UNITED STATES OF AMERICA
BEFORE THE NATIONAL LABOR RELATIONS BOARD
WASHINGTON, D.C.

CAESARS ENTERTAINMENT CORPORATION d/b/a RIO ALL-SUITES HOTEL AND CASINO	)	
and	)	Case No. 28-CA-060841
INERNATIONAL UNION OF PAINTERS AND ALLIED TRADES, DISTRICT COUNCIL 15, LOCAL 159, AFL-CIO	)	

BRIEF *AMICUS CURIAE* OF THE CENTER FOR WORKPLACE COMPLIANCE

Rae T. Vann
Michael J. Eastman
Counsel of Record
NT LAKIS, LLP
1501 M Street, NW
Suite 1000
Washington, DC 20005
meastman@ntlakis.com
(202) 629-5600

Attorneys for *Amicus Curiae*
Center for Workplace Compliance

October 5, 2018

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES

FEDERAL REGULATIONS

OTHER AUTHORITIES

The Center for Workplace Compliance respectfully submits this brief *amicus curiae* in response to the National Labor Relations Board's (NLRB or the Board) Notice and Invitation to File Briefs, dated August 1, 2018. The brief urges the Board to overrule its decision in *Purple Communications, Inc.*, 361 N.L.R.B. 1050 (2014), and return to the standard adopted in *Register Guard,* 351 N.L.R.B. 1110 (2007), *enforced in relevant part and remanded sub nom.*, *Guard Publ'g Co. v. NLRB*, 571 F.3d 53 (D.C. Cir. 2009).

INTEREST OF THE *AMICUS CURIAE*

Founded in 1976, the Center for Workplace Compliance (CWC) (formerly the Equal Employment Advisory Council (EEAC)) is the nation's leading nonprofit association of employers dedicated exclusively to helping its members develop practical and effective programs for ensuring compliance with fair employment and other workplace requirements. Its membership includes more than 240 major U.S. corporations, collectively providing employment to millions of workers. CWC's directors and officers include many of industry's leading experts in the field of equal employment opportunity and workplace compliance. Their combined experience gives CWC a unique depth of understanding of the practical, as well as legal, considerations relevant to the proper interpretation and application of equal employment policies and other workplace compliance requirements.

The vast majority of CWC's member companies are employers subject to the National Labor Relations Act (NLRA), 29 U.S.C. §§ 151 *et seq*., as well as Title VII of the Civil Rights Act of 1964 (Title VII), 42 U.S.C §§ 2000e *et seq.*, and other federal employment nondiscrimination laws. A large majority also are federal government contractors subject to the nondiscrimination and affirmative action requirements of Executive Order 11,246 (EO 11246),

30 Fed. Reg. 12,319 (Sept. 24, 1965), the Vietnam-Era Veterans' Reemployment Adjustment Act (VEVRAA), 38 U.S.C. §§ 4211 *et seq.*, and Section 503 of the Rehabilitation Act of 1973 (Section 503), 29 U.S.C. § 793. As such, CWC's interest in the ability of employers to lawfully restrict non-work-related employee access to corporate email and information technology systems includes, but is much broader than, the potential NLRA issues raised by the Board's questions. Because of its interest in both the application of the nation's fair employment laws, as well as the effective mitigation of enterprise-wide risk, the issues presented in this case are extremely important to the nationwide constituency that CWC represents.

CWC has an interest in, and a familiarity with, the practical issues and policy concerns raised in this case. Indeed, because of its significant experience in these matters, CWC is well-situated to brief this Board on the importance of the issues beyond the immediate concerns of the parties to the case.

STATEMENT OF THE CASE

Caesars Entertainment Corporation (Caesars) employs approximately 3,000 employees at the Rio All-Suites Hotel and Casino in Las Vegas, Nevada. *Caesars Entertainment d/b/a Rio All-Suites Hotel and Casino,* 362 N.L.R.B. No. 190 (2015), at 1. The company maintains an employee handbook that includes numerous rules with which employees are expected to comply. *Id*. Among them is a rule entitled, "Use of Company Systems, Equipment, and Resources" (Computer Resources Rule). *Id.* at 5. In relevant part, the Rule prohibits employees from using computer resources to:

- Share confidential information with the general public, including discussing the company, its financial results or prospects, or the performance or value of company stock by using an internet message

> board to post any message, in whole or in part, or by engaging in an internet or online chatroom;
>
> - Convey or display anything fraudulent, pornographic, abusive, profane, offensive, libelous, or slanderous;
>
> - Send chain letters or other forms of non-business information;
>
> ***
>
> - Solicit for personal gain or advancement of personal views; or
>
> - Violate rules or policies of the Company[.]

Id. at 5 n.13. In addition, the policy states:

> Do not visit inappropriate (non-business) websites, including but not limited to online auctions, day trading, retail/wholesale, chat rooms, message boards and journals. Limit the use of personal email, including streaming media (*e.g.,* video and audio clips) and downloading photos.

Id.

