

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

DATE: October 8, 2015

TO: Margaret Diaz, Regional Director  
Region 12

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

SUBJECT: Space Coast Credit Union  
Case 12-CA-141201

512-5012-0100-0000  
512-5012-0125-0000  
512-5012-0133-5000  
512-5012-3322-0000

The Region submitted this case for advice as to whether certain provisions in the Employer's policies and guidelines are unlawfully overbroad in violation of Section 8(a)(1). We conclude that the following provisions in the Employer's "Fraud, Bribery, Confidentiality and Code of Conduct Policies" are unlawfully overbroad: the rule prohibiting the unauthorized use of computer time or equipment; the rule prohibiting the personal use or disclosure of confidential or proprietary information learned or acquired in the course of employees' work; and the rule prohibiting the commission of acts discreditable to the Employer, fellow employees, or employees themselves. We conclude that the following provisions in the Employer's "End User Guidelines" are also unlawfully overbroad: the rule prohibiting the unauthorized use of the Employer's software; the rule prohibiting the sending of confidential, offensive, defamatory, or other inappropriate communications; the rule prohibiting the use of the internet for purposes that are harmful to the Employer;<sup>1</sup> the rule prohibiting the sending or forwarding of emails containing instructions to forward the message to others; and the rule prohibiting the transmission of any content that is offensive. However, we conclude that the Employer's rule prohibiting the posting of spam messages to large numbers of Usenet newsgroups is not unlawful. Finally, we conclude that this case presents a good vehicle to urge the Board to extend its recent decision in *Purple Communications, Inc.*,<sup>2</sup> which involved the use of an employer's email system, in order to find that the Employer's blanket prohibitions on employees'

---

<sup>1</sup> The Region did not request advice on whether this rule is unlawful. However, this rule was grouped with other provisions that the Region submitted for advice.

<sup>2</sup> 361 NLRB No. 126 (Dec. 11, 2014).

use of the Employer's internet to access personal email and to engage in instant messaging are unlawfully overbroad.

### **FACTS**

The Employer, Space Coast Credit Union, operates a federal credit union and provides other banking and financial services at approximately 60 locations throughout Florida. The Employer's total workforce includes roughly 500 employees, none of whom are currently represented by a labor organization. The Charging Party was employed as a (b) (6), (b) (7)(C) until (b) (6), (b) (7)(C) termination in (b) (6), (b) (7)(C) 2014.<sup>3</sup> The "End User Guidelines" document distributed to employees, which will be discussed further below, specifies that "Internet Access is provided to all employees of the Credit Union for use in their position or for access to web based employee services." The document specifies that systems such as "Internet Service" and "WWW browsing" are to be used primarily for business purposes. Enumerated examples of "acceptable use[s]" for employees who utilize the Employer's internet for work-related purposes include: accessing "commercial, regulatory or governmental Web Sites," accessing "search database and engines via the Internet for information as needed to support the business of the [Credit Union]," using the internet "to support or promote Internet Banking," and using the internet "to access information systems of Credit Union Service providers." The Employer's written policies indicate that the computer network is protected by a firewall, anti-virus software, and other internet security precautions.

The Employer maintains a number of policies and guidelines that are distributed to employees during new employee orientations and periodically by email, and which are accessible via the Employer's intranet system. In particular, the Employer maintains documents labeled "Fraud, Bribery, Confidentiality and Code of Conduct Policies" and "End User Guidelines." These policies and guidelines contain the following provisions at issue in the present case:

---

<sup>3</sup> The Employer discharged the Charging Party for violating its social media policy. In Case 12-CA-136505, the Charging Party alleged that the Employer had violated Section 8(a)(1) by terminating (b) (6), (b) (7)(C). The Region found no merit to the discharge allegation based on its conclusion that the Charging Party was not engaged in protected concerted activity. However, the Region determined in that case that the Employer's social media policy is unlawfully overbroad and violates Section 8(a)(1).

**FRAUD, BRIBERY, CONFIDENTIALITY AND  
CODE OF CONDUCT POLICIES**

**Fraud Policy**

Space Coast Credit Union considers any form of fraud or dishonesty on the part of its employees as totally unacceptable conduct. Acts, which are considered to be either fraudulent or dishonest, include, but are not limited to:

\* \* \*

9. Unauthorized use of computer time or equipment and software piracy.

\* \* \*

**Employee Agreement Regarding Confidentiality and Code of Conduct**

As an employee of Space Coast Credit Union, I will:

\* \* \*

5. Maintain the confidentiality of proprietary information learned or acquired in the course of my work, except when authorized or otherwise legally obligated to disclose such information. Confidential or proprietary information learned or acquired in the course of my work will not be used for my personal advantage or disclosed to any person or firm except as required in the performance of my duties with the Company or after termination of my employment with the Company, unless such information is in the public domain other than through my wrongful disclosure.

