SOMETHING OLD AND SOMETHING NEW: BALANCING “BRING YOUR OWN DEVICE” TO WORK PROGRAMS WITH THE REQUIREMENTS OF THE NATIONAL LABOR RELATIONS ACT

Patrick J. Beisell

TABLE OF CONTENTS

I. Introduction ........................................................................................................... 498
II. Background ......................................................................................................... 500
    A. The Current State of BYOD ........................................................................ 500
    B. Benefits of BYOD Programs ..................................................................... 502
    C. Issues With BYOD Programs .................................................................... 503
    D. Section 7 of the NLRA .............................................................................. 505
III. Analysis .............................................................................................................. 508
    A. The Register-Guard Decision .................................................................... 508
       1. Background ............................................................................................. 508
       2. Arguments of the Parties and Amici Before the Board ................. 510
       3. The Board’s Opinion ............................................................................. 511
       4. The Politicization of the Board ............................................................. 513
       5. Purple Communications ....................................................................... 515
       6. Applying Register-Guard to BYOD .................................................... 517
    B. Employer Monitoring of BYOD Devices ............................................... 520
    C. BYOD Policies Are Mandatory Subjects of Bargaining .................... 523
IV. Recommendation .............................................................................................. 527
V. Conclusion .......................................................................................................... 530

* J.D., University of Illinois College of Law, May 2015. M.Ed., Secondary Education, University of Missouri - St. Louis, June 2011. B.A., English Literature, Portland State University, May 2009. I thank the JLTP staff for their diligence and dedication to publishing excellent work. I would also like to thank my Note Editors, Joshua Gross and Michael Park, for their guidance and feedback during the writing and editing of this Note. Professor Matthew Finkin deserves particular praise for inspiring me to write this Note and for taking the time to share with me his wealth of Labor Law knowledge. Finally, I wish to thank my family and friends for their love, support, and understanding throughout my law school career.
I. INTRODUCTION

While the phrase “consumerization of technology” was not coined until 2001, the idea dates back at least to the advent of the personal computer in the 1980s and 1990s.1 The consumerization of technology eschews the old enterprise-driven paradigm, wherein the employer determines what technological tools employees use in the workplace,2 for the consumer driven paradigm wherein consumers are the ones developing, identifying, and spreading a particular piece of technology (e.g., a phone, a tablet, a mobile application, etc.) with businesses following suit.3 The effect of this paradigm shift is a disruption to the paternalistic model of businesses exerting near total control over IT decisions.4

The consumerization of technology has expanded rapidly in the last five years, due in large part to the proliferation of, and market popularity of, the iPhone, the iPad, and Android devices.5 This sea change has prompted many businesses to allow employee-selected devices (i.e., the ones that predominate in the consumer market) to interface with employer IT systems or, in some cases, to replace employer-owned devices.6 In fact, the decision to allow employee-owned or selected devices to replace employer-owned or selected devices has become a significant trend, even garnering the nickname “Bring-Your-Own-Device” to work (BYOD).7 Moreover, in recent years BYOD has expanded from the private workplace into the public sphere, including use by the United States government and at least one state-wide education system.8 This expansion into multiple sectors and industries evidences that BYOD is more than a trend, it is a “leading indicator[] of long-term structural change

3. Id.
5. See Mukerji, supra note 2, at 31–32 ("Enterprise IT policies are now being influenced by the consumer uptake of technologies, and investing in many popular consumer technologies and products such as tablets, instant messaging, social media, location-aware services and mobility applications.").
7. See Understanding the Bring-Your-Own-Device Landscape, DELLOITE LLP 2 (2013), http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/Industries/TMT/ak-tmt-understanding-byod-v2.pdf (noting that BYOD “is not a single idea or way of working. Rather it represents a broad spectrum of devices, capabilities and responses indicative of the evolving role of technology in the relationship between work and personal lives.").
8. In 2012, the U.S. government released a BYOD policy toolkit with suggested policies for federal agencies and an analysis of federal agency pilot programs. CIO COUNCIL, BRING YOUR OWN DEVICE: A TOOLKIT TO SUPPORT FEDERAL AGENCIES IMPLEMENTING BRING YOUR OWN DEVICE (BYOD) PROGRAMS (2012). In the 2013 and the 2014 General Sessions, the Utah State Senate promoted BYOD as a component of their proposed “Student-centered Learning Pilot Program,” stating that schools should “encourage students to utilize BYOD ‘bring your own device’ as part of the school’s technology device policy.” S.B. 171, 60th Leg., Gen. Sess. (Utah 2014).
occurring in the [IT] industry, not the demands of a few errant staff demanding their favorite brand of technology.9

What the consumerization of technology and the advent of BYOD demonstrate is that the workplace is becoming increasingly electronic. Email has become a ubiquitous, even necessary, communication tool and it would strike the average employee as unusual if the workplace functioned without email.10 Workplaces are now replete with more technological tools than ever before—cloud storage, Google documents, Skype and online meetings, etc. BYOD programs are just one example of the growing desire to make the workplace more technologically adept. While BYOD programs may create a more efficient workplace, they also have the potential to create liability for employers. One concern is that, under the National Labor Relations Act (NLRA), a BYOD program may be a mandatory bargaining subject and a restrictive BYOD policy “could chill an employee’s ability to communicate with others about wages, hours, and working conditions or to engage in otherwise protected activity.”11

The National Labor Relations Board (NLRB or “the Board”), charged with interpreting and enforcing the NLRA,12 has only recently confronted issues stemming from this increasingly electronic workplace.13 The NLRB has dealt with the degree of statutory protection afforded to employees’ email usage,14 the appropriate bargaining unit where no employees have a fixed work location and all report electronically,15 and union access to employees in a

13. See, e.g., In re Guard Publ’g Co. & Eugene Newspaper Guild, 351 Decisions and Orders of the National Labor Relations Board (N.L.R.B.) 1110 (2007) (deciding to what extent policies can prohibit employees from utilizing email for non-job functions) [Hereinafter Register-Guard II].
14. See, e.g., id. (holding that employees have no statutory right to use employer’s property, including email systems, for Section 7 purposes); Timekeping Sys., Inc. & Leinweber, 323 Decisions and Orders of the National Labor Relations Board (N.L.R.B.) 244, 248–50 (1997) (finding employee’s email critique of employer’s new vacation benefits entitled to statutory protection); E. I. DuPont de Nemours & Co. & Chem. Workers Ass’n, 311 Decisions and Orders of the National Labor Relations Board (N.L.R.B.) 893, 897 (1993) (finding employer violated NLRA when it prohibited employees from distributing union literature over the company email system).
virtual workplace. This Note explores the tension between the NLRA and BYOD programs and argues that (1) the Board needs to update its view of the modern workplace and overturn Register-Guard and (2) the unique features of BYOD require sensitive consideration of employee Section 7 rights under the NLRA. Part II discusses the present state of BYOD and the benefits and problems inherent in a BYOD program. Part III analyzes three labor law issues in the context of a BYOD program: first, the Board’s decision in Register-Guard is analyzed as an example of the Board’s approach to employee Section 7 rights within the context of new technologies, the politicization of the Board is considered, and Purple Communications (a case that could potentially overturn Register-Guard) is briefly discussed; second, employer monitoring of employee’s electronic speech and action in the context of BYOD is assessed; third, this Note analyzes whether or not the institution of a BYOD program is a mandatory subject of bargaining under the NLRA. Part IV recommends rejecting Register-Guard, updating the Board’s approach to securing employee rights in the modern technologized workplace, and ensuring that employers implement a comprehensive and careful BYOD policy sensitive to the dictates of the NLRA.

