please review the policy on Use and Privacy of [Company] Assets on [company intranet or in company handbook.] There is no privacy interest between you and [Company] with regard to emails stored on [Company] assets.
As among employees, access to any E-mail box that is not your own shall occur only as follows:

- Employees shall not provide their User ID or password to allow anyone else access to their e-mail box;
- Employees may give delegation authority as provided by [Company]'s Guidelines on E-mail Use; or
- The message recipient's immediate supervisor shall make a written or E-mail request from to the appropriate security administrator for a password to the mail box; the request must state the reason access is needed and be counter-signed by or forwarded from the User ID of a second [Company] supervisor or manager.

The company shall have access to employees' e-mail stored on [Company] assets at its own discretion at all times.

Voice Mail Monitoring
Voice mail "boxes" are protected by passwords that, by [Company] policy, are supposed to be known only to the owner of the telephone extension (Phone mail). There are two ways for a person other than the owner to gain access to messages in these "boxes:"

- with the oral permission of the message recipient and his/her voluntary disclosure of the password necessary to gain access;
- with a written or E-mail request from the message recipient's immediate supervisor to the appropriate security administrator for a password to the mail box; the request must state the reason access is needed and be counter-signed by or forwarded from the User ID of a second [Company] supervisor or manager.

Once access to the voice mail box has been obtained, certain guidelines must be followed:

- Only messages in which [Company] has a business or legal interest may be monitored; once it is clear that a message holds no business or legal interest, monitoring must cease;
- personal information learned while determining if the message is of a personal or business nature may not be used against the employee in any way, except in a case where the employee's personal use of voice mail or E-mail has been previously prohibited or restricted by his/her management; misconduct in violation of company policy has occurred; or if it causes [Company] to have heightened potential legal liability;
- except in cases of an ongoing investigation of possible employee misconduct, the person monitoring the message must notify the intended recipient whenever the content of a message is monitored; this should be done as soon as possible following the event.

Monitoring and Potential Employee Misconduct
Any monitoring of telephone conversations or of fax, voice mail or E-mail messages in connection with an investigation of possible employee misconduct shall include an Employee Relations Consultant from the Human Resources Department and others on a need to know basis only.

Effective [Date]

ICT usage policies

By: Chris Edwards

USA
July 24 2008

The ubiquitous nature of information communications technology in the modern work environment has proved to be both a blessing and a curse for companies. The advantages provided by the Internet, emails and instant messaging are tempered with the risks that such functionality can bring when used improperly by employees.

Numerous examples exist of companies paying the price for misuse of ICT by their employees. In the United States it has been reported that by 2007, 27 per cent of Fortune 500 companies had dealt with claims stemming from employee misuse and abuse of corporate email and Internet systems. For example, Chevron Corp. settled with four employees for $2.2million after offensive messages had been sent to them by co-workers using its internal email system.

In order to avoid financial and reputational damage and ensure ICT systems operate efficiently, companies need to provide their employees with clearly worded and comprehensive policies which mark the boundaries of acceptable usage of company-owned ICT.

In this article, we highlight some of the key issues and offer some practical guidance for companies who are seeking to either create an ICT usage policy or perhaps ensure an existing policy meets best practice.

A policy should seek to specifically define the type of behaviour, in relation to ICT, which is strictly prohibited. At a minimum, this should include:

use for illegal purposes;
threatening, intimidating or harassing other employees;
storage and distribution of unlicensed copyright material;
introduction of viruses/trojan horses;
creating and/or distributing offensive content;
unauthorised access to ICT; and
unauthorised distribution of confidential information via ICT systems.

A policy should also provide as much guidance as possible on the scope of what may be acceptable. Areas often covered include:

the use of storage devices with company ICT;
downloading of content from the Internet; and
express rules relating to certain websites (eg personal blogs/social networking/p2p sites).

In addition, the company needs to ensure a policy co-exists with relevant employment and business rules/regulations.