\* \* \*

8. Refrain from committing acts discreditable to the Company, my fellow employees, or myself.

\* \* \*

**END USER GUIDELINES**

The procedures and guidelines contained within this End User Guideline have been established to protect confidential member information, Credit Union's computer resources and information assets. The guidelines outlined in the following pages are

intended to reduce the Credit Union's risk due to loss of vital data, member privacy, monetary loss, and to ensure legal and regulatory compliance. . . .

**I. Microcomputers – Responsibilities of All Personnel**

\* \* \*

9. Unauthorized copying or use of Credit Union software and data files is strictly prohibited.

\* \* \*

**IV. Electronic Mail and Electronic Monitoring**

\* \* \*

Confidential, foul, offensive, defamatory, pornographic or other inappropriate communication is strictly prohibited via electronic mail (or any other means). . . .

\* \* \*

**V. Internet Usage**

\* \* \*

**Unacceptable use**

Employees must not use the Internet for purposes that are illegal, unethical, and harmful to the Credit Union. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable uses. Examples of unacceptable use are:

- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.

\* \* \*

- Transmitting any content that is offensive, harassing, or fraudulent.
- Using the Credit Unions Internet Service to access personal email accounts to send or receive email communications using any other type of email service other than the SCCU owned and managed Email systems.

- Using the Credit Unions Internet Service for instant messenger communications.

\* \* \*

- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

### ACTION

We conclude that the following provisions in the Employer’s “Fraud, Bribery, Confidentiality and Code of Conduct Policies” are unlawfully overbroad: the rule prohibiting the unauthorized use of computer time or equipment; the rule prohibiting the personal use or disclosure of confidential or proprietary information learned or acquired in the course of employees’ work; and the rule prohibiting the commission of acts discreditable to the Employer, fellow employees, or employees themselves. We conclude that the following provisions in the Employer’s “End User Guidelines” are also unlawfully overbroad: the rule prohibiting the unauthorized use of the Employer’s software; the rule prohibiting the sending of confidential, offensive, defamatory, or other inappropriate communications; the rule prohibiting the use of the internet for purposes that are harmful to the Employer; the rule prohibiting the sending or forwarding of emails containing instructions to forward the message to others; and the rule prohibiting the transmission of any content that is offensive. However, we conclude that the Employer’s rule prohibiting the posting of spam messages to large numbers of Usenet newsgroups is not unlawful. Finally, by extension of the Board’s holding in *Purple Communications*, we conclude that the Employer’s blanket prohibitions on employees’ use of the Employer’s internet to access personal email or to engage in instant messenger communications are unlawfully overbroad.

The mere maintenance of a rule that would “reasonably tend to chill employees in the exercise of their Section 7 rights” constitutes a violation of Section 8(a)(1).<sup>4</sup> The unlawful effect of such a rule is “to inhibit employees who are considering engaging in legally protected activities by convincing them to refrain from doing so rather than risk discipline.”<sup>5</sup> The Board has developed a two-step inquiry to determine whether

---

<sup>4</sup> *Lafayette Park Hotel*, 326 NLRB 824, 825 (1998), *enforced mem.*, 203 F.3d 52 (D.C. Cir. 1999).

<sup>5</sup> *Continental Group, Inc.*, 357 NLRB No. 39, slip op. at 3 (Aug. 11, 2011).

an employer rule or policy would have such an effect.<sup>6</sup> First, a rule is unlawful if it explicitly restricts activity protected by Section 7. If it does not, a rule is nonetheless unlawful 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.<sup>7</sup> In the present case, there is no evidence that the Employer's policies and guidelines were promulgated in response to union activity, or applied to restrict the exercise of Section 7 rights. As a result, we proceed with an analysis of whether employees would reasonably construe the language of the Employer's policies and guidelines as restricting Section 7 activities.

A. Unlawful Provisions in the Employer's Fraud, Bribery, Confidentiality and Code of Conduct Policies.

First, we conclude that provision number nine in the Employer's Fraud Policy, which classifies the "[u]nauthorized use of computer time or equipment" as unacceptable conduct and a form of fraud or dishonesty, is unlawfully overbroad. As the Board recently held in *Purple Communications*, employees who already have been granted access to their employer's email system in the course of their work enjoy a presumptive right to use their employer's email system for Section 7-protected communications during nonworking time.<sup>8</sup> It necessarily follows that employees have a right to use their employer's "computer time [and] equipment" to engage in protected email communications. Here, where the Employer has granted its employees access to its computers and email system in the regular course of their work, a reasonable employee would interpret the rule in question as constituting a total ban on his or her right to engage in Section 7-protected email communications during nonworking time without prior authorization, in violation of Section 8(a)(1).