The International Union of Painters and Allied Trades, District Council 15, Local 159, AFL-CIO filed an unfair labor practice charge with the Board, claiming that the Computer Resources Rule and other employer policies not presently at issue unlawfully interfered with employees' rights to engage in protected concerted activity. Thereafter, the Board's General Counsel issued a complaint alleging that Caesars' maintenance of the rule violated 8(a)(1) of the NLRA. Interpreting the provision under then extant law, an Administrative Law Judge (ALJ) found that the General Counsel failed to establish that employees would reasonably construe the rule to prohibit protected activity and recommended dismissal of the relevant portion of the complaint. *Id.* at 12. The Board later remanded in light of its intervening decision in *Purple Communications*, 361 N.L.R.B. 1050 (2014). An ALJ, applying *Purple Communications*, determined that the rule was an overly broad computer use policy that effectively prohibited

employees from using the employer's email system to engage in Section 7 communication during nonworking time, in violation of Section 8(a)(1) of the NLRA. *Caesars Entertainment Corp.*, No. 28-CA-060841 (N.L.R.B. Div. of Judges May 3, 2016), at 1-2.

Caesars filed exceptions to the ALJ's decision with the full Board, which on August 1, 2018 published a Notice and Invitation to File Briefs addressing the following questions:

1. Should the Board adhere to, modify, or overrule *Purple Communications*?

2. If you believe the Board should overrule *Purple Communications*, what standard should the Board adopt in its stead? Should the Board return to the holding of *Register Guard* or adopt some other standard?

3. If the Board were to return to the holding of *Register Guard*, should it carve out exceptions for circumstances that limit employees' ability to communicate with each other through means other than their employer's email system (*e.g.,* a scattered workforce, facilities located in areas that lack broadband access)? If so, should the Board specify such circumstances in advance or leave them to be determined on a case-by-case basis?

4. The policy at issue in this case applies to employees' use of the Respondent's "[c]omputer resources." Until now, the Board has limited its holdings to employer email systems. Should the Board apply a different standard to the use of computer resources other than email? If so, what should that standard be? Or should it apply whatever standard the Board adopts for the use of employer email systems to other types of electronic communications (*e.g.,* instant messages, texts, postings on social media) when made by employees using employer-owned equipment?

SUMMARY OF ARGUMENT

The Board should overrule *Purple Communications*, 361 N.L.R.B. 1050 (2014), and return to the standard articulated in *Register Guard*, 351 N.L.R.B. 1110 (2007), *enforced in relevant part and remanded sub nom.*, *Guard Publ'g Co. v. NLRB*, 571 F.3d 53 (D.C. Cir. 2009), which held that employees do not have a statutory right under the National Labor Relations Act (NLRA), 29 U.S.C. §§ 151 *et seq*., to use an employer's equipment or media for non-work

purposes, so long as the employer's restrictions are applied in a nondiscriminatory manner. In *amicus curiae* CWC's view, *Purple Communications* is deeply flawed.

Longstanding precedent under the NLRA recognizes employer property rights. *See, e.g., Lechmere, Inc. v. NLRB*, 502 U.S. 527 (1992) (holding that an employer can prohibit all solicitation in retail store parking lot); *Union Carbide Corp. v. NLRB*, 714 F.2d 657, 663 (6th Cir. 1983) (observing that an employer "*unquestionably* had the right to regulate and restrict employee use of company property"); *Container Corp. of Am.*, 244 N.L.R.B. 318, 318 n.2 (1979) (noting that "there is no statutory right of employees or a union to use an employer's bulletin board"), *enforced in part, denied in part*, *NLRB v. Container Corp. of Am.*, 649 F.2d 1213 (6th Cir. 1981). These rights must be balanced with employee rights to communicate for Section 7 purposes. While the Board purported to balance these rights in *Purple Communications*, it addressed employer property interests in employer-provided email systems in only the most cursory way.

Among the issues that the Board should have considered when evaluating employer property interests in employer-provided email systems is the very significant risk associated with unfettered employee access to such systems for personal use. In particular, company-provided email systems expose employers to cybersecurity risks and can facilitate harassment and other workplace misconduct.

It is critical that employers actively manage cybersecurity risks to reduce the chance that an outside attack will be successful, and to protect client, customer, and employee data and information. The risk of data breaches and other cybersecurity threats has increased significantly over time.

Employer-provided email systems can also be used to engage in workplace misconduct, including harassment. Employers have a strong interest in developing policies and practices, and in taking proactive efforts, to prevent workplace harassment. *See, e.g., Burlington Industries, Inc. v. Ellerth*, 524 U.S. 742 (1998); *Faragher v. City of Boca Raton*, 524 U.S. 775 (1998). Email provides an easy avenue for employees to disseminate inappropriate comments, cartoons, highly sexualized or derogatory language, jokes, or propositions to large numbers of recipients with little effort. Policies restricting non-work email use are often an important component of an employer's harassment prevention strategy.

The risks posed by email systems are thus dramatically greater than those posed by more traditional forms of employee communication at issue in Board precedent, such as via bulletin boards and landline telephones – which counsels strongly in favor of *greater* employer regulation of company-provided email systems, not less, as called for in *Purple Communications*.

The Board also failed to consider the fact that employer-provided email is not the "natural gathering place" for employees, as claimed by the majority in *Purple Communications*, having been all but supplanted by more sophisticated and effective modes of communication, such as social media and text messaging. For these reasons, *Purple Communications* should be overruled.

The *Register Guard* standard appropriately balances employer property rights with employees' right to communicate for Section 7 purposes, providing employers the flexibility to design email use policies as appropriate to manage different types of cybersecurity and workplace risk, while leaving intact employee rights to communicate on non-work time.