II. BACKGROUND

A. The Current State of BYOD

In 2011, an international study of the consumerization of technology indicated that the phenomenon had reached a tipping point. The report collected data from 600 surveys completed by companies across a myriad of countries and industries. Fifty-six percent of respondents favored the use of personal devices at work (i.e., BYOD programs). However, different countries have adapted to the BYOD trend at vastly different rates: seventy-five percent of US companies said “yes” to consumerization, while only fifty-nine percent of German companies said “yes,” and thirty-six percent of Japanese companies said “yes.” An examination of industry assent demonstrated a similar pattern: Education (80%), Health Care (69%), Business Services (67%), Manufacturing (48%), Government (39%), and Utilities (36%).

In 2011, the Aberdeen group surveyed 415 companies across the globe and reported an even more significant acceptance of BYOD. Of the

employees report electronically).
companies surveyed, seventy-five percent allowed employees to use their personal device for and at work.\textsuperscript{23} Also in 2011, Forester Research surveyed roughly 1,600 US information technology workers and reported that forty-eight percent of respondents were allowed to purchase the smartphone of their choice and use it for work.\textsuperscript{24}

While BYOD appears to be edging toward a firm majority foothold in the workplace, this position is a recent development. The International Data Corporation and Unisys completed a study in 2010 and 2011 of 3,000 information workers and business executives in nine countries.\textsuperscript{25} The 2011 study reported that forty percent of devices used by respondents at work were personal devices.\textsuperscript{26} More to the point, this was a ten percent increase from the 2010 study.\textsuperscript{27} This BYOD trend appears to have staying power. A recent study by Gartner predicts that by 2017, half of all employers will require employees to provide their own device for work purposes.\textsuperscript{28}

Given the prevalence of BYOD programs, it is useful to consider how employers are approaching the implementation of BYOD. BYOD programs will contain, at minimum, three substantive components: a software application that manages any device connecting to the company network (usually referred to as Mobile Device Management (MDM) software), a policy defining the responsibilities of both the employer and the user, and an agreement that users must sign, acknowledging that they have read, understand, and agree to be bound by the policy.\textsuperscript{29} The policy itself will vary among employers depending on the needs of the company, the types of devices being used, the size of the network, and the sensitivity of accessible data. However, a basic policy will include provisions for acceptable use, types of devices allowed and supported by the network and the IT Department, reimbursement (or lack thereof), security, and, of course, a catch-all section on liability.\textsuperscript{30} A recent sampling of BYOD policies across three industries—a software vendor, a school district, and a global bioscience company—showed that BYOD policies are all relatively similar in substance and vary only in structure and level of specificity.\textsuperscript{31}

\begin{itemize}
  \item \textsuperscript{23} Id.
  \item \textsuperscript{24} Id.
  \item \textsuperscript{26} Id.
  \item \textsuperscript{27} Id.
  \item \textsuperscript{28} Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes, GARTNER (May 1, 2013), http://www.gartner.com/newsroom/id/2466615.
  \item \textsuperscript{29} Megan Berry, BYOD Policy Template, IT MANAGER DAILY, http://www.itmanagerdaily.com/byod-policy-template (last visited Oct. 18, 2014).
  \item \textsuperscript{31} See generally Sandra Gittlen, A Sample of BYOD User Policies, NETWORK WORLD (May 1,
B. Benefits of BYOD Programs

Three rationales are typically proffered in support of a BYOD program: increased employee productivity, employee satisfaction, and cost savings.\(^{32}\) As to the first rationale, since BYOD is based on the consumerization of technology, employees will tend to select the device that they are most interested in, making it more likely that they will become expert users.\(^{33}\) Moreover, since the employee has selected the device and exercises it for personal use, they are more likely to upgrade the device regularly.\(^{34}\) Both of these factors can contribute to employees using their devices in more productive ways. According to a recent report by Forrester Group and TrendMicro,\(^{35}\) eighty-two percent of companies surveyed said they thought BYOD programs increased staff productivity, with the largest group claiming it increased productivity by ten to twenty percent.\(^{36}\)

As to the second rationale, according to IBM, eighty-three percent of users considered their mobile device more important than their morning cup of coffee.\(^{37}\) Allowing employees to select their own device increases the likelihood that employees will choose a device that they enjoy. Consequently, employees will be more likely to use the preferred device at home and at work, thereby reducing the likelihood of employees having to carry multiple devices.

The third rationale proffered, that BYOD programs result in cost savings, remains contested.\(^{38}\) As IBM has stated, “BYOD programs _sometimes_ save budget[s] by shifting costs to the user, with employees paying for mobile devices and data services. However, this often results in little to no savings.”\(^{39}\) For example, the Forrester Group report indicated that BYOD programs resulted in an eight percent increase in the number of help desk calls, a seven percent increase in mobile device management costs, a three percent increase in corporate liable data costs, a three percent increase in server costs, and a two percent increase in regulatory compliance expenses.\(^{40}\) However, the same report also noted that BYOD programs resulted in a fifteen percent decrease in device replacement costs, an eight percent decrease in reimbursement for employee data expenses, a five percent decrease in training and education

\(^{33}\) _Id._
\(^{34}\) _Id._
\(^{37}\) _Id._
\(^{38}\) _Id._
\(^{39}\) _Id._ (emphasis in original).
\(^{40}\) Garlati, _supra_ note 17.
costs, and a three percent increase in bottom line revenues. Consequently, cost savings appears to be an ambiguous, or at least misleading, rationale for adopting a BYOD program.

C. Issues With BYOD Programs

One overarching concern across industries is that employers are not communicating their BYOD policy to employees. In a 2012 study, Globo reported that sixty-eight percent of respondents use their personal devices for work, “while only twenty-nine percent said that their company actually has a BYOD policy in place.” Furthermore, forty-two percent of respondents don’t know if their company’s BYOD policy allows IT to have full access to their personal devices.

Apart from this communication quandary, BYOD programs in the abstract present numerous challenges for employers. Beyond financial concerns, employers with BYOD programs face a variety of security issues: unknown third-party access via mobile apps, challenges in tracking data, data management, segregation difficulties for compliance, data leakage due to stolen or lost mobile devices, and disgruntled employees. To combat such issues, employers have turned to MDM service providers.

MDM is a software platform that provides security and uniformity among employees’ mobile devices across multiple service providers and operating systems. Implementation of MDM generally occurs in four phases. In phase one, the device inherits an enterprise identity and the corporate network infrastructure is created to avoid resource complexity and duplication.

41. Id.
43. Id.
44. Id.
47. See Vangie Beal, Mobile Device Management – MDM, WEBOPEDIA, http://www.webopedia.com/TERM/M/mobile_device_management.html (last visited Oct. 18, 2014) (defining MDM as “security software used . . . to monitor, manage and secure employees’ mobile devices that are deployed across multiple mobile service providers and across multiple mobile operating systems being used in the organization”).
49. Id.
phase two, the IT team begins to actively manage all devices to ensure the enterprise persona remains intact.\textsuperscript{50} At this point the network infrastructure is fully functional and users are given access to corporate resources and information.\textsuperscript{51} Moreover, in phase two, users are generally provided with the terms of agreement outlining what is acceptable and unacceptable use of the device and corresponding network.\textsuperscript{52} In phase three, the IT team becomes responsible for managing mobile apps for all users.\textsuperscript{53} In the final phase, the MDM software uses an application-programming interface to detect and reduce mobile service plan overages.\textsuperscript{54}

Under an MDM, when new devices are added to the enterprise, the existing persona is imprinted on the device prior to the user gaining access to corporate resources.\textsuperscript{55} Moreover, the MDM can create different personae and different levels of permission so that particular users (e.g., senior executives) can access different levels of secure corporate resources and information.\textsuperscript{56} If and when an employee leaves the company, the MDM is capable of removing the enterprise and any accompanying permissions and access to company property.\textsuperscript{57} The MDM can complete a selective wipe, leaving personal data, such as pictures, music, and other files, intact.\textsuperscript{58} However, the MDM is also capable of performing a complete wipe of a device.\textsuperscript{59} Unfortunately, many company policies require a complete wipe of a device if it is reported lost or stolen.\textsuperscript{60} As the wiping function makes clear, the MDM platform is primarily focused on the security and integrity of corporate resources and information.\textsuperscript{61}

\textsuperscript{50} Id.
\textsuperscript{51} Id.
\textsuperscript{52} Id.
\textsuperscript{53} Id.
\textsuperscript{54} Id.
\textsuperscript{55} Id.
\textsuperscript{56} Id.
\textsuperscript{57} Id.
\textsuperscript{58} Id.
\textsuperscript{59} Id.