Second, we conclude that provision number five in the Employee Agreement Regarding Confidentiality and Code of Conduct is unlawfully overbroad, insofar as it applies to "[c]onfidential or proprietary information learned or acquired in the course of my work," and prohibits the use of such information for "personal advantage" or the disclosure of such information "to any person or firm except as required in the performance of my duties with the Company." The rule fails to make clear that "confidential or proprietary information" does not refer to employee-related information. Absent additional language clarifying what information is covered by the

---

<sup>6</sup> *Lutheran Heritage Village-Livonia*, 343 NLRB 646, 646-47 (2004).

<sup>7</sup> *Id.* at 647.

<sup>8</sup> 361 NLRB No. 126, slip op. at 1, 14. The Employer does not contest the applicability of the Board's holding to the present workplace.

rule, a reasonable employee would read the provision as including any information that was “learned or acquired in the course of [the employee’s] work” and that is not already “in the public domain.”<sup>9</sup> Thus, a reasonable employee would interpret the rule as prohibiting the use or disclosure of information regarding terms and conditions of employment, and other information that is non-public and acquired in the course of employment, but which is often central to the concerted activities protected by Section 7.<sup>10</sup> To the extent that the rule is ambiguous as to what constitutes confidential or proprietary information, any ambiguity must be construed against the Employer as the promulgator of the rule.<sup>11</sup>

---

<sup>9</sup> Employees are entitled to use information and knowledge that comes to their attention in the normal course of work activity and association for Section 7 purposes. *Compare Ridgely Mfg. Co.*, 207 NLRB 193, 196-97 (1973) (finding employee engaged in protected activity where, for organizing purposes, he memorized the names of coworkers from timecards located near the time clock), *enforced*, 510 F.2d 185 (D.C. Cir. 1975), and *MCPc, Inc.*, 360 NLRB No. 39, slip op. at 1, 5-6 (Feb. 6, 2014) (finding employee’s discussion of newly hired manager’s \$400,000 salary to be protected where complaint about high executive compensation was based on a “combination of employee rumors and an estimate derived from internet research,” rather than the unauthorized access of the employer’s computer files), *with First Data Resources, Inc.*, 241 NLRB 713, 719 (1979) (finding employee engaged in unprotected activity when she opened and read a personnel file the employer had instructed her not to look at while copying personnel files from a filing cabinet as part of her job).

<sup>10</sup> *See Rio All-Suites Hotel & Casino*, 362 NLRB No. 190, slip op. at 2 (Aug. 27, 2015) (rule prohibiting employees from sharing “any information about the Company which has not been shared by the Company with the general public” found “extraordinarily broad in scope” and thus unlawful, since even “[w]ithout more” the initial rule implicated terms and conditions of employment); *Boch Honda*, 362 NLRB No. 83, slip op. at 1 n.4, 10 (April 30, 2015) (rule prohibiting disclosure of “confidential and proprietary information,” which defined that phrase to include information about prospective customers and suppliers and company policies, procedures, and litigation activity, found unlawfully overbroad); *cf. HTH Corp.*, 356 NLRB No. 182, slip op. at 2, 25 (June 14, 2011) (rule issued during union boycott requiring employees to maintain “confidentiality” of “[a]ny information acquired by myself during the performance of my duties pursuant to my employment” found unlawfully overbroad, since it would be construed as prohibiting the discussion of wages, hours, or terms and conditions of employment with other employees or with outside individuals such as union representatives), *enforced*, 693 F.3d 1051 (9th Cir. 2012).

