UNITED STATES OF AMERICA
BEFORE THE NATIONAL LABOR RELATIONS BOARD

CAESARS ENTERTAINMENT CORPORATION
d/b/a RIO ALL-SUITES HOTEL AND CASINO,

and Case 28-CA-060841

INTERNATIONAL UNION OF PAINTERS AND
ALLIED TRADES, DISTRICT COUNCIL 15,
LOCAL 159, AFL-CIO

BRIEF OF *AMICI CURIAE*
COALITION FOR A DEMOCRATIC WORKPLACE,
THE RETAIL INDUSTRY LEADERS ASSOCIATION,
THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA,
THE INDEPENDENT ELECTRICAL CONTRACTORS, INC.,
THE INTERNATIONAL FOODSERVICE DISTRIBUTORS ASSOCIATION,
THE NATIONAL ASSOCIATION OF WHOLESALER-DISTRIBUTORS,
THE NATIONAL RETAIL FEDERATION, THE RESTAURANT LAW CENTER,
THE AMERICAN HOTEL & LODGING ASSOCIATION,
AND ASSOCIATED BUILDERS AND CONTRACTORS
IN SUPPORT OF RESPONDENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

Rachel Everly, USING INTERNAL SOCIAL NETWORKS TO ENHANCE EMPLOYEE PARTICIPATION, https://gethppy.com/employee-engagement/using-internal-social-networks-to-enhance-employee-participation (last accessed Oct. 4, 2018) 19

Rhitu Chatterjee, A NEW SURVEY FINDS 81 PERCENT OF WOMEN HAVE EXPERIENCED SEXUAL HARASSMENT, NPR (2018), https://www.npr.org/sections/thetwo-way/2018/02/21/587671849/a-new-survey-finds-eighty-percent-of-women-have-experienced-sexual-harassment (last visited Oct. 4, 2018) 21

Scott Allison, EMAIL STINKS—EMBRACE SOCIAL IN THE WORKPLACE INSTEAD (2013), http://www.forbes.com/sites/scottallison/2013/07/22/email-sucks-embrace-social-in-the-workplace-instead/#3cb67294020 (last visited Oct. 4, 2018) 16

Semantic Corporation, INTERNET SECURITY THREAT REPORT VOL. 23 (2018) 10, 11, 12

SMS, WIKIPEDIA (2018), https://en.wikipedia.org/wiki/SMS (last visited Oct. 4, 2018) 14

Sophia Said Birch, IBM'S CEO ON HACKERS: CYBER CRIME IS THE GREATEST THREAT TO EVERY COMPANY IN THE WORLD (2015), https://www.ibm.com/blogs/nordic-msp/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/ (last visited Oct. 4, 2018).....9

Steve Morgan, CYBER CRIME COSTS PROJECTED TO REACH $2 TRILLION BY 2019 (2016), https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#494c89993a91 (last visited Oct. 4, 2018) 12

Towers Watson, HOW THE FUNDAMENTALS HAVE EVOLVED AND THE BEST ADAPT (2013). 19

Tracey Caldwell, RISKY BUSINESS: WHY SECURITY AWARENESS IS CRUCIAL FOR EMPLOYEES (2013), https://www.theguardian.com/media-network/media-network-blog/2013/feb/12/business-cyber-security-risks-employees (last visited Oct. 4, 2018).....9

WIKIPEDIA (2018), https://en.wikipedia.org/wiki/Instant_messaging (last visited Oct. 4, 2018) 14

Yuki Noguchi, #METOO COMPLAINTS SWAMP HUMAN RESOURCES DEPARTMENTS, NPR (2018), https://www.npr.org/2018/06/04/615783454/-metoo-complaints-swamp-human-resource-departments (last visited Oct. 4, 2018) 21

Amici Curiae the Coalition for a Democratic Workforce, the Retail Industry Leaders Association, the Chamber of Commerce of the United States of America, Independent Electrical Contractors, Inc., the International Foodservice Distributors Association, the National Association of Wholesaler-Distributors, the National Retail Federation, the Restaurant Law Center, the American Hotel & Lodging Association, and Associated Builders and Contractors (together, the "*Amici*") respectfully submit this brief in response to the Board's August 1, 2018 Notice and Invitation to File Briefs in the above-captioned matter.

INTEREST OF THE *AMICI CURIAE*

The **Coalition for a Democratic Workforce** ("CDW") represents hundreds of employer associations, individual employers, and other organizations that together represent millions of businesses of all sizes. CDW's members employ tens of millions of individuals working in every industry and every region in the United States.

The **Retail Industry Leaders Association** ("RILA") is a trade association of retail companies. RILA members include more than 200 retailers, product manufacturers, and service suppliers, which together account for more than $1.5 trillion in annual sales, more than 42 million American jobs and more than 100,000 stores, manufacturing facilities, and distribution centers domestically and abroad.

The **Chamber of Commerce of the United States of America** ("Chamber") is the world's largest business federation, representing 300,000 direct members and indirectly representing an underlying membership of more than three million U.S. businesses and professional organizations of every size in every sector and geographic region of the country.

Independent Electrical Contractors, Inc. ("IEC") is the nation's premier trade association representing America's independent electrical and systems contractors, with over 50

chapters representing 3,400 member companies that employ more than 80,000 electrical and systems workers throughout the United States. IEC member companies are responsible for over $8.5 billion in gross revenue annually.

The **International Foodservice Distributors Association** ("IFDA") is the non-profit trade association for the foodservice distribution industry, representing more than 135 companies. With a combined annual sales volume of almost $300 billion, foodservice distributors are vital drivers of the American economy. IFDA member companies play a critical role in the foodservice industry supply chain and providing hundreds of jobs in each of their communities.