“Sandboxing,” a commonly used technique for mobile device management, is a containerization method that allows employees to isolate and “manage corporate data and run business apps [on their mobile devices] . . . without having them intermingle with personal data.” Isolating virtual workspaces has the added benefit of permitting selective remote wiping of corporate data on a lost or stolen device, thereby protecting business assets while leaving personal data and settings intact.

A dual SIM card device eliminates the need for an employee to carry two devices, one for work and one for personal use, but permits the separation of communications and data through personal and work modes.

Private cloud sharing, which allows employees to access private clouds, as opposed to Dropbox or iCloud, appeases employees’ desire for connectivity, allows them to be productive, and abates security and data leakage risks. As an added bonus to the employee, cloud-based architecture also saves an employee’s personal data if a device needs to be remotely wiped.

Corporate mobile applications let employees use their mobile devices to link to Sharepoint
While security issues are a pertinent concern for BYOD employers, there remain more basic, threshold concerns: when is a BYOD device employee-owned or employer-owned? What are the rights of employees using a BYOD device? At this juncture, BYOD should be distinguished from Company (or Corporate-Owned-Personally-Enabled (COPE) programs. In a standard BYOD program, the employee purchases the device and pays for all of, or most of, the costs associated with the device. In a standard COPE program, the company owns the device and pays for all of, or most of, the costs associated with the device. The company allows the employee to install applications, music, video, and the like, and to use a “non-work” portion for personal purposes. Moreover, the company generally provides employees with a finite list of devices to choose from. By contrast, assuming that the employee owns the BYOD device, policies limiting usage and communications have direct implications on employees’ statutory rights under the NLRA.

D. Section 7 of the NLRA

As this Note is devoted to exploring the tensions and possible implications a BYOD policy might generate in a workplace protected by the NLRA, it is useful to examine some basic aspects of the NLRA that will serve as a foundation for the following legal analysis.

Section 7 of the NLRA states, in pertinent part, that “[e]mployees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection . . .” To be insulated from adverse employer action, the speech or action, whether by a unionized worker or a non-unionized worker, must be both “concerted” and “for mutual aid and protection.”

One understanding of concerted activity would be action that is “arranged by mutual agreement, done in concert, coordinated . . . united in action or documents that allow communal editing features, and let an institution maintain security while giving employees additional flexibility to be productive and efficient. Id.

62. IBM, supra note 32.
64. See generally Lorenc & Nelson, supra note 46 (“Comprehensive application deployment, management and security provides the ability to push and install mandatory apps and publish recommended apps to users through a corporate app storefront to the Work Space, without impacting their ability to access and use personal apps and content in their Personal Space.”).
65. See, Gitten, supra note 31 (“Employees that purchase a device on their own that is not in line with our standard approved device lists may not be allowed to have their devices added to the servers. It is highly recommended that the employee refer to the Smart phone support site to review the devices that are being supported by IT.”).
67. Id. (emphasis added).
intention. Thus, given the emphasis on action that is “mutual,” “in concert,” or “coordinated,” one could read “concerted activity” as requiring two or more employees to work together toward a common goal. Indeed, if two employees agreed to lodge a protest and to designate one of them to speak to management alone, for himself as well as on behalf of the more timid co-worker, the spokesman would also be deemed to have engaged in concerted activity, immune from disciplinary reprisal. While this interpretation of “concerted activity” often holds true of non-union employees, it is not necessarily applicable to unionized employees. In some instances, a union employee acting alone in protest of a work assignment or an unfair labor practice has been deemed to be acting in concert because she is seeking to enforce provisions of the collective bargaining agreement. However, the factual contours of each case may result in a different outcome.

Indeed, situations characterized as “personal protest,” “individual protest,” or “personal gripe” cases have been uniformly rejected as unprotected, unconcerted activity.

70. Id.
72. Minimark Corp. v. NLRB, 7 F.3d 547, 550 (6th Cir. 1993) (non-union truck driver who complained to a supervisor about the maintenance of trucks and sick pay was not protected because he expressed only a personal complaint).
73. See, e.g., NLRB v. City Disposal Sys., 465 U.S. 822, 823 (1984) (“The NLRB reasonably concluded that Brown’s honest and reasonable assertion of his right to be free of the obligation to drive unsafe trucks, even though he did not explicitly refer to the collective-bargaining agreement when he refused to drive the truck, constituted concerted activity within the meaning of § 7.”); Interboro Contractors, Inc., 157 N.L.R.B. 1295, 1298 (1966) (“[E]ven if the complaints were made by John alone, they still constituted protected activity since they were made in the attempt to enforce the provisions of the existing collective bargaining agreement.”). See generally Richard Michael Fischl, Self, Others, and Section 7: Mutualism and Protected Protest Activities Under the National Labor Relations Act, 89 COLUM. L. REV. 789, 816 (1989) (discussing the requirement of “concert” and the relationship between the individual protest and those that come to aid the individual’s protest, often termed the “promise of reciprocal benefit”).
74. Gorman & Finkin, supra note 71, at 290.
75. Id. at 290–93 (documenting numerous cases supporting the proposition that:
the prevailing principle of law—endorsed both by the courts of appeals and the NLRB—is that
section 7 does not protect ‘personal gripe’ by individual employees. If an individual complains
to management about working conditions affecting him alone, this will be treated as individual
rather than concerted activity, and the employee will not be protected against discharge.)
Gorman and Finkin suggest a broader reading of “concerted activity” based on the legislative history of the NLRA. They suggest that
the history of the language of section 7 and an examination of the policy it was designed to
effect suggest a far more expansive reading—one that encompasses the individual’s right to
complain and to act in his own self-interest. It is anomalous to read the Act to provide that an
individual who protests of mistreatment can be summarily fired unless he is accompanied by a
fellow worker making the same complaint. It is even more anomalous that a letter written by an
individual worker to a supervisor should render him subject to discharge while a disruptive mass
This rationale has been justified by the Board on two grounds: (1) an individual employee’s actions to enforce the collective bargaining agreement are an extension or manifestation of the concerted action that produced the agreement and (2) the individual’s assertion of a right under a collective bargaining agreement will be assumed to affect the rights of all employees covered under the agreement. Under this logic of “constructive concert” of action, the Board and the courts have created a broad definition of concerted action ranging from speech that is a “logical outgrowth” of previous group activity, to independent action not preceded by any group discussion or agreement and not characterized as protest.