<sup>11</sup> *See, e.g., Lily Transportation Corp.*, 362 NLRB No. 54, slip op. at 1 n.3 (Mar. 30, 2015). The Board has construed similarly vague confidentiality requirements against

Third, we conclude that provision number eight in the Employee Agreement Regarding Confidentiality and Code of Conduct, which requires employees to “[r]efrain from committing acts discreditable to the Company, my fellow employees, or myself” is unlawfully overbroad. As written, the provision in question does not provide any further context instructing employees as to what constitutes a “discreditable” act, and thus a reasonable employee would read the broad rule as applying to Section 7-protected conduct.<sup>12</sup> Employees have a Section 7 right to publicly engage in concerted acts protesting their employer and working conditions, and such acts would have little impact if they were not to some extent “discreditable” to an employer’s image.<sup>13</sup> The Board has thus found broad prohibitions of similar employee conduct to be unlawful.<sup>14</sup> For these reasons, we conclude that the Employer’s rule in the present case is also unlawful.<sup>15</sup>

---

the employer to find them unlawful. *E.g.*, *Trinity Protection Services, Inc.*, 357 NLRB No. 117, slip op. at 1-2 & n.5 (Nov. 30, 2011) (analogizing to rules cases and finding employer’s oral statement that employees were not to divulge “any company knowledge to any client” violated Section 8(a)(1) because employees would reasonably conclude that disclosing wages, hours, or working conditions was thereby prohibited).

<sup>12</sup> See *Sheraton Anchorage*, 362 NLRB No. 123, slip op. 1 n.4 (June 18, 2015) (finding that employees would reasonably fear that employer prohibitions on “conflict[s] of interest” and “behavior that violates common decency or morality or publicly embarrasses the hotel” apply to “any conduct the Respondent may consider to be detrimental to its image or reputation or to present a ‘conflict’ with its interests, such as informational picketing, strikes, or other economic pressure”).

<sup>13</sup> Of course, there are also limits to these rights. See *Linn v. Plant Guard Workers Local 114*, 383 U.S. 53, 61-63 (1966) (defamatory statements unprotected if they were circulated with malice and caused employer damages); *NLRB v. Electrical Workers Local 1229 (Jefferson Standard)*, 346 U.S. 464, 476-78 (1953) (disloyal disparagement of employer’s product unprotected).

<sup>14</sup> *First Transit, Inc.*, 360 NLRB No. 72, slip op. at 2 n.5, 12 (Apr. 2, 2014) (rules prohibiting “outside activities that are detrimental to the company’s image or reputation” and “conduct [that] would be detrimental to the interest or reputation of the Company” found unlawfully overbroad because their wording would not lead employees to understand the rules were limited to unprotected misconduct); *Hills & Dales General Hospital*, 360 NLRB No. 70, slip op. at 2 (Apr. 1, 2014) (requirement that employees “represent [the employer] in the community in a positive and professional manner” found unlawfully overbroad); see also *Sears Holding Corp.*, Case 18-CA-117684, Advice Memorandum dated May 23, 2014, at 4-5 (rule requiring employees to “never engage in behavior that would undermine the reputation of [the

B. Unlawful Provisions in the Employer's End User Guidelines.

Employees would reasonably construe provisions in the Employer's microcomputer usage policy, electronic mail and monitoring policy, internet usage policy, and specific provisions banning use of personal email accounts and instant messaging to prohibit Section 7 activity.

---

employer], your peers or yourself" found unlawfully overbroad); *NRG Energy*, Case 05-CA-111283, Advice Memorandum dated March 26, 2014, at 7-8 (rules prohibiting behavior that would "discredit the Company in its relations with the community it serves" and any action that would "cause damage to the Company's business or reputation" found unlawfully overbroad).

<sup>15</sup> In reaching our conclusion that the present rule is unlawful, we are mindful of older Board decisions finding broadly similar rules to be lawful. *Cf. Albertson's, Inc.*, 351 NLRB 254, 258-59 (2007) (rule against conduct that "could have a negative effect on the Company's reputation or operations"); *Ark Las Vegas Restaurant Corp.*, 335 NLRB 1284, 1284 n.2 (2001) (rules against conduct "with the potential of damaging the reputation or a department of the Company" and conduct "that tends to bring discredit to, or reflects adversely on" the employer), *enforced in part*, 334 F.3d 99 (D.C. Cir. 2003); *Lafayette Park Hotel*, 326 NLRB at 825-27 (rule against conduct affecting "the hotel's reputation or good will in the community"). We note that under *Lutheran Heritage Village-Livonia*, 343 NLRB at 646-47, reasonable employees might interpret particular language differently given the surrounding context and workplace at issue. The Board has subsequently distinguished these cases by finding that in each one the lawful provisions were part of a broader context that employees would have understood as referring solely to "uncooperative, improper, unlawful or otherwise unprotected employee misconduct." *First Transit, Inc.*, 360 NLRB No. 72, slip op. at 2 n.5. We also find it noteworthy, though not controlling, that unlike in each of the above cases, here the Employer's workforce is not represented by a labor organization. *Cf. Ark Las Vegas Restaurant Corp.*, 335 NLRB at 1291 (ALJ, affirmed by Board, finding "discredit" language lawful despite its ambiguity, largely because employees were "guided by knowledgeable union officials . . . well aware of the [statutory] limits of protected conduct"). Because there is neither an explanatory context limiting the rule to unprotected conduct nor a unionized workplace, we find the older cases cited above factually distinguishable and the policy provisions at issue inapposite.