In its Notice and Invitation to File Briefs, the Board also asks whether it should carve out any exceptions for workplaces where employees must use employer-provided email to communicate. In *amicus curiae* CWC's view, this is a question best left for a future case. Neither *Purple Communications*, *Register Guard*, nor this case involve facts suggesting that employees have no means of effective communication other than employer-provided email.

Should the Board return to its holding in *Register Guard*, then *amicus curiae* CWC urges the Board to adopt the same standard to additional forms of employer-provided electronic resources.

ARGUMENT

I. THE BOARD SHOULD OVERRULE *PURPLE COMMUNICATIONS*

The first question posed by the Board in its August 1, 2018, Notice and Invitation to File Briefs is whether the Board should "adhere to, modify, or overrule *Purple Communications*." *Caesars Entertainment Corp. d/b/a/ Rio All-Suites Hotel and Casino*, 28-CA-060841 (Aug. 1, 2018) (NOTICE AND INVITATION TO FILE BRIEFS), at 1. For all of the reasons explained below, *amicus curiae* CWC respectfully submits that *Purple Communications* should be overruled.

A. The NLRA Requires That The Board Balance Section 7 Rights With Employer Property Rights

The National Labor Relations Act (NLRA), 29 U.S.C. §§ 151 *et seq*., makes it unlawful for an employer to interfere with, restrain, or coerce employees in the exercise of their rights to organize, participate in unions, and "engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection." 29 U.S.C. §§ 157, 158(a)(1). These provisions have been interpreted to prohibit employers from adopting and enforcing rules that

unduly restrict the ability of employees to communicate about matters relating to unions and working conditions.

At the same time:

> The NLRA was enacted to improve the capitalist system. Consequently, capitalism's basic assumptions concerning private ownership of property became an implicit part of the statute. As a result, several rights of employers, although not expressly provided for in the Act, have been read as essential ingredients in the statutory scheme.
>
> Chief among these are the employer's property rights. The Supreme Court articulated the statute's foundation of respect for property rights in *NLRB v. Babcock & Wilcox Co*.: "Organization rights are granted to workers by the same authority, the National Government, that preserves property rights. Accommodation between the two must be obtained with as little destruction of one as is consistent with the maintenance of the other."

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, 6 (2000) (footnotes omitted). With that principle in mind, courts have interpreted the NLRA as permitting employers to place reasonable restrictions on workplace communications in order to protect legitimate business interests. The Act does not protect workplace speech or conduct that is genuinely insubordinate, disloyal or unduly disruptive, for instance. *See, e.g., Bob Evans Farms, Inc. v. NLRB*, 163 F.3d 1012, 1024 (7th Cir. 1998) (NLRA "does not protect employees who protest a legitimate grievance by recourse to unduly and disproportionately disruptive or intemperate means").

In addition, recognizing that "[w]orking time is for work," *Peyton Packing Co.*, 49 N.L.R.B. 828, 843 (1943), *enforced*,142 F.2d 1009 (5th Cir. 1944), this Board, the U.S. Supreme Court, and federal courts of appeals long have allowed employers to ban solicitation of employees at their work stations during working time. *See also Republic Aviation Corp. v. NLRB*, 324 U.S. 793 (1945); *Cooper Tire & Rubber Co. v. NLRB*, 957 F.2d 1245, 1250-51 (5th

Cir. 1992). It also is well-established that employers generally may restrict employees' use of company property, such as bulletin boards, telephones, copying and fax machines, to business-related purposes, provided they enforce those restrictions uniformly, without regard to the subject matter of the communications. See, for example, *Mid-Mountain Foods*, 332 N.L.R.B. 229 (2000), *enforced*, 269 F.3d 1075 (D.C. Cir. 2001).

In *Register Guard*, 351 N.L.R.B. 1110 (2007), the Board held that employees do not have a statutory right under the NLRA to use an employer's email for nonwork purposes, so long as the employer's restrictions are applied in a nondiscriminatory manner. In doing so, it relied on a long line of cases addressing property rights in employer-owned equipment, including *Mid-Mountain Foods*, 332 N.L.R.B. 229 (2000) (television in break room), *enforced*, 269 F.3d 1075 (D.C. Cir. 2001); *Eaton Techs.*, 322 N.L.R.B. 848 (1997) (bulletin board); *Champion Int'l Corp.*, 303 N.L.R.B. 102 (1991) (copy machine); *Churchill's Supermarkets*, 285 N.L.R.B. 138 (1987) (telephone system), *enforced*, 857 F.2d 1474 (6th Cir. 1988); and *Union Carbide Corp.*, 259 N.L.R.B. 974 (1981) (telephone system), *enforced in part, set aside in part*, *Union Carbide Corp. v. NLRB*, 714 F.2d 657 (6th Cir. 1983).

The Board rejected that rationale in *Purple Communications*, 361 N.L.R.B. 1050 (2014), concluding that *Register Guard* placed too much emphasis on employer property rights and did not recognize the critical role of email in employee communications. It thus created a presumption that employees who have access to their employer's email system in the course of their work have a right to use that system to engage in Section 7 communications on nonworking time, absent special circumstances.