While concert of action may be superficially simple to determine (i.e., more than one person), “for mutual aid and protection” necessitates an inquiry into intentions and has proved more difficult to define. “Mutual aid and protection” is “understood to be roughly equivalent to the goal of affecting ‘terms and conditions of employment,’ a phrase which is found at several vital points in the National Labor Relations Act.” In Eastex, the Supreme Court gave a broad construction to the “mutual aid or protection” clause. The Court held that the phrase “terms and conditions of employment” embraced union leafleting urging employees to protest incorporation of a state “right to work” statute into the state constitution and a presidential veto of an increase in work stoppage in the midst of the workday should be protected. Such anomalies could be tolerated if it were clearly the will of the legislature; but the policy of the Act is to ensure the liberty and dignity of the individual working person.

---

Id. at 344.

77. Interboro Contractors, Inc., 157 N.L.R.B. 1295, 1298 (1966) (“We believe that the General Counsel proved a prima facie case of unlawful discharge by showing that the discharged employees had made complaints about working conditions which were a protected concerted activity . . . .”).
78. Gorman & Finkin, supra note 71, at 293–303 (discussing “constructive concert” in the context of union and non-union employees). Gorman and Finkin summarize the constructive theory as applied by the Board and courts:

An individual complaint is said to have been made “on behalf of” a group of workers not because the complainant has been delegated to speak but rather because rectification of his grievances will inure to the benefit of others. Others will also benefit whenever an individual asserts a claim which can plausibly (even if after the fact) be linked to a collective bargaining agreement. Even in the absence of such an agreement, group benefit is presumed to flow from claims concerning safety and health, or from claims which find their source in any statute or public regulations. Through the accumulation of these fictions and presumptions, the Board has accorded “protected concerted” status to the great majority of individual complaints (sometimes accompanied by a refusal to work) about conditions in the workplace. Yet the Board continues to cling to the notion that certain such complaints are merely “personal gripes,” and continues to place specific factual situations into that category with little apparent consistency, a most unfortunate failing given the fact that fundamental rights of employers and employees are in the balance.

Id. at 309.
79. See Every Woman’s Place, Inc., 282 N.L.R.B. 413, 413 (1986) (holding that an employee’s independent action was concerted because she and coworkers had already met and discussed related workplace issues and brought concerns to the employer).
80. See NLRB v. Mike Yurosek & Son, Inc., 53 F.3d 261, 263–65 (9th Cir. 1995) (involving four individuals who individually refused to work overtime without previously discussing their actions with each other or characterizing their refusal as protest; nonetheless, their activities were “concerted” because they implied a common goal).
81. Gorman & Finkin, supra note 71, at 289 (citing 29 U.S.C. §§ 151, 152(9), 158(d), 159(a) (1976)).
82. Id.
the federal minimum wage. In the course of its decision, the Court equated activity for “mutual aid or protection” with activity “to improve terms and conditions of employment or otherwise improve [the] lot” of the employees. Moreover, the Court ruled that the clause encompasses employee assistance of another employer’s employees (including honoring a picket line and distributing literature or demonstrating in support of another employer’s employees) as well as general employee action to improve working conditions or terms, provided the speech or action is connected to a tangible workplace issue.

This requirement of relating to an actual workplace dispute has proved to be one of the more salient features of Eastex. The Board and other courts have gone on to define the parameters of “mutual aid and protection” to include speech relating to uncommon concerns (e.g., posting a sign and alerting news media that a mysterious illness was afflicting workers) as well as more common concerns (e.g., wages, hours, and working conditions).

The importance of Section 7 as a means for securing employee rights cannot be overstated. As the NLRB begins confronting novel issues stemming from modern technologies, Section 7 must adapt to these changes. As will be seen from the case analysis below, Section 7 is central to understanding how a BYOD program would interface with the NLRA.

III. ANALYSIS

There are three labor concerns that this Note will deal with in the context of BYOD: first, how BYOD policies interface with employee’s Section 7 rights following Register-Guard; second, how employer actions unique to BYOD programs can create an improper impression of surveillance that chills employee’s Section 7 rights; and third, whether or not a BYOD program is a mandatory bargaining subject of a collective bargaining agreement.

A. The Register-Guard Decision

1. Background

Union employee’s Section 7 rights were implicated directly in a case dealing with an employee’s use of an employer’s computer and email system. The case, Register-Guard, is a useful introduction to how the Board has adapted to new technologies in the workplace and serves as a springboard for anticipating how the Board might approach the tension between a BYOD

84. Id. at 565.
85. Id. at 569–70.
86. See, e.g., Martin Marietta Corp., 293 N.L.R.B. 719, 724 (1989) (involving employees who agreed to embark on a public campaign to disclose recent outbreaks of a mysterious illness, carried through by posting notice inviting other employees to talk about the illness on television; the actions were held to be protected activity).
87. See generally The Developing Labor Law 83 (John E. Higgins, Jr. ed., 5th ed. 2006) (discussing examples in concluding the definition of “for mutual aid and protection” is broad).
program and the protections under the NLRA.

The Register-Guard, a daily newspaper in Eugene, Oregon, had a Communication Systems Policy (CSP) governing the use of communication systems, including email.\textsuperscript{88} The CSP provided that:

Company communication systems and the equipment used to operate the communication systems are owned and provided by the company to assist in conducting the business of The Register-Guard. Communication systems are not to be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.\textsuperscript{89}

Approximately 150 of the company’s employees constituted a unit represented by the Eugene Newspaper Guild, CWA Local 37194, AFL-CIO.\textsuperscript{90} The union president, Suzi Prozanski, was a copy editor in the newspaper’s features department.\textsuperscript{91} On May 4, 2000, Prozanski sent an email to other employees, through the employer’s communication system, concerning a union rally held the previous week.\textsuperscript{92} The next day, Prozanski received a disciplinary warning from the managing editor for violation of the CSP.\textsuperscript{93}

In August 2000, Prozanski sent employees two more emails, both dealing with upcoming union events.\textsuperscript{94} On August 22, Cynthia Walden, the Register-Guard’s director of human relations, sent Prozanski another disciplinary warning for violation of the CSP.\textsuperscript{95} Based on these warnings, the union filed an unfair labor practice charge with the Board.\textsuperscript{96} The union alleged both that the Register-Guard violated Sections 8(a)(1) and 8(a)(3) of the NLRA in its maintenance and enforcement of an overbroad no-solicitation policy and that the Register-Guard discriminatorily enforced its policy against Ms. Prozanski because her email regarded union matters.\textsuperscript{97} Moreover, since the CSP explicitly prohibited employees from using email “to solicit,” the union argued that Ms. Prozanski’s email was not a solicitation and thus not a violation of the CSP.\textsuperscript{98}

Since the Register-Guard CSP, like many employer communication policies, specifically prohibited solicitation,\textsuperscript{99} understanding the difference between solicitation and distribution is critical to determining whether a workplace CSP has in fact been violated. Solicitation is generally defined as “[t]he act or an instance of requesting or seeking to obtain something; a request or a petition.”\textsuperscript{100} By definition, solicitation seeks a response while distribution