1. Microcomputer Usage.

We conclude that provision number nine in the Employer’s microcomputer usage guidelines, which prohibits the “[u]nauthorized . . . use of Credit Union software . . .,” is unlawfully overbroad.<sup>16</sup> Like provision number nine in the Employer’s fraud policy, which broadly prohibits the unauthorized use of “computer time or equipment,” we first note that the prohibition on the unauthorized use of “Credit Union software” is arguably unlawful under *Purple Communications*.<sup>17</sup> The Employer has granted its employees access to its email system in the course of their work, and employees are typically only able to access employer-provided email through software owned or licensed by their employer. Thus, a blanket prohibition on the unauthorized use of any “Credit Union software” could reasonably be construed as prohibiting use of the Employer’s email on nonworking time for Section 7 purposes.<sup>18</sup>

In any event, the “Credit Union software” rule is unlawfully overbroad under an appropriate expanded application of the Board’s reasoning in *Purple Communications*. Employees would reasonably construe the rule as prohibiting the use of all employer-owned software applications—which are already provided to employees in the course of their work—for Section 7 purposes on nonworking time. Employees could reasonably utilize a web browser,<sup>19</sup> word-processing software, image-editing software, or other software applications to facilitate or enhance Section 7-related communications, and thus a broad prohibition on the unauthorized use of

---

<sup>16</sup> We agree with the Region that this rule’s prohibition on the unauthorized use of “data files” is not unlawful because employees would construe that phrase to refer to customer account records. *See Lafayette Park Hotel*, 326 NLRB at 826 (finding rule prohibiting disclosure of “Hotel-private information” lawful because employees would construe it as limited to guest information and similar data). Thus, the following analysis is limited to the prohibition on the unauthorized use of the Employer’s software.

<sup>17</sup> 361 NLRB No. 126, slip op. at 1, 14.

<sup>18</sup> *Cf. TU Electric*, Case 16-CA-19810, Advice Memorandum dated October 18, 1999, at 7-8 (rule stating that “computer software may be used only for Company business” found unlawful where it was discriminatorily used to restrict Section 7-related solicitation and distribution via email).

<sup>19</sup> We conclude further below that employees should have a presumptive right to use their employer’s internet to access personal email or engage in instant messaging for Section 7-related purposes on nonworking time—activities which naturally require the use of “Credit Union software,” if only just a web browser.

any and all employer-provided software would interfere with the exercise of employees' Section 7 rights. Although employers may have an ownership interest in the work-related software provided to employees, the Board has questioned the continued validity of the general proposition that "employees have no right to use, for Section 7 purposes, employer equipment that they regularly use in their work," and explicitly has rejected such a proposition in the context of modern technologies like an employer-provided email system.<sup>20</sup> Computer software is firmly in this category, given the lack of physical limitations on its use, and given that employees' Section 7-related use of computer software would present employers with essentially no additional costs. As a result, we conclude that the rule in question is unlawfully overbroad.

## 2. Electronic Mail and Monitoring Policy.

We conclude that the provision in the Employer's electronic mail and monitoring policy stating that "[c]onfidential, . . . offensive, defamatory, . . . or other inappropriate communication is strictly prohibited via electronic mail (or any other means)" is unlawfully overbroad. The Board has found vague terms such as "offensive,"<sup>21</sup> "defamatory,"<sup>22</sup> and "inappropriate"<sup>23</sup> to constitute unlawfully

---

<sup>20</sup> *Purple Communications, Inc.*, 361 NLRB No. 126, slip op. at 10-11.

<sup>21</sup> *UPMC*, 362 NLRB No. 191, slip op. at 1 & n.5, 21-22 (Aug. 27, 2015) (rule prohibiting use of email in a way that may be "offensive" found unlawfully overbroad); *NCR Corp.*, 313 NLRB 574, 577 (1993) (rule prohibiting bulletin board postings containing "offensive language" found unlawfully overbroad, since employees would reasonably interpret that phrase as applying to union literature); *see also KMOV-TV*, Case 14-CA-107342, Advice Memorandum dated January 6, 2014, at 6 (rule against the use of "offensive, derogatory, or prejudicial comments" found unlawfully overbroad).

