

United States Government
National Labor Relations Board
OFFICE OF THE GENERAL COUNSEL
Advice Memorandum

DATE: September 27, 2016

TO: Cornele A. Overstreet, Regional Director
Region 28

FROM: Barry J. Kearney, Associate General Counsel
Division of Advice

SUBJECT: Cascade Financial Services
Case 28-CA-176473

512-5012-0125
512-5012-0133-5000
512-5012-1725
512-5012-1725-0150
512-5012-1725-8800
512-5012-1737
512-5012-1737-0183
512-5012-1737-6900
512-5012-3322
512-5024-5400
512-5072-2000

The Region submitted this case for advice as to whether it is an appropriate vehicle to urge the Board to expand its holding in *Purple Communications, Inc.*¹ to find the Employer's prohibition against its employees' use of its internet connection for non-business purposes on nonworking time unlawful. Further, the Region requested advice as to whether some of the Employer's content restrictions contained in its "Acceptable Use of Electronic Communications" protocol are similarly unlawful. Finally, the Region also requested advice as to whether the Employer's rule reserving its right to monitor the employees' use of its electronic communications system is lawful.

The Employer's rules explicitly prohibit personal use of its internet connection. We therefore conclude that given that employees use the Employer's electronic communications systems, including the internet connection, extensively while at work, this matter is an appropriate vehicle to expand the rationale of *Purple Communications* to cover the Employer's internet connection and find that employees have a Section 7 right to use that connection during nonworking time for protected communications. Furthermore, we find that certain of the provisions in the Employer's "Acceptable Use of Electronic Communications" policy are overly broad

¹ 361 NLRB No. 126 (Dec. 11, 2014).

because they chill employees' exercise of their Section 7 rights under *Lutheran Heritage Village-Livonia*.² However, we conclude that the Employer's reservation of the right to monitor employees' use of its electronic communications system is lawful.

FACTS

The Employer underwrites, originates, and services loans for the manufactured housing industry. It has its headquarters in Gilbert, Arizona, and offices in Buda and Dallas, Texas.

The Employer reports that all of its employees use the Employer's computer system and internet connection on a daily basis. Some use those resources several times a day, while others use them constantly. Employees use those resources to engage in email communications with customers, vendors, and colleagues as needed to fulfill job responsibilities; prepare and process loan applications; schedule meetings; conduct research to gather information required for processing loan applications; create spreadsheets, presentations, letters, and other business documents; log into a web-based time-keeping system; and complete other projects. The Employer uses several different computer programs and provides employees with access to Google Chrome and Internet Explorer so they may fulfill their job responsibilities. Employees do not share computers, and each employee has access to their own personal network.

The Employer has a multilayered anti-virus system, which scans emails and documents for viruses and malware, a virus protector on its firewall, and an anti-virus program on its servers and PCs.

The Employer maintains a personnel handbook. The handbook includes certain policies relating to electronic communications and internet usage, including a ban on personal use of its internet connection and a reservation of the right to monitor internet usage. The Employer also requires employees to sign a separate document that substantially reproduces these policies and also includes an "Acceptable Use of Electronic Communications" protocol. Relevant parts of both documents are reproduced below.

² 343 NLRB 646, 646-47 (2004).

A. The Employer's Policies For Use of Its Internet and Electronic Communications Systems

Internet Usage

... The Internet is intended for business use only. Use of the Internet for any non-business purpose, including but not limited to, personal communication or solicitation, purchasing personal goods or services, gambling and downloading files for personal use, is strictly prohibited.

Acceptable Use of Electronic Communications

... [I]ncidental and occasional personal use of our Systems³ that does not interfere or conflict with productivity or the company's business is permitted

Employees may not use our Systems in a manner that violates our policies including but not limited to Non-Harassment, Sexual Harassment, Equal Employment Opportunity, Confidentiality of Borrower Matters, Care of Borrower Records, Solicitation and Distribution, Electronic Mail and Monitoring, Voice Mail and Monitoring, and Internet Usage and Monitoring. Employees may not use our Systems in any way that may be seen as insulting, disruptive, obscene, offensive, or harmful to morale. Examples of prohibited uses include, but are not limited to, sexually-explicit drawings, messages, images, cartoons, or jokes; propositions or love letters; ethnic or racial slurs, threats, or derogatory comments; or any other message or image that may be in violation of company policies.