\textsuperscript{88} Register-Guard I, supra note 13, at 1111.
\textsuperscript{89} Id.
\textsuperscript{90} Id.
\textsuperscript{91} Id.
\textsuperscript{92} Id.
\textsuperscript{93} Id.
\textsuperscript{94} Id. at 1112.
\textsuperscript{95} Id.
\textsuperscript{96} Id.
\textsuperscript{97} Id.
\textsuperscript{98} Id.
\textsuperscript{99} Id. at 1111.
\textsuperscript{100} BLACK’S LAW DICTIONARY 1427 (8th ed. 2004).
seeks to convey material to another without requiring a reply.\footnote{\textit{Shorter Oxford English Dictionary}, supra note 69, at 426, 1249 (defining “distribution” as “the giving out or division among a number,” and “solicitation” as “asking; enticing; urgent request”); see also Allegra Kirsten Weiner, \textit{Business-Only E-mail in the Labor Organizing Context: It is Time to Recognize Employee and Employer Rights}, 52 \textit{Fed. Comm. L.J.} 777, 780–81 (2000) (internal citations omitted) (explaining that “solicitation normally involves oral communications between workers regarding organizing,” and “distribution . . . normally involves the circulation of written union literature by an employee”).} Put differently, solicitation is an attempt to engage in a two-way exchange: the initiating party’s purpose is to garner a response from the targeted party; however, a distribution is a one-way track with no intention of exchange. Email adds a layer of complexity to this distinction since email can be viewed as a hybrid of solicitation and distribution: when an email simply states information and is communicated from a sender to a recipient it resembles distribution, but when it encourages action or dialogue it is more akin to solicitation.\footnote{See Elena N. Broder, \textit{(Net)workers’ Rights: The NLRA and Employee Electronic Communications}, 105 \textit{Yale L.J.} 1639, 1661 (1996) (discussing that the decision to classify emails as either speech or distribution has no clear answer); Andrew F. Hettinga, \textit{Note, Expanding NLRA Protection of Employee Organizational Blogs: Non-Discriminatory Access and the Forum-Based Disloyalty Exception}, 82 \textit{Chi. Kent L. Rev.} 997, 1008 (2007) (explaining that emails are a hybrid between distribution and solicitation).} Often times, an email does both of these things simultaneously. This distinction between solicitation and distribution is important context for understanding the Board’s decision.

2. \textit{Arguments of the Parties and Amici Before the Board}

The General Counsel for the Board argued that the features and functions of email do not allow for it to be characterized as either “solicitation” or “distribution.”\footnote{\textit{Register-Guard I}, supra note 13, at 1112.} Moreover, the General Counsel distinguished email systems from other forms of equipment the Board previously considered (e.g., telephones, bulletin boards, etc.) “on the basis that those cases did not involve interactive, electronic communications regularly used by employees, nor did they involve equipment used on networks where thousands of communications occur simultaneously.”\footnote{\textit{Id.} at 1112–13.} The National Employment Lawyers Association (NELA) filed a brief concurring with the General Counsel, wherein NELA argued that employer email systems are analogous to lunchrooms and break rooms, and, as such, an attempt to limit employee communications during nonwork time would contravene \textit{Republic Aviation}.\footnote{\textit{Id.} at 1113. In \textit{Republic Aviation Corp. v. NLRB}, 324 U.S. 793, 794–95 (1945), the employer had a broad no solicitation rule prohibiting solicitation of any kind on the employer’s property. One employee was discharged for soliciting union membership during lunch periods and three other employees were discharged for wearing union steward buttons in the workplace. \textit{Id.} at 795. The Supreme Court affirmed the Board’s ruling that, in pertinent part, the employer’s no solicitation rule interfered with employees’ rights under Section 8 of the NLRA. \textit{Id.} at 805.} The National Workrights Institute also filed a brief noting that email is the predominant means of business communication in the workplace and that most employer email communications policies are so vague as to chill employee Section 7 communications.\footnote{\textit{Register-Guard I}, supra note 13, at 1113.}
In defense of their CSP, the Register-Guard argued that (1) employees have no Section 7 right to use the employer’s email system, (2) the email system is inextricable from the computer system, which the employer owns, and (3) the case was distinguishable from Republic Aviation and its progeny because those cases dealt with oral solicitation rather than employer equipment.\footnote{Register-Guard I, supra note 13, at 1110.}

3. *The Board’s Opinion*

As discussed above, the Board was presented with a number of issues for consideration. However, the issue most pertinent to this Note was whether the CSP violated Section 8(a)(1) of the NLRA\footnote{29 U.S.C. § 158(a)(1) (2012) (“It shall be an unfair labor practice for an employer to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed [in Section 7] of this title.”).} as being an overly broad no-solicitation policy. The Board (in a 3-2 decision) held that the employees had no statutory right to use the employer’s email system for Section 7 matters.\footnote{Register-Guard I, supra note 13, at 1110.} The Board’s rationale was that an employer has certain basic property rights and can thus regulate and restrict employee use of company property, provided the employer does so on a non-discriminatory basis.\footnote{Id. at 1114.} Perhaps most significant, the Board held that “use of e-mail has not changed the pattern of industrial life at the Respondent’s facility to the extent that the forms of workplace communication sanctioned in Republic Aviation have been rendered useless . . . .”\footnote{Id. at 1116.}

Contrarily, the two dissenting Board members read Republic Aviation\footnote{Republic Aviation Corp. v. NLRB, 324 U.S. 793, 803 n.10 (1945) (noting that although an employer may make and enforce “reasonable rules” covering the conduct of employees on working time, “time outside working hours . . . is an employee’s time to use as he wishes without unreasonable restraint, although the employee is on company property”) (emphasis added).} as requiring a balancing of an employee’s Section 7 right to communicate with the employer’s right to protect its business interests (i.e., maintenance of production and discipline).\footnote{Register-Guard I, supra note 13, at 1125 n.6 (Liebman & Walsh, Members, dissenting).} As such, the dissent noted that “[n]o restriction may be placed on the employees’ right to discuss self-organization among themselves, unless the employer can demonstrate that a restriction is necessary to maintain production or discipline.”\footnote{Id. at 1124 (Liebman & Walsh, Members, dissenting).} Most importantly, the dissent found that email has dramatically changed the way people communicate at work and, as such, “it is simply absurd to find an email system analogous to a telephone, a television set, a bulletin board, or a slip of scrap paper.”\footnote{Id. at 1125 (Liebman & Walsh, Members, dissenting).} Such equipment is finite and consequently only a limited number of people can post on a bulletin board, and only one person can use the phone at a time (excepting modern innovations such as conference calling).\footnote{Id.} However, a potentially infinite number of people can use one email system at the same time without

\begin{itemize}
\item \footnote{Id.}
\item \footnote{Id. at 1152 (Liebman & Walsh, Members, dissenting).}
\item \footnote{Register-Guard I, supra note 13, at 1125 n.6 (Liebman & Walsh, Members, dissenting).}
\item \footnote{Id. at 1124 (Liebman & Walsh, Members, dissenting).}
\end{itemize}
impairing the employer’s interest in production and discipline.\textsuperscript{117} The dissent would have employed the rule “that banning all nonwork-related ‘solicitations’ is presumptively unlawful absent special circumstances.”\textsuperscript{118} Under this rebuttable presumption, given that Register-Guard showed no special circumstances for its ban, the dissent would have found a violation of Section 8(a)(1).\textsuperscript{119}

The difference between the majority and dissenting opinions has important implications for BYOD programs. The Register-Guard majority decision provides employers with broad latitude to control and regulate their property interests provided such regulation is not facially discriminatory.\textsuperscript{120} Moreover, the majority did not distinguish between solicitation and distribution.\textsuperscript{121} In contrast, the dissent would have applied the Republic Aviation balancing test, thus requiring a legitimate business reason for a CSP that prohibits Section 7 communications.\textsuperscript{122} Perhaps most importantly, the dissent viewed email as a wholly different medium of communication than bulletin boards, telephones, and the like.\textsuperscript{123} As such, the dissent would have had the Board adapt to the change in communication technologies by updating the interpretation of the NLRA to encompass the new “water cooler” around which employees gather to communicate.\textsuperscript{124}