<sup>22</sup> *Quicken Loans, Inc.*, 359 NLRB No. 141, slip op. at 1 n.3, 5 (June 21, 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); (b) (7)(A)

(b) (7)(A)

(b) (7)(A); *see also 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*, 383 U.S. at 61 (false statements remain protected under Section 7 unless they are malicious)

overbroad restrictions on employees' Section 7 rights. Likewise, in light of the confidentiality provision we have already found unlawfully overbroad above, reasonable employees would interpret this additional prohibition on "confidential" communication, with no additional context, as encompassing Section 7-protected messages. Although the Employer's rule includes these terms in a list alongside clearly unprotected types of communication, such as those that are "pornographic," the disparate nature of the terms listed would not provide sufficient context to a reasonable employee so as to resolve the meaning of the ambiguous terms.<sup>24</sup> Reasonable employees would read these rules to include communications that are statutorily protected, such as emails with non-public information concerning working conditions, and emails about unionization that the Employer or anti-union coworkers might subjectively regard as offensive, defamatory, or inappropriate. Furthermore, the Employer's rule prohibits such communications not only by email, but also by "any other means," which constitutes an additional overbroad prohibition that is reasonably likely to chill employees in the exercise of their rights.

---

<sup>23</sup> *Triple Play Sports Bar & Grille*, 361 NLRB No. 31, slip op. at 7 (Aug. 22, 2014) (rule prohibiting the use of the internet to engage in "inappropriate discussions" found unlawfully overbroad); *First Transit, Inc.*, 360 NLRB No. 72, slip op. at 3 (rule prohibiting "[d]iscourteous or inappropriate attitude or behavior to passengers, other employees, or members of the public" found unlawfully overbroad, due to "patent ambiguity" of the language).

<sup>24</sup> For example, "confidential," "defamatory," and "pornographic" refer to entirely unrelated forms of communication, and thus the inclusion of "pornographic" does not resolve the meaning of the terms we find unlawful. *E.g.*, (b) (7)(A)

(b) (7)(A)

(b) (7)(A); see also *Southern Maryland Hospital Center*, 293 NLRB (rule prohibiting "derogatory attacks" found unlawful despite being combined with lawful rule prohibiting "malicious gossip," because employees would still read unlawful portion as applying to protected statements), *enforced in relevant part*, 916 F.2d 932 (4th Cir. 1990).

### 3. Internet Usage.<sup>25</sup>

First, we conclude that the provision in the Employer’s internet usage policy warning employees that they “must not use the Internet for purposes that are . . . harmful to the Credit Union” is unlawfully overbroad.<sup>26</sup> Like the rule prohibiting acts “discreditable” to the Employer, discussed above, the ambiguity of the broad “harmful to the Credit Union” language would lead a reasonable employee to interpret this language as encompassing certain Section 7-protected activities that the Employer might consider “harmful” to its interests—for example, using email communications to help organize a union or inform employees of a pending strike.<sup>27</sup> Although the sentence in question also prohibits the use of the internet for purposes that are “illegal” or “unethical,” these contextual cues do not negate the ambiguity of the later phrase “harmful to the Credit Union,” particularly since many of the ensuing examples of prohibited internet usage (some of which we find to implicate protected activities) are neither illegal nor unethical.<sup>28</sup>

Second, we conclude that the unacceptable-use example prohibiting employees from “[s]ending or forwarding chain email, i.e., messages containing instructions to

---

<sup>25</sup> Although we conclude further below that the Board should extend *Purple Communications* to additional forms of employee communications over the internet, such as browser-based personal email or instant messaging, we note that the Employer’s “Internet Usage” and “Unacceptable use” subsections specifically refer, at least in part, to traditional employer-provided email communications. As such, it is unnecessary to expand the Board’s existing *Purple Communications* decision in order to find the rules discussed in this subsection of the memorandum unlawful.

<sup>26</sup> As noted above, we address the legality of this rule even though the Region did not request advice on whether this provision is unlawfully overbroad.

<sup>27</sup> Cf. *First Transit, Inc.*, 360 NLRB No. 72, slip op. at 2 n.5 (rule prohibiting “conduct [that] would be detrimental to the interest or reputation of the Company” found unlawfully overbroad where wording of rule would not lead employees to understand it was limited to unprotected conduct); see also *Sheraton Anchorage*, 362 NLRB No. 123, slip op. 1 n.4; *TeleTech Holdings, Inc.*, Cases 19-CA-33026 et al., Advice Memorandum dated June 13, 2012, at 8 (rule prohibiting any conduct “not in the best interest of [the employer]” found unlawfully overbroad).