The **National Association of Wholesaler-Distributors** ("NAW") is a non-profit trade association that represents the wholesale distribution industry, the link in the supply chain between manufacturers and retailers as well as commercial, institutional, and governmental end users. NAW is comprised of approximately 40,000 companies operating at more than 150,000 locations throughout the nation. The wholesale distribution industry generates $5.6 trillion in annual sales volume and provides stable and good-paying jobs to more than 5.9 million workers.

The **National Retail Federation** ("NRF") is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants, and Internet retailers. Retail is the nation's largest private sector employer, supporting one in four U.S. jobs—42 million working Americans—and contributing $2.5 trillion to annual GDP.

The **Restaurant Law Center** ("Law Center") is a public policy organization created with the purpose of providing the restaurant and foodservice industry's perspective on legal issues significantly impacting it. The restaurant industry is a very labor-intensive industry comprised of over one million restaurants and other foodservice outlets employing almost 15 million people–

approximately 10 percent of the U.S. workforce. Restaurants and other foodservice providers are the nation's second largest private-sector employers.

The **American Hotel & Lodging Association** ("AHLA") represents all sectors and stakeholders in the lodging industry, including hotel owners, REITs, chains, franchisees, management companies, independent properties, bed and breakfasts, state hotel associations, and industry suppliers. The AHLA represents 24,000 properties nationwide, which support over 8 million jobs.

Associated Builders and Contractors ("ABC") is a national construction industry trade association representing more than 21,000 members. ABC's membership represents all specialties within the U.S. construction industry and is comprised primarily of firms that perform work in the industrial and commercial sectors.

The *Amici* regularly advocate for their members on issues of labor law and workplace policy, including by submission of *amicus* briefs in matters before the National Labor Relations Board ("NLRB") and various courts. The questions presented by the Board in its August 1, 2018 Notice and Invitation to File Briefs ("Notice") are of great importance to the *Amici*, as their determination will have immediate and long-lasting effects on their members' property rights, cyber security risks, financial viability, and workforce productivity.

SUMMARY OF ARGUMENT

In *Purple Communications,* 361 NLRB 1050 (2014) ("*Purple Communications*"), the Board reversed longstanding law and precedents and improperly created a new employee right to utilize employer equipment for union organizing and other Section 7 purposes. The *Purple Communications* decision should be overruled and the holding of *Register Guard,* 351 NLRB 1110

(2007), *enfd. in part and remanded sub nom Guard Publishing v. NLRB*, 571 F.3d 53 (D.C. Cir. 2009) ("*Register Guard*"), should be reinstated.

Prior to *Purple Communications,* for decades the Board consistently held, when approaching each and every technological evolution, that employees have no fundamental right to use employer equipment for Section 7 activity. The advent of email did not justify – let alone compel – a departure from this long-standing precedent, most recently clearly affirmed in *Register Guard*. To the contrary, the increasing pace of technological development and workplace innovation argues *against* the reactionary creation of new substantive rights, and in favor of continued application of a time-tested balancing test. Yet against this backdrop, without any legitimate basis, *Purple Communications* upended well-established Board precedent to create a new employee right to the employer's property.

Not only was *Purple Communications* short-sighted, gratuitous and unjustified, but in the few years since its passage, it has exposed employers to exponentially increasing, unnecessary risk. Cyber security threats have substantially increased both in volume and sophistication, especially those targeted at—and in some cases, created by—companies' own employees. Moreover, the potential damage to employers from such breaches has drastically increased, as more and more confidential, private, and business information is stored electronically on servers rather than in paper format, and therefore susceptible to cyber-crime. This rise in electronically stored confidential business information, along with the corresponding increase in data infiltration and piracy efforts, mandate that employers' property interests in their email and information systems be given greater import than the Board granted in *Purple Communications*.

At the same time, granting employees access to their employer's email system provides little benefit to employees exercising their Section 7 rights. Technological advances like

smartphones, SMS text, social media networks, and instant messaging applications have connected employees via more affordable — even free — options to a greater degree than ever before. These platforms are much better suited to simultaneous electronic communication, or purported "gathering," than their employers' business email. Employees' use of employers' property for Section 7 communication is far *less* necessary than ever, and far more dangerous to legitimate employer interests than any prior employer property historically protected by the Board. Accordingly, *Purple Communications* now manifests an entirely needless and hazardous infringement upon employer property rights.

Moreover, the increased risk being forced upon employers will stifle innovation and interfere with efficient business operations. Technological innovation in the workplace, particularly in the retail, food service and hospitality industries, is increasingly expanding to include tablets, handheld devices, and portable technology, all of which provide the capacity for constant access to the internet. Messages, chats, emails, etc. may instantaneously appear and are not easily, or even practically, separated into those that are work-related and those which are only to be viewed on non-working time. Under the standard imposed by *Purple Communications*, employers must now choose between either innovation with less control over both the technology itself and their employees' productivity, or halting innovation to preserve their property rights and protect their businesses.

The holding in *Register Guard*, which reflected longstanding board law and precedents, should be reinstated. Employers should lawfully be permitted to impose Section 7-neutral restrictions on employees' non-work-related uses of their email systems, without need to argue for predetermined exceptions. Moreover, there is no compelling reason to depart from the balancing test for any other "computer resources." Like all its other property, an employer should lawfully

be able to impose Section-7 neutral restrictions on the use of its other computer resources, even as employer-owned and maintained technology and equipment continue to evolve.

ARGUMENT

I. Response to Question 1: The Board Should Overrule *Purple Communications.*

In the Notice, the Board first asks whether it should adhere to, modify, or overrule *Purple Communications*. The *Amici* respond that *Purple Communications* should be overruled.[1]

A. The Board's decision in *Purple Communications* was an abrupt and unnecessary departure from decades of legal precedent.