The Board’s decision was appealed to the Court of Appeals for the District of Columbia, but the union did not challenge the lawfulness of the company’s CSP.\textsuperscript{125} As such, the Court of Appeals only examined whether the CSP was applied in a discriminatory manner and whether Register-Guard committed an unfair labor practice.\textsuperscript{126} While the Court of Appeals’ decision allows employers to continue applying a neutral ban on personal email use that includes union solicitations, it is likely that the newly constituted Obama Board will review the issue.\textsuperscript{127} At least one commentator speculates that “given the NLRB’s current political make-up, it is likely that the Board will find a neutral ban to be presumptively unlawful.”\textsuperscript{128} Indeed, the political makeup of each iteration of the Board often dictates Board rulings, regardless of precedent and regardless of the principles of the Act. Register-Guard is a

\textsuperscript{117} Id.
\textsuperscript{118} Id. at 1127 (Liebman & Walsh, Members, dissenting).
\textsuperscript{119} Id.
\textsuperscript{120} Id. at 1116.
\textsuperscript{121} Hettinga, supra note 102, at 1008 (stating that, indeed, “the Board has not decided whether employee organizational speech sent via email is distribution or solicitation.”).
\textsuperscript{122} Register-Guard I, supra note 13, at 1127 (Liebman & Walsh, Members, dissenting).
\textsuperscript{123} Id. at 1125–26 (Liebman & Walsh, Members, dissenting).
\textsuperscript{124} Id. at 1125 (Liebman & Walsh, Members, dissenting).
\textsuperscript{125} In the union’s view, while the Board’s decision on the validity of the company’s policy was wrong, the union deemed that decision to be a policy choice within the Board’s discretion that the appellate court was unlikely to overturn. See Susan J. McGolrick, Unfair Labor Practices: D.C. Circuit Rules Guard Publishing Illegally Disciplined Copy Editor for E-mails, 7 WORKPLACE L. REP. (BNA) NO. 959 (July 10, 2009) (evaluating the case history and validity of the board’s ruling).
\textsuperscript{126} Guard Publ’g Co. v. NLRB, 571 F.3d 53, 59 (D.C. Cir. 2009).
\textsuperscript{127} Jonathan C. Wilson, Labor & Employment Law Update, 50 ADVOC. (TEX.) 1, 11 (2010); see also, infra section III.A.5.
\textsuperscript{128} Id.
strong example of this politically driven decision-making process.

4. The Politicization of the Board

The politicization of the Board has always drawn criticism, but since 2004 the Board’s political make-up has become more galvanizing. Board decisions in the last ten years have “elicited sharp disapproval from legal academics as well as unions.” Instead of adapting the Act to modern circumstances “by encouraging the practice and procedure of collective bargaining and . . . protecting . . . workers’ . . . full freedom of association” the Board has undermined a range of employee protections including some that seemed well-established under prior decisions. On a broader scale, the labor movement in the past decade has criticized the Board and its accompanying legal regime as obstacles to fulfilling the purposes of the Act.

Originally, the Board was conceived of as a non-partisan body: “[w]hen Congress established the NLRB in 1935, it considered a tripartite structure consisting of representatives from industry, labor, and government, but chose instead a ‘strictly nonpartisan’ Board composed of ‘three impartial government members.’” The initial impartiality of the Board’s members was maintained for quite some time: “Presidents Roosevelt and Truman acted consistently with Congress’s intent, drawing their Board appointees primarily from government service and secondarily from academia. Of the fourteen individuals who joined the Board between 1935 and 1952, only one came from either the labor or management sectors.” However, beginning with President Eisenhower, this conscious attempt to appoint impartial Board members was exponentially eroded: two of Eisenhower’s early Board appointees had strong roots in the management sector. “During the nearly three decades from 1953 to 1980, roughly one-half the Board members appointed by Republican Presidents came from the management sector. By contrast, Democratic Presidents Kennedy, Johnson, and Carter continued to draw all their Board appointments from government service or academia.” It might be argued that a partisan-appointment does not necessarily result in partisan-minded decision-making. However, the response to such an argument is that “appointees selected from the management bar would effectively use service on the Board to enhance their partisan status in subsequent career moves.”

130. Id. at 226.
132. Id.
133. Id. at 243–44.
134. Id. at 245.
135. Id.
136. Id.
137. Id. at 246.
management positions returned straight to management representation upon leaving the Board.”

The concern about partisan appointments and decision-making came to fruition in the Reagan administration. Reagan’s appointees were “not establishment-type management representatives with a basic commitment to the NLRA’s purposes and processes.”

“Rather, they were apostles for union avoidance, with professional backgrounds and philosophies that questioned or challenged the agency’s traditional approach to applying the Act.” As James Brudney points out, while “the Nixon-Ford Board of 1975–76 and the Carter Board of 1979–80 each had upheld complaints filed against employers about 84% of the time . . . the Reagan Board upheld only 52% of the nearly 800 unfair labor practice complaints brought against employers—a decline of roughly two-fifths in the General Counsel’s success rate.” Reagan’s politicization of the Board was the first of many Republican attempts to turn the Board into an anti-union tool; however, Democratic presidents also attempted to appoint pro-union members just as often. Thus, it should come as no surprise that the Board majority, as constructed by President George W. Bush, took up a decidedly anti-union position:

Since the start of 2004, the [Bush] Board has issued a remarkable series of decisions weakening the rights of workers to engage in organizing and collective bargaining under the National Labor Relations Act (“NLRA” or “Act”). These decisions invariably have been authored by appointees of President Bush and typically have been accompanied by an angry or despairing dissent. In the aggregate, they have limited the Act’s coverage over numerous distinct groups of employees, restricted the basic right of workers to engage in “concerted activities for the purpose of . . . mutual aid or protection,” and substantially augmented the ability of employers to interfere with or intimidate employees who seek to organize or to bargain collectively. Many of the Board’s decisions have overruled or disregarded prior precedent. The Board also has invited review in two additional cases that suggest it may be prepared to abandon its decades-old commitment to principles of voluntary recognition.

As such, when the Bush Board decided Register-Guard in a manner that elevated supposed employer-rights by using antiquated concepts of the workplace and ignoring prior Board precedent, it no doubt came as little surprise to experienced Board observers. However, the Bush Board has proved to be one of the more isolated and politicized iterations of the Board: the Bush Board “has been roundly criticized from within its own ranks for refusing to

138. Id.
139. Id.
140. Id. at 248.
141. Id.
142. Id. at 248–50 (noting also that President Clinton, who took office after twelve years of Republican control, appointed “three experienced union-side attorneys” as well as “three experienced management attorneys,” during his eight years in office).
143. Id. at 221–22.
examine the practical consequences of Clinton-era decisions before overturning them, for failing to engage the arguments advanced in dissenting opinions, and for overruling precedent without first seeking input from the interested communities through amicus briefs.”

As each political party seeks to control the composition of the Board, the see-saw effect only becomes more apparent and the reputation of the Board because increasingly denigrated. With the election of President Obama, many anticipated the Board to be comprised of pro-union appointees and to begin overturning many of the Bush Board’s decisions. In fact, in 2014 the Obama Board took up *Purple Communications, Inc. and Communications Workers of America, AFL-CIO* with the express purpose of considering the viability of *Register-Guard*.

5. **Purple Communications**

In *Purple Communications*, the employer maintained a rule prohibiting the use of company equipment including computers, Internet, and email systems for anything other than business purposes. The rule also specifically prohibited the use of that equipment for “engaging in activities on behalf of organizations or persons with no professional or business affiliation with the company.” The General Counsel argued that this policy was overly-broad and interfered with employees’ exercise of Section 7 rights in violation of Section 8(a)(1). However, the General Counsel also conceded that finding a violation would require overruling the Board’s decision in *Register-Guard*. The Administrative Law Judge (ALJ) noted that “[i]f the General Counsel’s arguments in favor of overruling *Register-Guard* have merits, those merits are for the Board to consider, not me.” As such, the ALJ dismissed the allegation.