<sup>28</sup> For the same reasons, our conclusion is not diminished by the provision’s use of the word “and” rather than the conjunctive “or.” To the extent the rule is ambiguous, “any ambiguity in the rule must be construed against the [Employer] as the promulgator of the rule.” *Lafayette Park Hotel*, 326 NLRB at 828.

forward the message to others,” is unlawfully overbroad. As noted, employees who already have been granted access to their employer’s email system in the course of their work have a presumptive Section 7 right to use their employer’s email system on nonworking time for protected communications.<sup>29</sup> Especially in the context of the present Employer, which operates nearly 60 locations throughout the state of Florida, it is reasonable to infer that protected employee communications might involve instructions to forward Section 7-related emails across and between individuals or different groups of employees. Particularly given the definition the Employer sets forth in the rule, we do not find the phrase “chain email” specific enough that a reasonable employee would interpret the rule as permitting protected communications involving the forwarding of emails.<sup>30</sup>

Third, we conclude that the unacceptable-use example prohibiting the transmission of “any content that is offensive” is unlawfully overbroad.<sup>31</sup> Like the provision in the Employer’s email usage guidelines discussed above, the prohibition on “offensive”<sup>32</sup> content is vague and a reasonable employee would interpret it as applying to Section 7-protected messages. Union organizing campaigns, and other protected activities, often involve content and messages that the Employer or certain

---

<sup>29</sup> *Purple Communications, Inc.*, 361 NLRB No. 126, slip op. at 1, 14.

<sup>30</sup> We also note that normal back-and-forth discussions via email between two individuals are often referred to as “email chains,” which would heighten the ambiguity of the existing rule from the perspective of a reasonable, but perhaps not technologically-savvy, employee.

<sup>31</sup> However, the Region should not allege that the prohibition on “fraudulent” transmissions violates Section 8(a)(1). Such a transmission would involve a knowing misrepresentation or concealment and is analogous to an unprotected malicious falsehood. We also conclude that the prohibition on “harassing” transmissions is not unlawful in the present case, because reasonable employees would interpret it in the context of the Employer’s overarching “Harassment Policy,” which prohibits sexual harassment and other forms of clearly unprotected conduct. *See Lutheran Heritage Village-Livonia*, 343 NLRB at 646 & n.3, 648 (finding rule prohibiting “harassment” to be lawful; rule was considered alongside rules prohibiting “abusive and profane language” and “verbal, mental and physical abuse”).

<sup>32</sup> *See UPMC*, 362 NLRB No. 191, slip op. at 1 & n.5, 21-22 (rule prohibiting use of email in a way that may be “offensive” found unlawfully overbroad); *see also KMOV-TV*, Case 14-CA-107342, Advice Memorandum dated January 6, 2014, at 6 (rule against the use of “offensive, derogatory, or prejudicial comments” found unlawfully overbroad).

coworkers could subjectively label “offensive.” As such, absent further clarifying language in the Employer’s guidelines, a reasonable employee would be unable to anticipate whether Section 7-protected messages would violate the Employer’s rule, and this would reasonably chill that employee in the exercise of his or her rights, in violation of the Act.

Finally, however, we conclude that the unacceptable-use example prohibiting employees from “[p]osting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam)” is not unlawful. Usenet, a relatively antiquated global discussion network, facilitates the exchange of messages posted to different discussion groups, or “newsgroups.” The provision in the Employer’s guidelines would reasonably be interpreted as referring to a specific practice of sending “spam” messages to external users across “large numbers” of different Usenet newsgroups, and thus the Employer’s policy would not reasonably be read to prohibit Section 7-related communications between coworkers or other individuals. Since there is no evidence of an internal Employer-specific network that a reasonable employee might misinterpret “Usenet newsgroups” as referring to, we find the unacceptable-use example in question to be permissible.

4. The Rationale in *Purple Communications* Should be Extended to Find that the Employer’s Policies on Personal Email and Instant Messaging are Unlawful.

With respect to the remaining two unacceptable-use examples in the Employer’s internet usage guidelines, concerning employee use of the Employer’s internet to access personal email or to engage in instant messenger communications, we conclude that this case presents a good vehicle to urge the Board to extend its holding in *Purple Communications* by applying it to these forms of electronic communications as well. After outlining the appropriate framework regarding access to employer-provided email in *Purple Communications*, the Board noted that “[o]ther interactive electronic communications, like instant messaging and texting, may ultimately be subject to a similar analysis.”<sup>33</sup> On that basis, the General Counsel recently has alleged that an employer’s total ban on the use of its “Internet and Intranet systems” for non-business purposes was unlawfully overbroad.<sup>34</sup> This case presents the more targeted question

---

<sup>33</sup> 361 NLRB No. 126, slip op. at 14 & n.70.