For decades the Board consistently held that an employer has a basic property right to regulate and restrict employee use of its equipment. The Board repeatedly held that employees generally have no right to use employer-owned property, equipment, or materials for purpose of Section 7 communications, as long as the employer's restrictions on such usage are not discriminatory. Pursuant to this precedent, the Board upheld employers' property right with regard to employer-owned bulletin boards, copy machines, telephones, public address systems, and televisions. *See, e.g., Eaton Technologies*, 322 NLRB 848, 853 (1997); *Champion International Corp.*, 303 NLRB 102, 109 (1991) (an employer has "a basic right to regulate and restrict employee use of company property" such as copy machines); *Union Carbide Corp.*, 259 NLRB 974, 980 (1981), *enfd. in* 714 F.2d 657 (6th Cir. 1983) (an employer "could unquestionably bar its telephones to any personal use by employees"); *Churchill's Supermarkets*, 285 NLRB 138, 155 (1987) ("[A]n employer ha[s] every right to restrict the use of company telephones to business-related

1 In addition to the arguments set forth in this brief, the *Amici* specifically incorporate by reference the arguments and legal grounds for overruling *Purple Communications* as set forth in the Brief of the General Counsel filed in this matter on September 14, 2018. The *Amici* strongly support and agree with the General Counsel's legal arguments in support of overruling the *Purple Communications* decision.

conversations"); *Mid-Mountain Foods*, 332 NLRB 229, 230 (2000) (no statutory right to use breakroom television to show a pro-union campaign video).

The intrinsic value of the employer's property — or lack thereof — did not determine whether the employer had the right to restrict employees' use of that property. For example, in *Johnson Technologies*, 345 NLRB 762 (2005), the Board held that employees have no statutory right to use employer property as "trivial" as a ***piece of paper***. *Id.* at 769.

As recently as 2007 in *Register Guard*, the Board properly applied the aforementioned precedent and recognized the property rights of employers with regard to their email systems. The Board reaffirmed that "[a]n employer has a 'basic property right' to 'regulate and restrict employee use of company property,'" and found that the employer's email system, which was purchased and maintained by the employer for use in its business, was company property akin to employer telephones, bulletin boards, televisions, and copy machines. *Register Guard*, 351 NLRB at 1114. Recognizing fully the technological advance that email represented over previous communication methods, the Board nevertheless found no reason to depart from precedent. *Id.* at 1116. The Board rightly found that an employer "may lawfully bar employees' nonwork-related use of its e-mail system, unless the [employer] acts in a manner that discriminates against Section 7 activity." *Id.*

Subsequently, however, in *Purple Communications,* the Board unnecessarily, and without any sound justification, abruptly departed from this precedent and overruled *Register Guard*. In *Purple Communications*, the Board held that:

> [W]e will presume that employees who have rightful access to their employer's email system in the course of their work have a right to use the email system to engage in Section 7-protected communications on nonworking time. An employer may rebut the presumption by demonstrating that special circumstances necessary to maintain production or discipline justify restricting its employees' rights.

Purple Communications, 361 NLRB at 1063. The Board attempted to justify its departure from precedent by emphasizing the dramatic technological change email represented over past business communication systems and the purported minimal impingement on employers' property rights due to email's less finite storage capacity. *Id.* at 1057-60.

The Board's justifications are meritless. Technological innovation did not—and still does not—necessitate departure from decades of legal precedent regarding employer property rights. Before business communications were revolutionized by emails, they were revolutionized by the fax machine; and before fax machines, by telephone systems. Throughout each new, evolving technological development, the Board consistently held that employees have no fundamental right to use employer equipment for Section 7 activity.

The Board's reliance on the purported minimal impingement on employers' property rights that its decision creates is likewise misplaced. First, due to very nature of property rights, the amount of loss to the employer cannot be a threshold question as to whether those rights should be infringed upon. Regardless of the value of the employer's equipment, the employer has not only the right to use and maintain its equipment as it sees fit to operate its business, but it also the right to restrict access and use of that equipment in a non-discriminatory manner. As such, employees should have no statutory right to use employer property for Section 7 purposes, no matter how trivial the property. *See Johnson Technologies*, 345 NLRB at 769.

Second, even if it were a valid question, the impingement on employers' property rights, as discussed below, is anything but "minimal," and businesses are needlessly burdened by the *Purple Communications* standard. The Board's decision in *Purple Communications* has a significant impact on employers' property rights, as it improperly forces employers to assume

additional and significant risk related to its email and electronic systems, additional disruptions to productivity, and their corresponding costs.

1. The increased cyber security risks that employers must accept under *Purple Communications* have grown exponentially.

Purple Communications compels employers to permit their employees to use their email systems for internal and external nonbusiness communications. Increasing the number of non-work-related emails, to or from an infinite range of unknown sources, needlessly increases the prospect that opportunistic hackers, cyber-criminals, or mischief-makers might gain access to and harm the employer's system and data. *Purple Communications* therefore forces employers to assume a risk greater than that otherwise required by the operation of their businesses.

IBM Corporation's CEO and President, Ginni Rometty, recently called cyber-crime "the greatest threat to every profession, every industry, every company in the world." Sophia Said Birch, IBM'S CEO ON HACKERS: CYBER CRIME IS THE GREATEST THREAT TO EVERY COMPANY IN THE WORLD (2015), https://www.ibm.com/blogs/nordic-msp/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/ (last visited Oct. 4, 2018). With this recent rise of data infiltration and piracy, employers' property interests have been implicated by *Purple Communications* to a far greater degree than ever considered at the time of the decision.

Cyber security threats have substantially increased in volume in the past five years, especially those targeted at, and created by, companies' own employees. People are now the weakest link in the security chain. Since 2013, more than 60% of external attacks have targeted employees via email. Tracey Caldwell, RISKY BUSINESS: WHY SECURITY AWARENESS IS CRUCIAL FOR EMPLOYEES (2013), https://www.theguardian.com/media-network/media-network-blog/2013/feb/12/business-cyber-security-risks-employees (last visited Oct. 4, 2018). The volume of spam emails containing malicious links or attachments quadrupled in 2016. IBM Corporation,

IBM X-FORCE THREAT INTELLIGENCE INDEX 2017 10 (2018). One in 131 emails contained malware in 2016, the highest rate in five years. Semantic Corporation, INTERNET SECURITY THREAT REPORT VOL. 23 66 (2018). In 2017 alone, approximately 26 email viruses were sent to each email user in the manufacturing industry, and approximately 20 email viruses to each email user in the retail industry. *Id.* at 68.