In addition, employees may **not** use our Systems:

- To download, save, send or access any defamatory, discriminatory or obscene material;
- ...

³ "Systems" are defined as various communications devices, including those with an internet connection.

- To download anything from the internet (including shareware or free software) without the advance written permission of the Systems Supervisor;
- ...
- To access any “blog” or otherwise post a personal opinion on the intranet;
- To solicit employees or others

B. The Employer’s Policy Regarding Monitoring of Internet Usage

Consistent with applicable federal and state law, the time you spend on the Internet may be tracked through activity logs for business purposes. All abnormal or inappropriate usage will be investigated thoroughly. For business purposes, management reserves the right to search and/or monitor the company's Internet usage and the files/transmissions of any employee without advance notice and consistent with applicable state and federal laws. Employees should expect that communications that they send and receive by the Internet will be disclosed to management. Employees should not assume that communications that they send and receive on Cascade property or through Cascade email are private or confidential.

C. Employer’s Position on Special Circumstances

In response to the Region’s inquiry about any special circumstances privileging its prohibition of non-business use of its computer system and Internet connection during nonworking time, the Employer explained that, since it is a mortgage company, its employees have access to highly confidential and privileged information about borrowers, protected by both state and federal law. The Employer states that its policies help protect it from liability associated with employees improperly using this privileged and highly confidential information and decrease the possibility of identity theft, which constitutes a real concern for its customers.

ACTION

We conclude that the Region should use this case as a vehicle to urge the Board to extend the rationale of *Purple Communications* and allege that the Employer's policies violate Section 8(a)(1) by prohibiting employees from using its internet connection during nonworking time for Section 7 purposes. Further, we conclude that given that the Employer's "Acceptable Use" protocol permits incidental personal use of its electronic communications systems, certain content restrictions contained therein, as described below, are overly broad under *Lutheran Heritage Village-Livonia*.⁴ Finally, we conclude that the Employer's rules reserving its right to monitor the employees' use of its electronic communications systems are lawful.

A. The Employer's Ban of Internet Access for Personal Use

Under the Board's recent decision in *Purple Communications*, employees have a Section 7 right to use their employer's email system for statutorily protected communications on nonworking time if employees have been granted access to the employer's email system in the course of their work.⁵ Thus, any rule maintained by an employer that limits or chills an employee's protected email communications on nonwork time is presumptively unlawful.⁶ To justify a total ban on employees' nonwork use of email, an employer must demonstrate that "special circumstances make the ban necessary to maintain production or discipline."⁷ The Board's decision in *Purple Communications* specifically focused on the employer's email system and did not address other electronic communications systems employees use at work.⁸ However, the Board noted that "[o]ther interactive electronic communications ... may ultimately be subject to a similar analysis."⁹

Here, the Employer bans employee access to its internet connection for non-business purposes. The internet shares many of the same features as email that were

⁴ 343 NLRB at 646-47.

⁵ 361 NLRB No. 126, slip op. at 1.

⁶ *See id.*

⁷ *Id.*

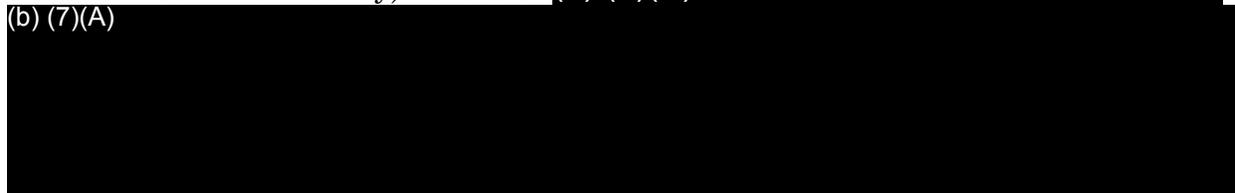
⁸ *Id.* at 14.