Personal use

Many employers have realised that personal Internet and email usage is now an accepted part of the modern working environment. Therefore, companies often seek to define specifically what they deem to be acceptable personal usage, eg "The Employee may make reasonable personal use of the Company's ICT provided it does not interfere with the Employee's duties (eg personal usage up to 30 minutes at lunchtimes is unlikely to be deemed excessive or interfering with duties)." In any such clause, it needs to be made clear that personal use of ICT remains at the sole discretion of the company, the principle being that such use is a privilege rather than a right.

Privacy

A policy should be clear that the company does not give any guarantee of "privacy" and that the employee should not have any expectation of privacy regarding his/her use of company owned ICT, including in relation to their personal use. Employees often wrongly assume that personal use of a company's ICT systems is private. Further, employees need to be aware that any content created during the course of their

employment belongs to the company (subject to applicable local laws). For example, many policies state that, "all electronic information created, stored, sent or received by the Employee using the Company's ICT is the property of the Company".

Monitoring

A company will need to review its own culture and internal systems before deciding on whether to monitor its employees' usage of ICT. It is critically important that companies seek local legal advice on the issue of monitoring in their respective jurisdiction. In the UK for example, a company is only allowed to monitor its employees' usage of ICT where there are legitimate reasons and the means used are proportionate to the objectives of the monitoring. It is prudent for all companies to obtain an employee's express consent before any monitoring occurs. A policy should clearly state that the company reserves its right to conduct routine monitoring and has the ability to intercept, read, review, delete and/or access all messages and computer files on an employee's ICT system (so far as is in accordance with local law).

ICT users

A policy should be drafted to ensure it covers the full range of potential users (including employees, part-time workers, subcontractors and customers) who may come into contact with and use company ICT. A policy should also seek to be "technology neutral" in order to capture the different technologies which comprise ICT and its evolving nature so as to avoid the need for continual revision upon the introduction of new company ICT.

Incorporation

A policy should be "visible" to employees at all times. Policies are often distributed with employment contracts requiring an employee's signature, available through a prominent weblink on a company's intranet site or through the provision to employees of staff handbooks. Different language versions of the policy should also be provided where applicable. Companies may also consider providing training courses to ensure employees cannot, at a later date, deny knowledge of the policy. These actions will ensure that employees are continually made aware of the scope of permitted usage of a company's ICT.

Enforcement

To be effective, enforcement of a policy is key. The policy should set out an enforcement mechanism (triggered by a breach of the "scope of use") that could lead to loss or limit on use of ICT before actual dismissal. The policy should be tied in to the company's general disciplinary procedures. In addition, a policy should state that a breach of the policy could result in civil or criminal penalties depending on the jurisdiction in question. Proper enforcement of a procedure set out in a policy will serve to put employees on notice as to the seriousness of misusing company-owned ICT systems. On a regular basis, a company should conduct regular reviews of a policy to ensure it remains relevant and is being adhered to.

Compliance with law

Although common best practice principles exist, the scope of policies are largely dictated by the applicable law in the jurisdiction in which the policy will be used. Before implementing a policy, a company should obtain specialist ICT and employment law advice to ensure a proposed policy is compliant with local law and practice. Failure to do so may result in the policy (or a part thereof) being unenforceable or even illegal.

We have outlined above some of the main elements of a policy covering employee usage of a company's ICT. In summary, a policy needs to reflect the practical reality that employees use ICT in a personal context and ensure that prohibited usage and associated penalties are accurately defined and understood.

Chris Edwards is an English qualified lawyer in the Technology, Media and Commercial group of DLA Piper based in Dubai.

Useful Links and Online Resources

Citizens Media Law Project: Newsgathering and Privacy

http://www.citmedialaw.org/legal-guide/newsgathering-and-privacy

Citizen Media Law Project: State Law: Recording

http://www.citmedialaw.org/legal-guide/state-law-recording

Reporters Committee for Freedom of the Press: "Can We Tape?"

http://www.rcfp.org/taping/

ELT's Whitepapers and Excerpts from the National Employer ® Chapter 18 Employee Privacy Rights

http://www.elt-inc.com/Employee_Privacy_Rights.htm