B. *Purple Communications* Improperly Dismissed Employers' Property Rights Interest In Employer-Provided Email Systems

In *Purple Communications*, the Board majority rejected *Register Guard's* reliance on the Board's equipment cases. Instead, the Board purported to analyze whether property rights, including the employer's right to control its equipment, must give way to competing Section 7 rights. *Purple Communications*, 361 N.L.R.B. at 1060 n.50. In doing so, however, the Board did not undertake any serious examination of the employer property rights at issue. The only aspect of property rights considered by the majority was the extent to which allowing personal use of email would interfere with others or add incremental costs. Finding these impacts to be negligible, the Board distinguished the use of email systems from the Board's other equipment cases. *Id.* at 1057.

Even if the Board's assumption about costs and burden is correct, the Board should have first conducted a thorough examination of the property rights at issue, including the legitimate business reasons that compel employers to adopt policies allowing limited use of their equipment.

C. *Purple Communications* Did Not Properly Consider The Risks Posed By Use Or Misuse Of Employer-Provided Technology, Employers' Interest In Managing That Risk, And Employers' Rights And Responsibilities To Determine How To Manage That Risk

The Board's disregard for employer property rights in *Purple Communications* was at least partially based on the notion that email has "'revolutionized communication [and one cannot reasonably contend] 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.'" *Purple Communications* at 1066 (citing *Register Guard*, 351 N.L.R.B. at 1121 (2007) (Liebman, M.,

dissenting in part)). This notion is correct, but not for the proposition cited by the dissent in *Register Guard* or the majority in *Purple Communications*. The differences between email systems and more traditional types of equipment used for communications instead counsel in favor of according greater weight to employer property interests in email systems, not less.

Employers utilize email systems for a variety of reasons. However, every email system comes with risk that employers have a duty to manage. Examples of risks posed by providing employees with email include the potential that the email system will be a vehicle for the installation of spyware, malware, or viruses that interfere with employer systems; data breaches; disclosure of confidential or sensitive information; and facilitation of harassment or other workplace misconduct. Employers must make decisions on how to manage such risk, as failure to do so can have serious consequences for the employer, its employees, customers and clients, and shareholders.

1. *Purple Communications* failed to consider employers' property rights interest in managing cybersecurity risk

A major, real-world concern that arises as soon as an employer's IT system is connected to the outside world is that of data security. One person opening the wrong outside e-mail, for instance, can unleash a virus that fatally corrupts vital system files, physically overloads a network, and brings the system to a halt, or worse. These types of consequences interfere with the productivity of all employees who are dependent upon the network to do their jobs.

The financial, reputational, and commercial business costs associated with increasingly common data security breaches can be incalculable. Even a declaration that "the network is down" often is extremely disruptive to a business operation. Cybersecurity concerns are

particularly acute among federal contractors that may have access to highly sensitive government data, which if compromised could in some instances have serious national security implications.

The risk to corporate America of data security breaches has grown significantly over the last 20 years. As one commentator observed:

> Around [the year] 2000, academic commentators and practicing risk professionals began to recognize the significant liability risks that the movement towards electronic data storage and Internet business posed to companies and organizations. Over a decade ago, businesses were confronting information theft, insertion of malicious codes, denial of service attacks, access violations, failure of computer security, programming errors, and misuse or misappropriation of intangible assets. In the late 1990s, some estimates put business costs related to computer security breaches in the hundreds of billions of dollars. … Damages as a result of electronic security breaches have not slowed since.

Lance Bonner, *Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches*, 40 Wash. U. J.L. & Pol'y 257, 262 (2012) (footnotes and internal quotations omitted). More recent developments include the proliferation of malware which is frequently delivered through email. Cisco 2018 Annual Cybersecurity Report at 14-21.[1] Malware includes ransomware, which can lock users out of systems until a ransom is paid, or even malicious code simply designed for "obliteration of systems and data." *Id.* at 3. Bulletin board postings, leaflets, or face-to-face communications are not dependent upon access to an employer's information technology systems, and thus do not raise the same level of data security concerns posed by non-work email communications.

[1] *Available at* https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf.

2. *Purple Communications* has impeded equal employment opportunity compliance efforts

By limiting an employer's ability to regulate non-business email, *Purple Communications* increases the opportunity for employees to engage in conduct implicating federal workplace equal employment opportunity (EEO) and nondiscrimination laws. Title VII of the Civil Rights Act of 1964 (Title VII), 42 U.S.C. §§ 2000e *et seq.*, for instance, makes it unlawful for an employer to discriminate "against any individual with respect to his compensation, terms, conditions or privileges of employment because of such individual's race, color, religion, sex or national origin." 42 U.S.C. § 2000e-2(a)(1). In *Meritor Savings Bank, FSB v. Vinson*, the Supreme Court ruled that a "plaintiff may establish a violation of Title VII by proving that discrimination based on sex has created a hostile or abusive work environment." 477 U.S. 57, 66 (1986). *See also Harris v. Forklift Sys., Inc.*, 510 U.S. 17 (1993) (establishing standards for determining when an environment is sufficiently hostile or abusive to be actionable). Accordingly, "many employers today aggressively react to sexual harassment allegations ...." *Brady v. Office of Sergeant at Arms*, 520 F.3d 490, 496 (D.C. Cir. 2008).