On April 30, 2014, the Board solicited the parties and interested amici to file briefs addressing issues related to whether the Board should overrule the holding in *Register-Guard* that “employees have no statutory right to use the employer’s email system for Section 7 purposes.”

---

144. Id. at 250.
146. Id.
148. Id.
149. Id.
150. Id.
151. Id.
152. Id.
153. *Register-Guard I*, supra note 13, at 1115. Specifically, the Board asked the following questions: (1) Should the Board reconsider its conclusion in Register Guard that employees do not have a statutory right to use their employer’s email system (or other electronic communications systems) for Section 7 purposes? (2) If the Board overrules Register Guard, what standard(s) of employee access to the employer’s electronic communications systems should be established? What restrictions, if any,
In its brief, the General Counsel sided with the dissenting members of Register-Guard, arguing that “[t]he Board should overrule Register-Guard and apply the framework set forth in Republic Aviation to balance employees’ Section 7 right to communicate with each other in workplaces that utilize electronic communications systems and employers’ management interests in maintaining production and discipline.”\textsuperscript{154} The General Counsel went on to argue that, “specifically, the Board should hold that employees who use their employer’s electronic communications systems to perform their work have a statutory right to use those systems for Section 7 purposes during nonwork time, absent a showing of special circumstances relating to the employer’s need to maintain production and discipline,”\textsuperscript{155}

The General Counsel also argued that the Bush Board ignored two basic labor law principles—“employees’ right to communicate with each other and the right to do so at work”—and mischaracterized email as equipment and placed misguided emphasis on the so-called “equipment” cases.\textsuperscript{156} Most notably, the General Counsel argued that, contrary to what the Register-Guard majority stated, email and telework have fundamentally changed the dynamics of the workplace and email is often the natural way to communicate and self-organize.\textsuperscript{157} To this end, and related to BYOD, the General Counsel argued that

the fact that employees in technological workplaces may have personal electronic devices, social media accounts, or personal email accounts does not diminish their Section 7 right to engage in electronic communication on the employer’s systems any more than the fact that the employees in Republic Aviation could speak by telephone or meet off the premises diminished their right to engage in solicitation at the plant.\textsuperscript{158}

While Purple Communications did not submit a supplemental brief in response to the Board’s Notice and Invitation to File Briefs, various employer-side amici did file supplemental briefs. In summary, the employer-side amici acknowledged the prevalence of email and the change in our modern workplace reality, but nonetheless argued that “an employer may maintain and

\begin{itemize}
\item may an employer place on such access, and what factors are relevant to such restrictions?
\item In deciding the above questions, to what extent and how should the impact on the employer of employees’ use of an employer’s electronic communications technology affect the issue?
\item Do employee personal electronic devices (e.g., phones, tablets), social media accounts, and/or personal email accounts affect the proper balance to be struck between employers’ rights and employees’ Section 7 rights to communicate about work-related matters? If so, how?
\item Identify any other technological issues concerning email or other electronic communications systems that the Board should consider in answering the foregoing questions, including any relevant changes that may have occurred in electronic communications technology since Register Guard was decided. How should these affect the Board’s decision?
\end{itemize}


154. Id. at 1.
155. Id.
156. Id. at 7, 9.
157. Id. at 10–14.
158. Id. at 21.
enforce a policy that allows for limited or incidental personal use of the email system . . . without allowing the system to be used for solicitation on behalf of outside organizations or purposes[,] including unions. 159

Given the aforementioned politicization of the Board, and the fact that the Obama Board is more union/employee-friendly than the Bush Board, it is likely that the Obama Board will overrule Register-Guard. Additionally, as the General Counsel and the dissenting Board members of Register-Guard have urged, the Board will likely return to Republic Aviation as the standard for balancing an employer’s property rights and business interests with an employee’s right to communicate for the purpose of self-organization. 160

6. Applying Register-Guard to BYOD

Since Purple Communications has not yet ruled on the continued validity of Register-Guard, Register-Guard remains the governing law. However, the Board’s ruling that employees have no statutory right to use an employer’s email system for Section 7 activity is fundamentally flawed for three reasons.

First, the Board majority applied an antiquated notion of workplaces and work time. The previous paradigm was that employees arrive at the workplace for a set period of time and during that time use employer-owned property. While this model may have dominated the early part of the 20th century when factories and plants were the more common blue-collar workplace, this model is no longer predominant. 161 Many workplaces are now mobile, with employees working outside of the employer’s business site, and a growing number of workplaces are entirely electronic. 162 Moreover, many employers allow employees to work remotely. Currently, eighty-eight percent of surveyed businesses worldwide offer some form of telework to their employees, and twenty-three percent of surveyed employees work at least some hours at home on an average workday. 163 In addition to formal telework


160. On September 24, 2014 the Board ruled on Purple Communications but the Board decided to “sever and hold for further consideration the question whether Purple’s electronic communications policy was unlawful.” Purple Commc’ns, Inc. Nos. 21-CA-095151, 21-RC-091531, and 21-RC-091584 (2014), available at http://www.nlrb.gov/case/21-CA-095151. At the time of printing, the Board has yet to decide the severed issue and Register-Guard remains the governing rule.

161. See Jeffrey M. Hirsch, The Silicon Bullet: Will the Internet Kill the NLRA?, 76 GEO. WASH. L. REV. 101, 125–26 (2008) (arguing that the manufacturing model of separate work area and break area is no longer the dominant model and the Board’s attempt to follow the same rules, in modern workplaces, is not meaningful or workable and will impede employee exercise of statutory rights); see also Nancy J. King, Labor Law for Managers of Non-Union Employees in Traditional and Cyber Workplaces, 40 AM. BUS. L.J. 827, 870–72 (2003) (“The NLRB should extend the rules on solicitation and distribution that protect employees’ Section 7 rights in the brick and mortar world and the balance of employee and employer rights that has been fashioned for that world to the cyber workplace.”).

162. See King, supra note 161, at 839 (discussing the differences between traditional and cyber workplaces).

163. See SURVEY ON WORKPLACE FLEXIBILITY 2013, WORLDATWORK (October 2013), http://www.worldatwork.org/waw/adminlink?id=73898 (illustrating the prevalence of flexible work arrangements offered by businesses); BUREAU OF LABOR STATISTICS, USDL 13-1178, AMERICAN TIME USE SURVEY-2012 RESULTS (June 20, 2013), available at http://www.bls.gov/news.release/atus.nr0.htm (showing
programs, the prevalence of electronic communications technology has increased the amount of time employees informally work outside of their physical offices and core business hours. For instance, a 2008 study showed that fifty percent of employed email users checked their work email on the weekends, and twenty-two percent did so “often.”\textsuperscript{164} Thirty-four percent of employees checked their work email while on vacation (eleven percent did so “often”) and forty-six percent of employees checked their work email while on sick leave (twenty-five percent checked “often”).\textsuperscript{165} This rise of both formal and informal telework amplifies the importance of electronic communication with respect to the effective exercise of Section 7 rights.