<sup>34</sup> (b) (7)(A)  
(b) (7)(A)

see also (b) (7)(A)  
(b) (7)(A)

of whether an employer, which already provides its employees broad access to the internet for work-related purposes, may specifically ban access to personal email and instant messaging. We conclude that an employer presumptively may not, and that the Employer's rules in the present case are unlawfully overbroad.

Like employer-provided email, personal email and instant messaging have become important means of communication for individuals in the twenty-first century.<sup>35</sup> At the same time, the workplace is uniquely well suited for the discussion of Section 7-related matters.<sup>36</sup> In keeping with the Board's analysis in *Purple Communications*, we find that the ability to use employer-provided internet to access personal email or engage in instant messaging in the workplace, during nonworking time, is an important mechanism for employees to "effectively communicate with one another at work regarding self-organization and other terms and conditions of employment."<sup>37</sup> Many employees may feel more comfortable engaging in Section 7-related communications via personal email or via instant messenger communications, as opposed to an employer-provided email account that employees use for work purposes.

We thus conclude that the Board should extend the framework established in *Purple Communications* to create a presumptive right for employees—who already have been granted access to their employer's internet in the course of their work—to use their employer's internet to access personal email and to engage in instant messaging on nonworking time.<sup>38</sup> While we recognize the potential for added internet

---

<sup>35</sup> See *Purple Communications, Inc.*, 361 NLRB No. 126, slip op. at 40-42 (Member Johnson, dissenting) (discussing the prevalence of personal email and social media); see also (b) (7)(A)

<sup>36</sup> See *Purple Communications, Inc.*, 361 NLRB No. 126, slip op. at 5-6, 13-14 & n.62; cf. *Republic Aviation Corp. v. NLRB*, 324 U.S. 793, 799 (1945) (affirming employees' right to engage in solicitation on company property on nonworking time, despite fact that employers' plants were not physically isolated such that offsite solicitation would have been ineffective).

<sup>37</sup> *Purple Communications, Inc.*, 361 NLRB No. 126, slip op. at 1.

<sup>38</sup> Given that some forms of "instant messenger communications" may require a separate software application, we stress that the present memorandum does not address the ability of employers to prohibit employees from independently downloading and installing software applications.

bandwidth and security costs associated with personal email usage and instant messaging, we note that the Board's *Purple Communication* framework allows for employers to demonstrate "special circumstances" that would outweigh employees' presumptive right to use those methods of communication for Section 7 purposes, such as costs or security concerns.<sup>39</sup> In the present case, the Employer already grants its employees broad access to the internet for work-related purposes, including visiting websites, accessing search engines, and performing other web browsing. The Employer already maintains a firewall, anti-virus software, and other internet security precautions. As a result, in the absence of concrete evidence that the Employer in the present case would face increased security risks or other harms that might constitute "special circumstances" justifying a total ban on personal email usage and instant messenger communications,<sup>40</sup> we conclude that the two unacceptable-use examples in question are both unlawfully overbroad.<sup>41</sup>

---

<sup>39</sup> 361 NLRB No. 126, slip op. at 9 n.36, 14 & n.66.

<sup>40</sup> In the event that the Employer comes forward with evidence indicating the presence of "special circumstances," the Region should contact the Division of Advice.

<sup>41</sup> Although the Employer operates a federal credit union and thus stores sensitive customer information, we do not find that the nature of the Employer's business makes the present case a poor vehicle for extending *Purple Communications*. First, the Board has already applied its framework to employer-provided email in cases involving employers with sensitive customer and patient data. *See Purple Communications, Inc.*, 361 NLRB No. 126 (employer providing private sign-language interpretation services); *UPMC*, 362 NLRB No. 191 (hospital). Second, the nature of the Employer's business arguably makes this a stronger case, given that the Employer already has security measures in place that are presumably much greater than an average employer. And third, there is no evidence in the record suggesting that employees' personal email usage or instant messaging for Section 7 purposes on nonworking time would actually result in any increased risk to the Employer's customer data, or that the Employer would be unable to mitigate any such risk without resorting to a blanket prohibition on protected uses. The Employer's workforce already utilizes employer-provided email and accesses the internet in the normal course of their work, and thus the Employer already tolerates a certain baseline security risk as part of its normal operations. Furthermore, application of the *Purple Communications* framework to personal email and instant messaging would be limited to Section 7-protected uses only, and not generalized personal use.

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

/s/  
B.J.K.

ADV.12-CA-141201.Response.SpaceCoast. 