In its dual holdings in *Burlington Industries, Inc. v. Ellerth*, 524 U.S. 742 (1998), and *Faragher v. City of Boca Raton*, 524 U.S. 775 (1998), the Supreme Court held that an employer is subject to vicarious liability for unlawful harassment of one employee by another, and in doing so established an affirmative defense to liability tied directly to an employer's diligence in preventing and correcting such behavior. Indeed, an essential element of the defense is that "the employer exercised reasonable care to prevent and correct promptly any sexually harassing behavior ...." *Ellerth*, 524 U.S. at 765, *Faragher*, 524 U.S. at 807.

The Court later described the defense as "a strong inducement [for employers] to ferret out and put a stop to any discriminatory activity in their operations as a way to break the circuit of imputed liability." *Crawford v. Metro. Gov't of Nashville*, 555 U.S. 271, 278 (2009) (citation omitted). In other words, the Court ruled that an employer must make an effort to prevent sexual harassment in the workplace. Where the employer has not been successful at prevention, it needs to act quickly to remedy the situation.

"Many of the behaviors that could give rise to a hostile work environment – propositions, the sharing of pornography, highly sexualized or derogatory language and jokes – can occur as easily via electronic communications as in face-to-face interactions …." Marion Crain & Pauline T. Kim, *A Holistic Approach to Teaching Work Law*, 58 St. Louis U. L.J. 7, 11 (2013) (footnote omitted). Indeed, the same types of comments, cartoons, and the like that can create a racially or sexually hostile working environment when conveyed in verbal or written form can be disseminated more broadly and with much greater ease via email. By requiring an employer to allow its employees unfettered access to company-provided electronic communications systems for non-work-related purposes only exacerbates the risk of EEO noncompliance. As the Seventh Circuit has observed, "the abuse of access to workplace computers is so common (workers being prone to use them as media of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible." *Muick v. Glenayre Elec.*, 280 F.3d 741, 743 (7th Cir. 2002).

The risk of an employer's electronic communications being misused in such a manner is far from isolated. Studies have shown, for instance, that as much as 70% of adult content internet traffic occurs during the workday, with work computers providing many employees'

primary means of accessing sexual material online. *See, e.g.,* Amanda J. Lavis, Note, *Employers Cannot Get the Message: Text Messaging and Employee Privacy*, 54 Vill. L. Rev. 513, 527 n.70 (2009).

The point here is not that the Board or any court ever would consider those types of behaviors to be NLRA-protected. Rather, the relative ease with which inappropriate and/or harassing behavior occurs online – during work hours – counsels strongly in favor of permitting an employer to restrict all non-work email and electronic communications, so as to minimize the *opportunity* for employees to engage in this type of misconduct.

It is impossible to eliminate entirely every conceivable risk associated with email use. However, employers must be free to make decisions about acceptable levels of risk and resources that are necessary to reduce that risk. Employers may limit the number of employees who may utilize the email system, install software or contract for services that attempt to screen out harmful or offensive email traffic, and/or monitor employee use of email systems for inappropriate use. In addition, many other employers will adopt policies that limit use of the email system. These are business decisions that will be addressed differently by every employer. However, the majority in *Purple Communications* did not address risk at all, must less the employer's right to devise its own method of managing that risk.

D. Employer Email Systems Are Not The "Natural Gathering Place" Claimed By The Majority In *Purple Communications* And Evidence Indicates That The Importance Of Employer Email For Communication Among Coworkers Is Decreasing

In *Purple Communications*, the Board relied heavily on its assertion that email is "fundamentally a forum for communication," and is "effectively a new 'natural gathering place,'" 361 N.L.R.B. at 1060-61 (citation and footnote omitted), such that a presumption in

favor of nonwork use trumped any property interests of employers in their email systems. However, there is every reason to believe that advances in technology have made work email a second-tier means of non-work-related communication among employees generally. "Although email is still widely used, further advancements of the Internet have largely turned email into a legacy application." Andrew C. Payne, Note, *Twitigation: Old Rules In A New World*, 49 Washburn L.J. 841, 844 (2010) (footnote omitted). Indeed, "social-networking websites have become the preferred form of communication. In 2009, social networking surpassed email in worldwide reach." *Id.* at 848 (footnotes omitted). The Board is acutely aware of the growing use of social media in the workplace, and has for some time now been actively regulating employer practices in that space.

In addition to social media use, other forms of electronic communications, such as texting, continue to grow in popularity. There are now several platforms that have been developed that allow organizers, including union organizers, to manage distribution of text messages in a manner that simply was not possible in the past. According to the CEO of one such platform, Hustle, "Texting in 2016 happens to be the best way to have the most real conversations with the greatest number of people with the least amount of friction." Josh Constine, *Hustle Is The Grassroots Personalized Mass-Texting Tool We Need*, TechCrunch (Nov. 15, 2016).[2] The founder of another texting platform agrees. "How many unread emails do you have? How many unread texts do you have? Text is king." David Ingram, *Coming to Your*

[2] *Available at* https://techcrunch.com/2016/11/15/blood-sweat-and-text/ (last visited Oct. 5, 2018).

Smartphone: Texts With a Personal Touch From Political Campaigns, NBC News (Oct. 3, 2018).[3]

> According to one online communications firm:
>
> > *Text messaging is the most widely used communication channel available today.* While not everybody uses email or makes phone calls regularly, 90% of the American population texts. … Not only is text messaging more popular than other channels, 99% of text messages are open and read within the first 90 seconds of receiving them. In comparison, only a third of emails are opened ….”