The latest threats are much more sophisticated than previous impersonal, widely broadcasted spam emails with generic links. Increasingly, cyber-attacks through email utilize "spear phishing," whereby the attacker uses information gleaned from social media to personalize an email to an individual. Semantic Corporation, INTERNET SECURITY THREAT REPORT VOL. 23 28-29 (2018); *see also* Bill Sweeney, SOCIAL ENGINEERING: HOW AN EMAIL BECOMES A CYBER THREAT (2015), https://www.securityweek.com/social-engineering-how-email-becomes-cyber-threat (last visited Oct. 4, 2018) (noting that as data increasingly moves online, "social engineering techniques, where cyber thieves perform reconnaissance, collecting personal information of company employees and then attempting to get those employees to take an action, have become far more personalized, technologically advanced and ultimately successful."). Employees are more likely to open an email with specific personal information in the header, making spear phishing attacks more successful than previous tactics. *See* Fahmida Rashid, TYPES OF PHISHING ATTACKS AND HOW TO IDENTIFY THEM (2017) https://www.csoonline.com/article/3234716/phishing/types-of-phishing-attacks-and-how-to-identify-them.html (last visited Oct. 4, 2018) (noting that "[s]pear phishing attacks are extremely successful because the attackers spend a lot of time crafting information specific to the recipient, such as referencing a conference the recipient may have just attended or sending a malicious attachment where the filename references a topic the recipient is interested in."); Adrien Gendre, SPEAR PHISHING EMAIL (2017), https://www.vadesecure.com/en/spear-phishing/ (last

visited Oct. 4, 2018). They may open innocent-looking attachments or give away further information, including confidential or sensitive business information, replying to those emails. Due to their personal nature, employees are not easily able to identify spear phishing emails as cyber-attacks: just 36 percent of employees sampled in a 2015 study reported they were "very confident" that they could recognize and resist a phishing attack. Daniel Humphries, PHISHING SCAMS: WHY EMPLOYEES CLICK AND WHAT TO DO ABOUT IT (2015), https://www.softwareadvice.com/security/industryview/phishing-scams-report-2015/ (last visited Oct. 4, 2018).

Spear phishing attacks are increasingly common: in 2016, the number of phishing attacks increased by 65 percent worldwide, and the number of phishing websites (i.e., counterfeit websites to which individuals are directed, mainly through attack emails) increased 250 percent from the last quarter of 2015 to the first quarter of 2016. The Anti-Phishing Work Group, PHISHING ACTIVITY TRENDS REPORT (2016). In 2017, spear phishing emails were the primary infection vector in over 70 percent of targeted attack groups. Semantic Corporation, INTERNET SECURITY THREAT REPORT VOL. 23 28 (2018).

Similar to spear-phishing, watering hole attacks also target employees, and have greatly increased in sophistication the past five years. Watering hole attacks identify, and then compromise, a website of interest to a victim group. When the group visits that identified site, which has been compromised, the malware spreads to and compromises the targets' computers and networked systems. Semantic Corporation, INTERNET SECURITY THREAT REPORT VOL. 23 28-29 (2018). "Attackers will often compromise a website that is likely to be visited by intended targets. For example, if their target is in the aviation sector, they may compromise an aviation forum." *Id.* at 28.

The aggregate impact and costs of cyber-crime are enormous and have dramatically increased since *Purple Communications*: from 2013 to 2015, cyber-crime costs quadrupled, and it is estimated that from 2015 to 2019 there will be another quadrupling to $2 trillion. Steve Morgan, CYBER CRIME COSTS PROJECTED TO REACH $2 TRILLION BY 2019 (2016), https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#494c89993a91 (last visited Oct. 4, 2018); *see also* Chinn, et al., *Risk and Responsibility in a Hyperconnected World: Implications for Enterprises*, MCKINSEY & COMPANY AND THE WORLD ECONOMIC FORUM (2014) ("The risk of cyberattacks could materially slow the pace of technology and business innovation with as much as $3 trillion in aggregate impact.")

The modern workplace creates conditions that favor these attacks, due to the large number of employees networked with one another and with the employer's systems and confidential business information. As the frequency, sophistication, and costs of attacks increase, employers must spend more of their finite resources to defend against cyber-attack. "Blocking attacks at the point of entry," or the contact point at which the attacker was able to get on the victim's network in the first place (i.e., each email to the employee), "is the most effective way of combatting targeted attacks." Semantic Corporation, INTERNET SECURITY THREAT REPORT VOL. 23 28 (2018).

By requiring employers to permit employee use of their business email networks to communicate with internal and external sources regarding nonbusiness matters, *Purple Communications* forces employers to assume additional risks of cyber-attack. Each additional email received, attachment opened, link clicked, or website accessed creates an additional security risk to the employer's system and information, particularly those from external, non-business sources. Moreover, to the extent that *Purple Communications* makes use of work email systems for non-work purposes more commonplace, or at least permissible, it renders employees less

suspicious of non-work emails. *Purple Communications* thus effectively limits companies' ability to block attacks at the point of entry – as it only takes a single click on a link or an attachment to compromise the employer's entire information system. With employers unable to forbid employees from opening non-work emails, an invitation to open what appears to be a birthday invitation or a union flyer, or to visit a social or union website, could instead be a spear phishing or watering hole attack on the employer's business systems, and the employer is helpless to prevent it. Consequently, *Purple Communications*' direction to allow employees to use their systems for Section 7 purposes as a matter of right imposes a substantial risk on employers' operations, property interests, and financial viability that the employer would not otherwise need to assume to conduct its business.