⁹ *Id.* at 14 n.70.

discussed by the Board in *Purple Communications*.¹⁰ Thus, the internet has become a critical means of communication in modern society, including for Section 7 purposes, for instance through social media and blogs.¹¹ Like communication by email, communication through the internet permits employees to wait to respond to messages until they are on nonworking time, and employees can easily ignore or delete messages.¹² Additionally, like email, not all employees have access to the internet outside of the workplace.¹³ Further, many employees may feel more

¹⁰ For example, the internet is one of the most efficient mechanisms for sharing information and opinions and has changed how individuals communicate in the twenty-first century. See, e.g., Jeffrey M. Hirsch, *The Silicon Bullet: Will the Internet Kill the NLRA?*, 76 Geo. Wash. L. Rev. 262, 274-75 (2008) (discussing the internet's transformative effect on how Americans communicate, providing access to websites, blogs, and instant messaging); Susannah Fox & Lee Rainie, *The Web at 25 in the U.S.* (February 27, 2014), available at <http://www.pewinternet.org/2014/02/27/part-1-how-the-internet-has-woven-itself-into-american-life> (87% of U.S. adults reported using the internet in 2014 study). See also (b) (7)(A)

(b) (7)(A)



¹¹ See, e.g., *Triple Play Sports Bar & Grille*, 361 NLRB No. 31, slip op. at 1-4, 6-8 (Aug. 22, 2014) (discussing employees' protected right to engage in Facebook discussions and finding employer's internet/blogging policy to be unlawfully overbroad), *aff'd sub nom. Three D, LLC v. NLRB*, 629 F. App'x 33 (2d Cir. 2015); *Purple Communications*, 361 NLRB No. 126, slip op. at 40-42 (Member Johnson, dissenting) (discussing the role of internet-accessible personal email and online social media networks); Jeffrey M. Hirsch, *The Silicon Bullet: Will the Internet Kill the NLRA?*, 76 Geo. Wash. L. Rev. at 274-75 (noting that "[w]idespread Internet availability in the workplace has provided unions with an important tool – which they have actively used – to organize and communicate with employees [U]nion campaigns frequently rely on employees' ability to use the Internet to instigate or support organizing activity.”).

¹² Cf. *Purple Communications*, 361 NLRB No. 126, slip op. at 15 & n.72 (noting the similar attributes of email).

¹³ Cf. *id.*, slip op. at 6 n.18 (recognizing that due to costs and other circumstances, “some employees do not privately use any electronic media”). Although the internet may not be the same “natural gathering place” for employees of a particular employer

comfortable engaging in Section 7-related communications via personal email over the internet or via instant messenger communications, as opposed to an employer-provided email account.

The Employer's employees regularly use the Employer's electronic communications systems, including its internet connection, in the course of their work, and the Employer explicitly bans all non-business use of its internet connection. In these circumstances, applying the underlying rationale of *Purple Communications*, we conclude that the Employer's ban violates the Act unless the Employer can establish special circumstances.

In order to establish a defense to its prohibition against Section-7 protected use of its internet connection, the Employer "must demonstrate the connection between the interest it asserts and the restriction" it imposed.¹⁴ "The mere assertion of an interest that could theoretically support a restriction will not suffice."¹⁵ The Employer essentially asserts that its ban on non-business use is justified by the need to protect sensitive private and financial information about clients. But the Employer maintains a multilayered anti-virus system to scan emails and documents for viruses and malware, a virus protector on its firewall, and an anti-virus program on its servers and PCs, all of which enable its employees to safely access the internet for work. Given these protections, the Employer has failed to explain how permitting employees to use its internet connection for non-business purposes during nonworking time would create any greater risk of disclosure of client information than permitting employees to access the internet for business purposes. In both circumstances access to the internet is initiated through the use of a web browser that is actively monitored and secured. Thus, the Employer has not established special circumstances.

as an employer's email system, *see id.*, workers are increasingly turning to social media while at work to build connections with their co-workers. A recent survey showed that 17% of workers use social media on the job to "build or strengthen personal relationships with coworkers" and the same percentage uses social media "to learn about someone they work with." *See* Kenneth Olmstead, Cliff Lampe & Nicole B. Ellison, *Social Media and the Workplace*, available at <http://www.pewinternet.org/2016/06/22/social-media-and-the-workplace> (June 22, 2016).