Julie Hsu, *The Marketer’s Guide to Text Messaging*, Twilio (July 12, 2017).[4]

The increase in effective alternative communications such as social media and texting, coupled with the substantial risks inherent in allowing access to corporate information technology systems for non-work purposes and the strong employer interests in maintaining the integrity of such systems, must outweigh the purported convenience to some, but not all, employees of utilizing company systems for communications unrelated to their specific job responsibilities.

II. THE BOARD SHOULD RETURN TO *REGISTER GUARD’S* HOLDING THAT EMPLOYEES DO NOT HAVE A STATUTORY RIGHT TO USE EMPLOYER-PROVIDED EMAIL SYSTEMS FOR NONWORK PURPOSES, SO LONG AS THE EMPLOYER’S RESTRICTIONS ARE APPLIED IN A NONDISCRIMINATORY MANNER

The second question posed by the Board in its Invitation and Notice to file briefs is, if the Board should overrule *Purple Communications*, should it return to the holding of *Register Guard* or adopt some other standard. For the reasons described below, *amicus curiae* CWC respectfully submits that the Board should return to the holding of *Register Guard*.

---

[3] *Available at* https://www.nbcnews.com/tech/tech-news/sofas-ipads-campaign-workers-use-text-messages-reach-midterm-voters-n915786 (last visited Oct. 5, 2018).

[4] *Available at* https://www.twilio.com/learn/call-and-text-marketing/the-marketers-guide-to-text-messaging (last visited Oct. 5, 2018).

A. *Register Guard* Established A Straightforward Rule That Is Understandable To Both Employers And Employees And Relatively Easy To Administer

In *Register Guard*, the Board considered the validity of a company policy prohibiting the use of its email system for "'nonjob-related solicitations'" of any nature, including NLRA Section 7 matters. 351 N.L.R.B. at 1110. In considering the question, the Board first observed that "[c]onsistent with a long line of cases governing employee use of employer-owned equipment," *id.* at 1114, an employer "has a 'basic property right' to 'regulate and restrict employee use of company property'" – which includes corporate email communications systems. *Id.* (citation omitted). It went on to note:

> Respondent has a legitimate business interest in maintaining the efficient operation of its e-mail system, and … 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 emails.

Id. The Board thus found "no basis … 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," *id.* at 1116 (footnote omitted), and concluded that employers may lawfully prohibit non-work-related employee use of its email system, so long as they do not act "in a manner that discriminates against Section 7 activity." *Id.* (footnote omitted).

As one commentator wrote shortly after *Register Guard* was decided, the *Register Guard* standard "appears as a sensible approach to the realities of email usage where monitoring employee email is costly, especially given the widespread use of technology in the workplace." Nicole Lindquist, *You Can Send This But Not That: Creating and Enforcing Employer Email Policies Under Sections 7 and 8 of the National Labor Relations Act After* Register Guard, 5 Shidler J. L., Commerce & Tech. 15, at *21 (2009). In addition, employers, employees, and

labor unions had seven years of experience utilizing the standard with no evidence that it had the effect of chilling exercise of Section 7 rights.

It is true that in general, email use policies can be very difficult to police. The standard implemented in *Purple Communications* made this job more difficult, requiring greater scrutiny and more regular monitoring of employee email communications. A return to *Register Guard* would provide more flexibility to employers to design appropriate policies and practices for workplace compliance and to mitigate risk from email systems.

B. If The Board Does Not Overrule *Purple Communications*, It Should Permit Employers To Implement Reasonable Restrictions On Email Use Without First Demonstrating That Failure To Use Such Restrictions Would Interfere With Efficient Functioning Of The System

In *Purple Communications*, the Board stated that it would "not prevent an employer from establishing uniform and consistently enforced restrictions, such as prohibiting large attachments or audio/video segments, if the employer can demonstrate that they would interfere with the email system's efficient functioning." 361 N.L.R.B. at 1064.

Should the Board decline to revive the *Register Guard* standard, *amicus curiae* CWC urges that it establish a workable alternative that allows employers to place reasonable restrictions on the time and manner of employee access to company-provided employer electronic communications for non-work-related purposes without requiring a demonstration regarding the efficient functioning of the employer's email system. Such a rule should make clear that where company policy does not already permit personal use of email, such use, whether for Section 7 purposes or not, cannot occur during times when the employee is expected and being paid to carry out business-related functions. This is consistent with one of the Board's "oldest, clearest, and most easily applied … standards 'Working time is for work.'" *Purple*

Communications, 361 N.L.R.B. at 1068 (Member Miscimarra, dissenting) (footnote omitted). Likewise, non-work email use may not unreasonably interfere with the job duties and performance of the user's co-workers or infringe upon employee privacy rights.

An alternative standard also must allow employers to implement policies prohibiting non-work employee email communications – *whether intended to exert Section 7 rights or not* – that harass, intimidate or otherwise discriminate against any employee on the basis of a legally protected characteristic or in retaliation for statutorily-protected conduct. Likewise, employers must be free to implement policies preventing disclosure of proprietary information regarding the employer's business, intellectual property, trade secrets, or other sensitive company information through email and other electronic means. Any alternative standard should also allow employers to require that employees comply in all respects with the company's information technology data security requirements when utilizing work email and other electronic communications for non-work purposes. Finally, should the Board not return to *Register Guard*, any replacement standard should create a rebuttable presumption that employer disciplinary action for failing to comply with any of the above-referenced requirements is lawful.