2. The increased risks forced upon employers are unnecessary, as technological advances have connected employees to a greater degree.

Technological advances since *Purple Communications* – including personal electronic devices, and free social media, messaging and email accounts – obviate any presupposed need to use an employer's electronic systems for union or other Section 7 activity.

Today, the vast majority of Americans own personal devices by which they can connect with their co-workers. As of January 2018, a staggering 95% of American adults own a cell phone, and 77% of American adults own internet-enabled smart phones. Pew Research Center, MOBILE FACT SHEET (2018), *available at:* http://www.pewinternet.org/fact-sheet/mobile/ (last visited Oct. 4, 2018). By way of contrast, in 2011 only 35% of American adults owned internet-enabled smart phones, and that figure remained below 50% in the year *Purple Communications* was decided. *Id.*

The public availability and use of free online social media networks has also increased. In 2011 only half of all Americans used at least one social media site; by 2018, 69% of the public uses some type of social media. Pew Research Center, SOCIAL MEDIA FACT SHEET (2018),

available at: http://www.pewinternet.org/fact-sheet/social-media/ (last visited Oct. 4, 2018). Facebook is the most widely used of all social media: 81% of adults ages 18-29, 78% of adults 30-49, and 65% of adults age 50-64 use Facebook. *Id.* Moreover, Americans visit frequently: 74% of Facebook users check the site daily, and 51% check several times a day. Monica Anderson and Aaron Smith, SOCIAL MEDIA USE IN 2018 (2018), http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/ (last visited Oct. 4, 2018).

Unions and employers readily use Facebook, evidencing the ease by which Facebook pages can be used for discussing employers and employment, and people are increasingly using social media platforms to obtain news and to discuss important matters. For example, in 2017 46% of people reported they had complained about a business on social media, Alfred Lua, 2018 SOCIAL MEDIA TRENDS REPORT: 10 KEY INSIGHTS INTO THE PRESENT AND FUTURE OF SOCIAL MEDIA (2018), https://blog.bufferapp.com/social-media-trends-2018 (last visited Oct. 4, 2018), and 67% of Americans reported that they get news on social media. Jeffrey Gottfried and Elisa Shearer, News Use Across Social Media Platforms 2017 (2017), http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/ (last visited Oct. 4, 2018).

Social and app-based messaging,[2] in addition to SMS-based text messaging,[3] has also become widespread since *Purple Communications*. Social messaging apps grew 44% from 2015 to 2016, and this growth shows no signs of slowing down. Facebook Messenger alone has more

[2] Instant messaging (IM) technology is a vehicle for online correspondence that offers real-time text transmission over the Internet. These systems were initially based on local computer networks, but became more web-based in the late 1990s and early 2000s. The last decade, however, has seen an increase in messaging over smartphone-based messaging applications like WhatsApp, Facebook Messenger, WeChat and Viber. *See* Instant messaging, WIKIPEDIA (2018), https://en.wikipedia.org/wiki/Instant_messaging (last visited Oct. 4, 2018).

[3] SMS (short message service) is a component of most telephone, internet, and mobile-device systems, which uses standard communication technology to enable devices to exchange short text messages. SMS, WIKIPEDIA (2018), https://en.wikipedia.org/wiki/SMS (last visited Oct. 4, 2018).

than 1.3 billion monthly active users, and it is only one of many widely used and available, free social messaging applications. Further, although emails have been around for decades and messaging apps are relatively new, over 45% of American consumers say they would choose a messaging app over email to get in touch with a business. Pedro Goncalves, 10 GRAPHS THAT SHOW WHY YOUR BUSINESS SHOULD BE AVAILABLE THROUGH MESSAGING APPS (2017), https://medium.com/hijiffy/10-graphs-that-show-the-immense-power-of-messaging-apps-4a41385b24d6 (last visited Oct. 4, 2018) (citing UbiSend, 2016 MOBILE MESSAGING REPORT (2016)).

Notably, employees with smartphones are no longer using them only outside of work. Of the roughly eight in 10 workers who own personal smartphones, 82% keep them within eye contact at work. Jennifer Grasz, NEW CAREERBUILDER SURVEY REVEALS HOW MUCH SMARTPHONES ARE SAPPING PRODUCTIVITY AT WORK (2016), https://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=6%2F9%2F2016&id=pr954&ed=12%2F31%2F2016 (last visited Oct. 4, 2018). A 2017 survey of individuals in the financial services industry reported that 42% requested to use text messaging for business reasons. Ellen Chang, CAN YOUR EMPLOYER BAN TEXTING AT WORK? (2017) https://www.thestreet.com/story/14153118/1/can-your-employer-ban-texting-at-work.html (last visited Oct. 4, 2018). This number doubled from 2016. *Id.* At the same time, the percentage of workers who recommend contacting them on their landline at work, as opposed to their personal cell or smartphone, decreased 14% from 2014 to 2017. Jamie Herzlich, EMAIL STILL KING FOR WORKPLACE COMMUNICATION, BUT IM'S BOOMING (2017), https://www.newsday.com/business/columnists/jamie-herzlich/email-still-king-for-workplace-communication-but-im-s-booming-1.13773982 (last visited Oct. 4, 2018).

Social media and messaging facilitate dialogue and discussion in the workplace, thereby creating more openness and transparency than email ever could. *See, e.g.,* Scott Allison, EMAIL STINKS—EMBRACE SOCIAL IN THE WORKPLACE INSTEAD (2013), http://www.forbes.com/sites/scottallison/2013/07/22/email-sucks-embrace-social-in-the-workplace-instead/#3cb67294020 (last visited Oct. 4, 2018). More than two-thirds (68 percent) of employees said they are connected with co-workers on social media. *Id.* To the extent workplace email was ever considered a "natural gathering place" – a misguided notion, at best – that has now shifted to personal device-based social media and messaging platforms, through which instantaneous and multi-person discussions can be conducted with relatively greater ease.