¹⁴ *Purple Communications, Inc.*, 361 NLRB slip op. at 14.

¹⁵ *Id.*

In all these circumstances, we conclude that this case is a good vehicle to present the Board with an opportunity to expand its holding in *Purple Communications* to the Employer's ban on the use of its internet connection for non-business purposes.

B. The Employer's "Acceptable Use" Policy

Since the Employer permits some personal use of its electronic communications systems under its "Acceptable Use" policy, we examine the substantive content restrictions in that policy to see if they limit or chill employees in the exercise of their Section 7 right.

It is well-settled that the mere maintenance of an overly broad rule violates Section 8(a)(1) because it "tends to inhibit or threaten employees who desire to engage in legally protected activity but refrain from doing so rather than risk discipline."¹⁶ The Board has developed a two-step inquiry to determine if a work rule would reasonably tend to chill protected activities.¹⁷ First, a rule is clearly unlawful if it explicitly restricts Section 7 activities. Second, if it does not, the rule will nonetheless violate Section 8(a)(1) if: (1) employees would reasonably construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights.¹⁸ In determining how an employee would reasonably construe a rule, particular phrases should not be read in isolation, but rather considered in context.¹⁹ Rules that are ambiguous as to their application to Section 7 activity and contain no limiting language or context that would clarify to employees that the rule does not restrict Section 7 rights are unlawful.²⁰ In contrast, rules that clarify and restrict their scope

¹⁶ *Beverly Health & Rehabilitation Services*, 332 NLRB 347, 349 (2000), *enforced*, 297 F.3d 468 (6th Cir. 2002). *See also Lafayette Park Hotel*, 326 NLRB 824, 825 (1998) (finding that the mere maintenance of a rule that would reasonably have a chilling effect on employees' Section 7 activity violates Section 8(a)(1)), *enforced mem.*, 203 F.3d 52 (D.C. Cir. 1999).

¹⁷ *Lutheran Heritage Village-Livonia*, 343 NLRB 646, 646-47 (2004).

¹⁸ *Id.*

¹⁹ *Id.* at 646.

²⁰ *See 2 Sisters Food Group*, 357 NLRB 1816, 1817 (2011) (finding rule that subjected employees to discipline for "inability or unwillingness to work harmoniously with other employees" unlawful absent definition of "work harmoniously"); *University Medical Center*, 335 NLRB 1318, 1320-22 (2001) (finding work rule that prohibited

by including examples of clearly illegal or unprotected conduct, such that they would not reasonably be construed to cover protected activity, are not unlawful.²¹ Any ambiguity in an employer's rule is construed against the employer as the promulgator of that rule.²²

Applying those principles here, we find the following rules unlawfully overbroad. First, in the "Acceptable Use" protocol the Employer bars use of the Employer's systems for various types of conduct that employees would reasonably understand to encompass Section 7 activities, including using the systems in a manner that could be seen as "insulting, disruptive ... offensive, or harmful to morale."²³ Although the rule subsequently sets forth some clarifying examples that do not implicate Section 7 concerns (such as sexually-explicit messages and ethnic or racial slurs), at least one example, the prohibition against "derogatory comments," does encompass Section 7 activity.²⁴

Second, in the first bullet point of the Employer's "Acceptable Use" protocol, the Employer prohibits the use of its electronic communications system "to download,

"disrespectful conduct towards [others]" unlawful because it included "no such limiting language [that] removes [the rule's] ambiguity and limits its broad scope"), *enforcement denied in relevant part sub nom., Community Hospital Centers of Central California v. NLRB*, 335 F.3d 1079 (D.C. Cir. 2003).

²¹ See *Tradesmen International*, 338 NLRB 460, 460-61 (2002) (determining that prohibition against "disloyal, disruptive, competitive, or damaging conduct" would not be reasonably construed to cover protected activity, given the rule's focus on other clearly illegal or egregious activity and the absence of any application against protected activity).