III. EMPLOYER PROVIDED EMAIL WAS NOT THE ONLY EFFECTIVE MEANS OF COMMUNICATING AMONG EMPLOYEES IN *REGISTER GUARD* AND THE BOARD SHOULD NOT ADDRESS WHETHER EXCEPTIONS TO *REGISTER GUARD*'S HOLDING ARE NECESSARY UNTIL PRESENTED WITH AN APPROPRIATE CASE

The third question posed by the Board in its Notice and Invitation to File Briefs is, if the Board should return to the holding of *Register Guard*, should it carve out exceptions for circumstances that limit employees' ability to communicate with each other through means other

than their employer's email system. *Amicus curiae* CWC respectfully suggests that the Board should not create any exceptions at this time, but instead wait for an appropriate case.

In *Register Guard* the Board observed that there was "no contention … that the … employees rarely or never see each other in person or that they communicate with each other solely by electronic means." 351 N.L.R.B. at 1116. Consequently, the Board did not address whether exceptions should exist in circumstances "in which there are no means of communication among employees at work other than e-mail." *Id.* at 1116 n.13. Similarly, in *Purple Communications*, there was no contention that workers lacked opportunities to communicate in person. 361 N.L.R.B. at 1086 (Member Johnson, dissenting).

It may be that exceptions to *Register Guard* are warranted in a case where employer provided email is the only realistic way for employees to communicate with each other. However, given the rapid advances in technology and alternative means of communication that are evolving, the Board should refrain from adopting any particular exceptions at this time. It would be preferable for the Board to wait for an appropriate case to ensure that any exception is appropriately tailored to address real world challenges rather than abstract concerns.

IV. THE BOARD SHOULD EXTEND THE HOLDING OF *REGISTER GUARD* TO POLICIES GOVERNING USE OF OTHER COMPUTER RESOURCES SUCH AS THOSE AT ISSUE IN THIS CASE

In its Notice and Invitation to File Briefs, the Board notes that the policy at issue in the current case concerns use of an employer's "computer resources." *Caesars Entm't Corp.*, Case No. 28-CA-060841 (Aug. 1, 2018) (NOTICE AND INVITATION TO FILE BRIEFS, at 1, 2). However, until now the Board "has limited its holdings to employer email systems." *Id*. at 2. The Board then poses its fourth question in three parts: whether the Board should apply a

different standard to the use of computer resources other than email? If so, what should that standard be? Or should it apply whatever standard the Board adopts for the use of employer email systems to other types of electronic communications (*e.g.*, instant messages, texts, postings on social media) when made by employees using employer-owned equipment?" *Id.*

Amicus curiae CWC's answer to these questions depends on whether the Board overturns *Purple Communications* and returns to the holding of *Register Guard*, because the *Register Guard* framework would be an appropriate and easily understood test to apply to different types of employer-owned communications equipment. However, the standard articulated in *Purple Communications* would not.

A. This Case Is An Appropriate Vehicle To Address Policies Restricting Use Of Electronic Resources Other Than Email Systems

In her dissent to the Board's Notice and Invitation to File Briefs, Member McFerran suggests that this case would not be appropriate to address policies addressing forms of communication other than email. In a footnote, Member McFerran states that the present case "concerns only email" and suggests that addressing matters outside of email use would resemble rulemaking rather than adjudication. NOTICE AND INVITATION TO FILE BRIEFS, at 6 n.4.

While the procedural posture of this case is complicated, at issue in the present proceeding is whether the employer violated Section 8(a)(1) by promulgating and maintaining a Computer Resources Rule that interferes with, restrains, or coerces employees in the exercise of Section 7 rights. While the focus has been on the application of this policy to email, on its face the policy at issue applies to the use of employer equipment used to visit non-business websites, chat rooms, and message boards. In addition, while the policy also addresses personal email, the policy is clearly drafted in contemplation of employees' use of personal email through employer-

provided equipment as indicated by restrictions on streaming media and downloading photos, restrictions that would be unnecessary if employees were using personal email on their own electronic devices on non-work time.

The question before the Board is not the narrow question of whether the employer's email policy violates Section 8(a)(1), but instead whether the employer's Computer Resources Policy is in violation. The Board does not cross the line from adjudication to rulemaking by answering this question.

B. If The Board Overrules *Purple Communications* And Returns To The Holding Of *Register Guard*, Then *Register Guard* Should Apply To Use Of Other Forms Of Electronic Resources Such As Those At Issue In This Case

The computer systems impacted by the employer's Computer Resources Rule include the employer-provided computers or other electronic devices, software and networking required for internet access, and the employer's bandwidth, electronic resources efficiency, and storage capacity. Like email systems, each of these systems comes with risk that employers have a duty to manage. Like email systems, this risk poses significant harm to the employer, its employees, customers and clients, and shareholders.