Email messages, though touted as a technological game changer in *Purple Communications*, offer nothing to today's workforce that messaging and social media platforms do not—perhaps better—provide. The rapidity of technological development and adoption described above will make bright-line changes to the law, as announced in *Purple Communications*, outdated by the time the principal case finds its way through the final adjudication process. *This* new reality argues in favor of tried-and-true general balancing tests, and against the wholesale creation of new rights, as in *Purple Communications.*

To the extent there ever arguably existed a compelling need for employees to use employer email for non-work purposes, there simply no longer is *any* need. Employee rights are not infringed by business-only email policies. Weighed against the increasing threats posed to the employer's operations by this usage, there is no reasonable basis to hold that the employer's property rights must give way. Accordingly, *Purple Communications* should be overruled in its entirety.

B. The *Purple Communications* decision has increasingly negatively impacted employers.

In addition to the increased risk of cyber-attack, the increased use of employer email and electronic resources for personal purposes negatively impacts employee productivity, stifles employer innovation, and places employers in the untenable position of being unable to comply with other federal laws. As technology has advanced and as technological use across industry has expanded since the *Purple Communications* decision, so too has the negative impact on employers.

1. The increased risks forced upon employers by *Purple Communications* interferes with efficient business operations and stifles innovation.

Absent a reversal of *Purple Communications*, employers' ability to minimize employee distraction and control employee productivity will continue to be diminished, if not made impossible, and business innovation will be stifled.

First, incremental increases in the non-business use of business equipment necessarily results in a decrease in the availability of the equipment for productive, business use. Even setting aside that increased volume over the employer's network may decrease its efficiency, the amplified distractions encountered by employees forced to sort through an additional quantity of emails unrelated to their work duties will necessarily hamper productivity. There simply is no segregating non-business emails into a "nonworking time" box in employees' inboxes. Even a diligent worker will have to spend time sorting through non-work emails in his or her business inbox so that he or she can ensure prompt review and response to his or her business related emails that are required to perform the duties of his or her position.

Second, despite its limitation to the employers' email systems, *Purple Communications* has predictably been expanded to other devices, such as cell phones. *See, e.g., Verizon Wireless*, Case 02-CA-157403 at *9 (Div. of Judges May 25, 2017) (finding "that the employees' right to use [the employer's] email systems to engage in protected activity should naturally extend to the

computer or cellular devices that the employees use at work to access the systems…). Technological innovation in the workplace is increasingly expanding to include tablets, handheld devices, and portable technology, all of which have the ability to constantly access the internet. *See, e.g.,* John Foley, 10 TECHNOLOGY TRENDS THAT WILL REVOLUTIONIZE RETAIL (2014), https://www.forbes.com/sites/oracle/2014/01/13/10-technology-trends-that-will-revolutionize-retail/#3d1b93af419c (last visited Oct. 4, 2018). Messages, chats, and emails instantaneously appear and are not easily, or even practically, separated into those to be viewed on non-working time and those that are work-related. For example, in retail, customer service representatives on the sales floor are increasingly provided tablets with internet connectivity both to provide customer service to visiting customers (e.g., looking up an item for sale or checking in a customer for an appointment) and to perform point of sale transactions. *See id.* (noting that "[r]etailers can create a more seamless experience for customers, and increase the productivity and effectiveness of employees, by incorporating mobile technologies beyond smartphone shopping. For example, store employees can be equipped with tablets that have point-of-sale capabilities.") Similarly, restaurant workers are provided tablets with internet connectivity to take guests' orders and to complete the sale at the end of the meal. The same tablets can wirelessly connect to printers to print receipts, or the internet to email receipts to the customers.

Finally, employers are increasingly developing internal social networking platforms, designed to foster employee communication, training, and to track and support company production goals. *See, e.g.,* Rachel Everly, USING INTERNAL SOCIAL NETWORKS TO ENHANCE EMPLOYEE PARTICIPATION, https://gethppy.com/employee-engagement/using-internal-social-networks-to-enhance-employee-participation (last accessed Oct. 4, 2018); Towers Watson, HOW

THE FUNDAMENTALS HAVE EVOLVED AND THE BEST ADAPT (2013). It is reasonably foreseeable – and troubling – that *Purple Communications* might be expanded to these new innovations.

Absent a balancing test that appropriately recognizes the property interests of employers who are investing in such technology and the risks inherent in providing it to its employees, employers will be forced to choose between forgoing innovation to maintain their property interests, on one hand, or their employees' productivity, on the other. Without the ability to prohibit non-business use of its systems, as employers provide internet-connected tablets with email capability to their employees such as those described above, or otherwise provide technological innovation to employees, employers will also have to provide use of those devices, systems, and emails to the employees for non-business purposes. As the reach of devices expands to more employees—and to more of employees' working time—there will be an inherent and increased loss of productivity. And, as more employees access more non-business related sites, applications, and email content from those devices, the employers' risk and costs increase.

As the law currently stands, without the ability to restrict equipment usage so that the employer's risk is commensurate with the needs of its business, the only other choice available to employers is to not innovate.

C. Purple Communications improperly requires employers to subsidize speech.

The recent Supreme Court decision in *Janus v. Am. Fed'n of State, Cnty., and Mun. Emps., Council 31*, 138 S. Ct. 2448 (2018), also reflects a subsequent development which compels revisiting and overturning *Purple Communications*. As clarified therein, the First Amendment does not allow the Board, as a government entity, to force an employer to subsidize speech with which the employer does not agree. *Janus*, 138 S. Ct. at 2464 ("Compelling a person to subsidize the speech of other private speakers raises … First Amendment concerns."); *see also Purple*

Communications, 361 NLRB at 1105-07 (Member Johnson, dissenting) ("The First Amendment violation is especially pernicious because the Board now *requires an employer to pay for its employees to freely insult* its business practices, services, products, management, and other coemployees in its own email.") (emphasis in original).