²² *Lafayette Park Hotel*, 326 NLRB at 828 (citing *Norris/O'Bannon*, 307 NLRB 1236, 1245 (1992)).

²³ See, e.g., *UPMC*, 362 NLRB No. 191, slip op. at 1 & n.5, 21 (Aug. 27, 2015) (electronic messaging policy that barred nonwork use that "may be disruptive" or "offensive" or "harmful to morale" found unlawful); *NCR Corp.*, 313 NLRB 574, 577 (1993) (unlawful rule restricting bulletin board postings that contain "offensive language").

²⁴ See *Southern Maryland Hospital*, 293 NLRB 1209, 1222 (1989) (rule prohibiting "derogatory attacks on ... hospital representative[s]" unlawful), *enforced in relevant part*, 916 F.2d 932, 940 (4th Cir. 1990)).

save, send or access any defamatory, discriminatory or obscene material.” The Board has found the term “defamatory” unlawfully overbroad because it would chill concerted communications regarding an employer’s treatment of its employees, among other Section 7 topics, for fear of discipline if someone determined that those statements were inaccurate or untrue.²⁵

Third, in a following bullet point, the Employer prohibits “download[ing] *anything* from the internet ... without the advance written permission of the Systems Supervisor” (emphasis added). This prohibition would be reasonably read to prohibit downloading material for protected activity, such as organizing materials (including election petitions and authorization cards) and information regarding statutory rights, and thus would unlawfully interfere with Section 7 activity. While the Employer specifically references “shareware and free software,” and might be able to establish special circumstances justifying a restriction upon downloading those,²⁶ the Employer’s rule prohibits downloading *anything* and thus is not narrowly tailored to address legitimate business concerns. Moreover, the requirement of prior managerial approval of such activity is also unlawful.²⁷

²⁵ See *Quicken Loans, Inc.*, 359 NLRB 1201, 1201 n.3, 1205 (2013) (rule requiring employees to not “publicly criticize, ridicule, disparage or defame” employer found unlawfully overbroad), *incorporated by reference*, 361 NLRB No. 94, slip op. at 1 n.1 (Nov. 3, 2014), *enforced*, ___ F.3d ___, 2016 WL 4056091 (D.C. Cir. 2016); *Great Lakes Steel*, 236 NLRB 1033, 1037 (1978) (rule prohibiting “defamatory” literature found unlawfully overbroad because rule would apply to employee speech that did not involve malice), *enforced*, 625 F.2d 131 (6th Cir. 1980). See generally *Linn v. Plant Guard Workers Local 114*, 383 U.S. 53, 61-63 (libelous statements remain protected under Section 7 unless they were made with malice).

²⁶ Cf. *Space Coast Credit Union*, Case 12-CA-141201, Advice Memorandum dated Mar. 2, 2016, pp. 8-10 (finding employer established a special circumstances defense with regard to downloadable instant messaging programs because of the increased security risk associated with them, particularly where the employer is in a business that deals with sensitive customer information).

²⁷ See, e.g., *Lily Transportation Corp.*, 362 NLRB No. 54, slip op. at 2-3, 8 (Mar. 30, 2015) (rule unlawfully overbroad where, among other things, it required prior approval before posting communications about the employer or employees on the internet); *Trump Marina Associates*, 354 NLRB 1027, 1027 n.2 (2009) (two-member Board) (rule requiring employees to obtain prior authorization from management before releasing statements to the media found overly broad), *adopted by a three-member panel*, 355 NLRB 585 (2010), *enforced mem.*, 435 F. App’x 1 (D.C. Cir. 2011).