As described above, *Purple Communications* failed to consider important employer property rights in any meaningful way. The consequences of any data breach or virus or malware attack that uses the employer's computer systems will be borne by employers. Employers should have the flexibility to tailor policies to most appropriately address the particular business risks that derive from the use of their electronic equipment. Thus, as with email systems, employer's legitimate interest in managing cybersecurity risk requires greater emphasis on employer property rights than permitted under *Purple Communications* and greater

than under the Board's prior equipment cases, which were questioned in *Purple Communications*. Restoration of *Register Guard* to employer-provided email systems and extension of its holding to additional employer-provided electronic resources such as those at issue in this case would allow employers to consider and develop flexible, individually-tailored policies to address workplace risk that is directly attributable to employee usage of employer-provided equipment.

In addition, *Purple Communications* has impeded employers' ability to manage equal employment opportunity compliance efforts. These efforts would only be further impeded if its holding were extended to other forms of electronic communications. However, application of *Register Guard* would give employers more ability to design policies and practices to ensure equal employment opportunity and mitigate risk of discrimination or harassment.

Extending *Register Guard*'s holding to additional electronic systems would not meaningfully impact employee Section 7 rights. Employers could not draft computer resources policies that discriminate along Section 7 lines and employers could not discriminate in their enforcement of such policies. In addition, *Register Guard* did not address a case where employer-provided email was the only effective means of communication. By extending *Register Guard* to the facts of this case, the Board would not prejudge whether an alternative rule is appropriate if employer-provided computer resources are the only effective means of communication.

To be clear, *Register Guard* only applied to employer-owned equipment. It did not address the lawfulness of employer policies that limit employee communication via personal email, text, social media posts, or any other means when done so on their own smart phone,

computer, or other device where employer property rights are not an issue. Extension of *Register Guard* to other employer-provided electronic resources would not impact employee communications unless those communications utilized employer-provided electronic resources.

For these reasons, if the Board does not overrule *Purple Communications*, then it should not apply its email standard to other types of electronic communications. However, if the Board does overrule *Purple Communications* and return to *Register Guard*, then that standard should be applied to other forms of computer and electronic resources as described above.

CONCLUSION

For the foregoing reasons, *amicus curiae* Center for Workplace Compliance respectfully submits that the Board should overrule *Purple Communications* and return to the standard articulated in *Register Guard*.

Respectfully submitted,

s/ Michael J. Eastman
Rae T. Vann
Michael J. Eastman
Counsel of Record
NT LAKIS, LLP
1501 M Street, NW
Suite 1000
Washington, DC 20005
meastman@ntlakis.com
(202) 629-5600

Attorneys for *Amicus Curiae*
Center for Workplace Compliance

October 5, 2018

CERTIFICATE OF SERVICE

I hereby certify that on this 5th day of October, 2018, an electronic copy of the foregoing was filed on the NLRB e-filing website and served by electronic mail on:

CASE PARTICIPANTS

Charged Party / Respondent
(Primary)
Jeff Soloman
Caesars Entertainment Corporation d/b/a Rio All-Suites Hotel and Casino
3700 West Flamingo Road
Las Vegas, NV 8910-4046

(Legal Representatives)
Elizabeth A. Cyr, Attorney
John T. Koerner, Attorney
Lawrence D. Levien, Attorney
James C. Crowley, Attorney
Akin Gump Strauss Hauer & Feld LLP
1333 New Hampshire Avenue NW
Suite 400
Washington, DC 20036-1564
Phone: (202) 887-4000
Fax: (202) 887-4288
Email: ecyr@akingump.com
Email: jkoerner©akingump.com
Email: llevien@akingump.com
Email: jcrowley@akingump.com

John D. McLachlan, Attorney
Fisher & Phillips LLP
1 Embarcadero Center
Suite 2050
San Francisco, CA 94111-3709
Phone: (415) 490-9017
Mobile: (650) 678-4330
Fax: (415) 490-9001
Email: jmclachlan@laborlawyers.com

(Legal Representatives for Charged Party/Respondent cont.)
Mark Ricciardi, Attorney
David B. Dornak, Attorney
Fisher & Philips LLP
300 South 4th Street
Suite 1500
Las Vegas, NV 89101
Phone: (702) 252-3131
Fax: (702) 252-7411
Email: mricciardi@laborlawyers.com
Email: ddornak@laborlawyers.com

Jim Walters, Attorney
Fisher & Phillips LLP
1075 Peachtree Street NE
Suite 3500
Atlanta, GA 30309-3900
Phone: (404) 240-4230
Mobile: (404) 580-3577
Fax: (404) 240-4249
Email: jwalters@laborlawyers.com

Charging Party
(Primary)
John Smirk, Business Manager
1701 Whitney Mesa Drive
Suite 105
Henderson, NV 89014-2046
Phone: (702) 452-2140

(Legal Representatives)
Caren P. Sencer, Attorney
David A. Rosenfeld, Attorney
Weinberg, Roger & Rosenfeld, PC
1001 Marina Village Parkway
Suite 200
Alameda, CA 94501-1091
Phone: (510) 337-1001
Mobile: (510) 715-3453
Fax: (510) 337-1023
Email: csencer@unioncounsel.net
Email: drosenfeld@unioncounsel.net
Email: nlrbnotices@unioncounsel.net

NLRB Regional Office
Cornele A. Overstreet
Regional Director, Region 28
2600 North Central Avenue
Suite 1400
Phoenix, AZ 85004-3099
Phone: (602) 640-2160
Email: NLRBRegion28@nlrb.gov

s/ Michael J. Eastman
Michael J. Eastman