D. *Purple Communications* puts employers in the untenable position of violating the NLRA by enforcing policies against use of its email systems for unlawful harassment.

The new employee right created in *Purple Communications* also places employers in the untenable position of violating the NLRA by enforcing policies against use of its email systems for unlawful harassment. Employers are obligated by law to provide a workplace free from sexual, racial, and other harassment. *See* 42 U.S.C. § 2000e *et seq* (1964); 29 C.F.R. Sec. 1604.11(f); *see also Meritor Savings Bank v. Vinson*, 477 U.S. 57 (1986). The Board, however, has increasingly shown a troubling willingness in recent years to protect racist, sexist, profane, and other forms of hateful speech under the guise of protecting Section 7 rights. *See e.g., Cooper Tire*, 363 NLRB No. 194 (2015) (protecting employees from termination based on racially charged remarks); *Consolidated Communications v. NLRB,* 837 F.3d 1 (D.C. Cir. 2016) ("…Board decisions' repeated forbearance of sexually and racially degrading conduct … goes too far.").

During the past year, the #MeToo and "Time's Up" movements have shined a bright, national spotlight on the ongoing problem of sexual harassment in the workplace, further magnifying an awareness growing steadily again in the years since *Purple Communications*. Bill Chappell, #METOO MOVEMENT IS PERSON OF THE YEAR, 'TIME' SAYS, *NPR* (2017), https://www.npr.org/sections/thetwo-way/2017/12/06/568773208/-metoo-movement-is-person-of-the-year-time-says (last visited Oct. 4, 2018). In 2015, soon after *Purple Communications*, the Equal Employment Opportunity Commission announced the formation of the EEOC Select Task

Force on the Study of Harassment in the Workplace. *See* EEOC to Study Workplace Harassment, 2015 JOB PATTERNS FOR MINORITIES AND WOMEN IN PRIVATE INDUSTRY (EEO-1), https://www1.eeoc.gov/eeoc/newsroom/release/3-30-15.cfm (last visited Oct. 4, 2018). In just this past year, more than 125 pieces of legislation have been introduced in 32 states to increase harassment prevention measures. Kathy Gurchiek, EEOC WANTS TO LEVERAGE TRANSFORMATIVE POWER OF #METOO, *SHRM* (2018), https://www.shrm.org/resourcesandtools/hr-topics/organizational-and-employee-development/pages/eeoc-wants-to-leverage-transformative-power-of-metoo-.aspx (last visited Oct. 4, 2018). News accounts report that the #MeToo movement "has created a deluge of complaints to human resource departments everywhere," perhaps tripling workplace investigation of harassment complaints. Yuki Noguchi, #METOO COMPLAINTS SWAMP HUMAN RESOURCES DEPARTMENTS, *NPR* (2018), https://www.npr.org/2018/06/04/615783454/-metoo-complaints-swamp-human-resource-departments (last visited Oct. 4, 2018). In a recent survey, 41% of women reported experiencing some form of "cybersexual harassment." Rhitu Chatterjee, A NEW SURVEY FINDS 81 PERCENT OF WOMEN HAVE EXPERIENCED SEXUAL HARASSMENT, *NPR* (2018), https://www.npr.org/sections/thetwo-way/2018/02/21/587671849/a-new-survey-finds-eighty-percent-of-women-have-experienced-sexual-harassment (last visited Oct. 4, 2018).

The right created in *Purple Communications* for employees to use the employer's email system to communicate on Section 7 issues thus gives employees free reign to use profanity, hate speech, or discriminatory comments over their employer's email systems, with little to no recourse for the employer. As frequent use of profanity or remarks regarding a protected category may constitute evidence of unlawful hostile work environment harassment, many employers may choose to employ a variety of email filtering technologies to prevent dissemination of

objectionable material over its email system. However, under *Purple Communications*, they are put in the untenable position of violating the NLRA – by interfering with protected communication between employees – should they do so.

In response to these concerns, the Board stated that employers are able to monitor "electronic communications on its email system … so long as the employer does nothing out of the ordinary, such as increasing its monitoring during an organizational campaign or focusing its monitoring efforts on protected conduct or union activists." *Purple Communications*, 361 NLRB at 1065. However, as the Board's decisions have made clear that sexist, profane, hateful, and disparaging comments themselves may be protected Section 7 conduct—the very speech that also may create a hostile work environment for other employees—the Board's exception is disingenuous. Either way, employers are placed in a precarious legal situation.

In sum, employers invest in and maintain their computer systems to be used for the purpose of their enterprise, and should assume only that much risk of exposure to the perils described above. Moreover, forcing employers to open their computer systems to the personal usage of their employees, in the face of a working population increasingly connected—and addicted—to immediately checking their messages, compels decreased productivity during working time and stifles innovation. *Purple Communications* should therefore be overruled.

II. Response to Question 2: The Board Should Reinstate the Holding of *Register Guard* and all Preceding Employer Equipment Precedent.

With respect to the second question contained in the Notice, The Board should return to the holding of *Register Guard* and all related precedent regarding employer equipment. *Purple Communications* unnecessarily changed the decades-old interpretation of unchanged statutory language. There remains no compelling reason to set aside the fundamental standards as set forth

in *Register Guard*, which, until *Purple Communications*, provided the industrial stability the Act is intended to support.

III. Response to Question 3: The Board Should Not Carve Out Any Exceptions from *Register Guard*'s Balancing Test, and Should Instead Consider Each Circumstance on a Case-by-Case Basis.

In response to the Board's third question, if the Board were to return to the holding of *Register Guard*—which it rightly should—the Board should not carve out exceptions for circumstances that purportedly limit employees' ability to communicate with each other through means other than their employer's email system. The notion that employees are limited in their ability to communicate with one another—even in situations such as a scattered workforce or in areas without broadband access—is a fallacy. Just as technology has rapidly and significantly advanced since the *Purple Communications* decision, so has connectivity across the nation.