Fourth, that portion of the Employer’s “Acceptable Use” protocol that prohibits the employees from “access[ing] any ‘blog’ or otherwise post[ing] a personal opinion on the intranet” would reasonably be construed to encompass protected activity, such as the voicing of opinions about unionization or the Employer’s labor relations policies, and is unlawful for that reason.²⁸

Lastly, the Employer’s “Acceptable Use” protocol bars use of the employer’s electronic communications system “to solicit employees or others.” This prohibition squarely encompasses Section 7 communications and, since the prohibition is not limited to working time, it is unlawfully overbroad.²⁹

Thus, each of these rules would be unlawful under a *Lutheran Heritage* analysis.³⁰

C. The Employer’s Policy Regarding Monitoring of Internet Usage

The Employer’s internet monitoring policy, which provides for tracking of internet usage and warns employees that their communications over the internet may

²⁸ See *Allegheny Ludlum Corp.*, 333 NLRB 734, 740, 744 (2001) (citation omitted) (Section 7 protects both the “right to express an opinion or to remain silent” about protected or union activity), *enforced*, 301 F. 3d 167 (3rd Cir. 2002).

²⁹ See, e.g., *Casino San Pablo*, 361 NLRB No. 148, slip op. at 3-4 (Dec. 6, 2014) (rule prohibiting solicitation in workplace at any time for any purpose overbroad and unlawful); *Our Way, Inc.*, 268 NLRB 394, 394 (1983) (“[t]he governing principle is that a rule is presumptively invalid if it prohibits solicitation on the employees’ own time,” citing to *Republic Aviation Corp. v. NLRB*, 324 US 793 (1945)). Cf. *Stoddard-Quirk Manufacturing Co.*, 138 NLRB 615, 621 (1962) (employer may lawfully prohibit solicitation on working time). We note that the Internet Usage policy also specifically bans solicitation over the internet, without limitation to working time, and is unlawful for that reason as well.

³⁰ Given that these rules are unlawfully overbroad under *Lutheran Heritage Village-Livonia*, it is unnecessary to consider whether they would also be “discriminatory” under *Register Guard* or under the discrimination standard in effect prior to *Register Guard*. Indeed, discrimination is relevant in Section 8(a)(1) cases only to the extent that it “weakens or exposes as pretextual the employer’s business justification.” *Register Guard*, 351 NLRB 1110, 1129 (2007) (Members Liebman and Walsh, dissenting) (citation omitted), *enforcement denied in part*, 571 F.3d 53 (D.C. 2009).

be disclosed to management, is lawful. Employers generally can monitor employee behavior at work for legitimate and nondiscriminatory business reasons.³¹ The Board has long held that management officials may observe public union activity without violating the Act so long as those officials do not “do something out of the ordinary.”³² Thus, an employer’s monitoring of electronic communications on its e-mail system will similarly be lawful so long as the employer does nothing out of the ordinary, such as increasing its monitoring during an organizational campaign or focusing its monitoring efforts on protected conduct or union activists.³³ And the Board has explicitly noted that an employer ordinarily may notify its employees that it monitors (or reserves the right to monitor) computer and e-mail use for legitimate management reasons and that “employees may have no expectation of privacy in their use of the employer’s email system.”³⁴

Here the Employer’s policy states that its monitoring will be “for business purposes” and to guard against “abnormal or inappropriate usage.” Moreover, there is no evidence that the Employer has done “something out of the ordinary” by focusing on employee Section 7 activity. Accordingly, this policy does not unlawfully create an impression of surveillance.

Accordingly, the Region should issue complaint, absent settlement, consistent with the foregoing.

/s/
B.J.K.

H:ADV.28-CA-176473.Response.cascade. (b) (6), (b) (7)

³¹ See *Caterpillar, Inc.*, 322 NLRB 674, 683–84 (1996) (holding supervisory monitoring to ensure that employees are doing the work for which they are paid is not unlawful simply because employees choose to conduct union activity in the sight of the supervisor). See also *Wal-Mart Stores*, 350 NLRB 879, 883 (2007) (finding no impression of surveillance where employees conducted union activity on shop floor that manager was overseeing).

³² *Eddyleon Chocolate Co.*, 301 NLRB 887, 888 (1991) (quoting *Metal Industries*, 251 NLRB 1523 (1980)). See *Purple Communications, Inc.*, 361 NLRB No. 126, slip op. at 16 (those who choose openly to engage in union activities at or near the employer’s premises cannot be heard to complain when management observes them).

³³ *Purple Communications, Inc.*, 361 NLRB No. 126, slip op. at 16.

³⁴ *Id.*