As of year-end 2016, 97% of Americans could get wired broadband at any speed where they lived. Patrick Brogan, US TELECOM THE BROADBAND ASSOCIATION U.S. BROADBAND AVAILABILITY YEAR-END 2016 (2018), *available at* https://www.ustelecom.org/sites/default/files/USTelecom%20Research%20Brief%202.22.18.pdf (last visited Oct. 4, 2018). Even if not at an employer's facility, free public Wi-Fi access is ubiquitous in public areas (e.g., public transportation, libraries, and parks) as well as commonly visited private places of business (e.g., grocery stores, drug stores, coffee shops, and restaurants).

Moreover, mobile broadband from multiple providers is now also widely available throughout the United States. As of year-end 2016, mobile broadband access using 4G LTE – a technology not yet available at the time of the *Purple Communications* decision – was available to 99.6% of Americans. *Id.* As discussed above, 95% of American adults own a cell phone, and 77% of American adults own internet-enabled smart phones. And, in America, at least 99.9% of Americans live within range of a mobile cellular signal, irrespective of whether or not they are

subscribers. International Telecommunications Union, MOBILE NETWORK COVERAGE, PERCENT OF THE POPULATION, 2016 (2016), *available at:* https://www.theglobaleconomy.com/rankings/Mobile_network_coverage/ (last visited Oct. 4, 2018).

Accordingly, even in a scattered workforce, an employee has multiple avenues through which he or she can connect with his or her co-workers. Within the context of 2018 connectivity, there exists no universally applicable circumstance, such as a purported lack of access to broadband connectivity, either wired or mobile, that justifies the Board specifying circumstances in advance to which *Register Guard* should not apply. If an individual case warrants exception, it should—and can, within the framework of *Register Guard*'s application of the decades-old *Republic Aviation* balancing test—be considered on a case-by-case basis.

IV. Response to Question 4: The Board Should Apply the Holding of *Register Guard* and all Longstanding Employer Equipment Cases to all Computer Resources.

In response to the Board's fourth and final question, the Board should apply the holding of *Register Guard* and all preceding employer equipment precedent to the use of employers' computer resources other than email. Prior to *Purple Communications*, the Board consistently held, throughout each new, evolving technological development, that employees have no fundamental right to use employer equipment for Section 7 activity. There was no legitimate reason to depart from *Register Guard*'s application of the decades-old precedent in *Purple Communications* with regard to email communications, and there is no compelling reason to depart from the *Register Guard* standard with respect to other new or existing computer resources. The same test should apply, and employers should be permitted to prohibit non-business use of its equipment and resources so long as the prohibition is non-discriminatory.

V. Conclusion.

For all the reasons set forth above, as well as the many thoughtful arguments laid out in the briefs before the Board, the Board should overrule *Purple Communications* and reinstate the holding of *Register Guard* that absent discrimination, employees have no Section 7 right to use employer equipment—including email, computers, tablets, and computer resources—for union organizing purposes.

Respectfully submitted this 5th day of October, 2018.

McGuireWoods LLP

/s/Seth H. Borden
Seth H. Borden
1251 Avenue of the Americas
20th Floor
New York, NY 10020-1104
(212) 548-2180
sborden@mcguirewoods.com

Richard B. Hankins
Brennan W. Bolt
Promenade
1230 Peachtree Street, NE
Suite 2100
Atlanta, GA 30309-3534
(404) 443-5727
rhankins@mcguirewoods.com
bbolt@mcguirewoods.com

Sarah K. Hawley
World Trade Center
101 West Main Street
Suite 9000
Norfolk, VA 23510-1655
(757) 640-3710
shawley@mcguirewoods.com

Attorneys for the Amici Curiae

Angelo I. Amador
Restaurant Law Center
2055 L Street, NW
Seventh Floor
Washington, DC 20036
(202) 331-5913
aamador@restaurant.org

Attorney for Restaurant Law Center

CERTIFICATE OF SERVICE

Pursuant to the Board's August 1, 2018 "Notice and Invitation to File Briefs," the undersigned hereby certifies that a copy of the foregoing amicus brief in Case 25-CA-060841 was electronically filed via NLRB E-Filing System with the National Labor Relations Board and served in the manner indicated to the parties listed below on this 5th day of October, 2018.

Caren Sencer
David A. Rosenfeld
WEINBERG ROGER & ROSENFELD
1001 Marina Village Pkwy
Suite 200
Alameda, CA 94501-1091
Counsel for Charging Party

Via Electronic Mail
csencer@unioncounsel.net
drosenfeld@unioncounsel.net

David Dornak
Mark Ricciardi
FISHER & PHILLIPS LLP
300 South 4th Street, Suite 1500
Las Vegas, NV 89101
Counsel for Respondent

Via Electronic Mail
ddornak@fisherphillips.com
mricciardi@fisherphillips.com

John McLachlan
FISHER & PHILLIPS LLP
1 Embarcadero Center, Suite 2050
San Francisco, CA 94111-3709
Counsel for Respondent

Via Electronic Mail
jmclachlan@fisherphillips.com

Jim Walters
FISHER & PHILLIPS LLP
1075 Peachtree Street, NE, Suite 3500
Atlanta, GA 30309-3900
Counsel for Respondent

Via Electronic Mail
jwalters@fisherphillips.com

Elizabeth Cyr
James C. Crowley
Lawrence Levien
John Koerner
AKIN GUMP STRAUSS HAUER & FELD LLP
1333 New Hampshire Avenue, NW, Suite 400
Washington, DC
20036-1564
Counsel for Respondent

Via Electronic Mail
ecyr@akingump.com
jcrowley@akingump.com
llevien@akingump.com
jkoerner@akingump.com

/s/ Seth H. Borden
Seth H. Borden