Second, the Board’s understanding of employer’s property rights regarding an email system does not account for modern email usage and ownership. The Board analogized email systems to telephones, a television set, a bulletin board, and a piece of paper to arrive at the conclusion that an employer can validly place non-discriminatory restrictions on employer-owned equipment and property.\textsuperscript{166} However, as the dissent noted, an email system is categorically and fundamentally different from any other employer-owned equipment.\textsuperscript{167} A bulletin board, for example, has finite parameters and thus use of a bulletin board by an employee will deprive others of that space. An email system has limited space as well, but does not suffer from the same usage concerns. In Register-Guard, the employer’s email system was receiving some 4000 email messages per day.\textsuperscript{168} No single bulletin board could possibly contain so much material. Moreover, an email system is designed to accommodate simultaneous messaging, while a telephone, for example, can only accommodate one message at a time. Thus, it would be fallacious to assert that an email system is similar to other forms of employer property. Moreover, such reasoning conflicts with at least one previous Board precedent.\textsuperscript{169}

Third, the Board incorrectly presumed that the employer has a basic property right to regulate employer-owned property.\textsuperscript{170} This apparent right should not trump employees’ ability to communicate with one another regarding self-organization absent a particularized showing that specific management interests relating to production or discipline outweigh the employees’ Section 7 right to use the system on their non-work time. Indeed, as the General Counsel recently declared, “it is axiomatic that without free

\textsuperscript{164} See Madden & Jones, \textit{supra} note 10, at 4–5 (displaying the number of employed Americans surveyed who said they checked their work-related emails on the weekends).

\textsuperscript{165} \textit{Id.} at 5.

\textsuperscript{166} Register-Guard I, \textit{supra} note 13, at 1125 (Liebman and Walsh, Members, dissenting).

\textsuperscript{167} \textit{Id.} (Liebman and Walsh, Members, dissenting).

\textsuperscript{168} \textit{Id.} (Liebman and Walsh, Members, dissenting).

\textsuperscript{169} In Timekeeping Sys., Inc., 323 N.L.R.B. 30, 249 (1997), the Board likened an employee’s email message to distribution cases where employees left pamphlets on co-worker’s desks to be discovered the next morning during working hours since it “could not have taken Respondent’s employees more than a few minutes to digest,” and therefore it could not have amounted to substantial disruption.

\textsuperscript{170} Register-Guard I, \textit{supra} note 13, at 1115–16.
discourse, there can be no collective action.”¹⁷¹ Indeed, employees’ ability to access information and communicate with each other is vital to their ability to have “full freedom of association, self-organization, and designation of representatives of their own choosing.”¹⁷² Moreover, the Supreme Court has long recognized that employees’ right to self-organize and bargain collectively “necessarily encompasses the right effectively to communicate with one another regarding self-organization at the jobsite.”¹⁷³ Thus, any “right” of the employer to control employees’ communication in the workplace must be balanced against the employees’ statutory right to communicate with one another on the jobsite.

Even assuming that an employer does possess this property right, the assumption that the employer owned the email account cannot be so simply relied upon. While one would hardly contest that the employer has a property right to control the use of the physical computers and hardware it owns, an email account is software and suffers from a less intuitive understanding of ownership. An email system cannot qualify as a traditional piece of “equipment.” Additionally, an email system is often not stored on an employer’s real property and in many instances the employer does not even manage or control the email system. For example, while an employer’s communications system might send and receive information on its bandwidth, many employers have external companies that provide server space, manage the email system, and respond to system problems.¹⁷⁴ Even assuming that the employer does “own” the workplace email accounts, it is unclear how the employer property right averred in Register-Guard would apply if the communications were completed using personal email accounts and servers (i.e., employee A sends employee B an email and both employees are using a Gmail account).

The Board’s reliance on the employer’s property right in Register-Guard means that the employer must own the property—whether it is an email system or a piece of equipment—for the rule to apply. In any BYOD program, the ownership question is blurred. Recall that there are two basic types of device programs: BYOD and COPE. Under a BYOD program, the employee purchases the device and pays for all of, or most of, the costs associated with the device. Under a COPE program, the company owns the device and pays for all of, or most of, the costs associated with the device. The company allows the employee to install apps, music, video, and the like, and to use a non-work portion for personal purposes.

The question in light of Register-Guard is: who owns a BYOD or COPE device? It would seem that the employee owns a BYOD device and an employer owns a COPE device. However, a BYOD device is often used for

¹⁷² Id. at 1101–02.
¹⁷³ Beth Israel Hosp. v. NLRB, 437 U.S. 483, 491 (1978) (citing Republic Aviation Corp. v. NLRB, 324 U.S. 793 (1945)).
¹⁷⁴ Weiner supra note 101, at 787.
work purposes during work time, and in work areas, opening up employee usage to employer monitoring and valid no-solicitation policies. Ownership of a device will generally carry with it expectations of privacy and control, but given the type of usage just mentioned, at least some of those expectations may be misplaced. Moreover, if the employee sends a protected communication, from a personal email account to another personal email account, but the email is sent over an employer owned network, it is unclear from Register-Guard how the employee’s and the employer’s ownership and statutory rights would interface. These nuances cannot be adequately resolved under the simplistic reasoning of Register-Guard. A COPE program suffers a similarly dissatisfying conclusion. While it would seem that a COPE device is employer-owned, the employer has intentionally given actual possession, i.e., direct physical control, of the device to the employee for the purpose of having him do some act for the employer. Moreover, while the company retains control over a COPE device, employees are generally authorized to use the device for personal activities, such as sending emails. Thus, if an employee on a COPE device sent a protected communication to another employee, it is unclear how the logic and rule of Register-Guard would apply.

Both types of programs are rife with potential NLRA issues and the standard set forth in Register Guard, based on employer property rights, provides no assistance in understanding how employees can exercise their Section 7 rights without impediment or fear of reprisal, or understanding how employers can manage their “property” and ensure their legitimate business interests within such a technologized workplace.

B. Employer Monitoring of BYOD Devices

Many employers monitor the electronic communications and Internet activity of their employees. A 2007 study estimated that forty-three percent of employers were actively monitoring their employees’ Internet uses. Employers have a variety of substantive reasons for monitoring employees’ electronic activity. Most monitoring focuses on tracking incoming and outgoing email messages, both on company email servers and on personal email servers accessed through the employer’s network. With a BYOD policy in place, the employer can install applications and interfaces on the device that track not only emails but texts, phone calls, downloads, and

---

175. 63 AM. JUR. 2D Property § 30 (2014).
177. Id. at 1.
178. See Matthew W. Finkin, Privacy in Employment Law 354 (3d ed. 2009) (noting five reasons why employers monitor employee email and internet access); see also Jeffrey A. Mello, Social Media, Employee Privacy, and Concerted Activity: Brave New World or Big Brother?, 63 LAB. L.J. 165, 166 (2012) (describing reasons employers have for monitoring employee electronic communication, such as protection from legal liabilities that could result from such communication).
browser history.\textsuperscript{180} The expansive nature of such monitoring would appear to be rife with concerns regarding employee privacy rights. However, employee privacy rights—at least in the private sector—are limited and piecemeal.\textsuperscript{181} As one scholar has noted, “[n]o comprehensive statutory scheme supplements the common law to provide protection for employees’ privacy or even simply from employer monitoring. Instead, a variety of federal and state laws offer only targeted and limited protections.”\textsuperscript{182} While not well-adapted to modern technologies, the NLRA covers private employees and has historically protected against some employer monitoring.\textsuperscript{183}

Employer surveillance or electronic monitoring typically implicates Section 8(a)(1). Section 8(a)(1) of the NLRA states that “[i]t shall be an unfair labor practice for an employer . . . to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in Section 7 . . . .”\textsuperscript{184} “Placing employees under surveillance for activity protected under the NLRA or creating the impression of surveillance is an unfair labor practice violative of the Act.”\textsuperscript{185} While passive or incidental observation of protected union activity in the workplace is not violative of the Act, the lines between passive or incidental observation and intentional monitoring or searching are not always clear.\textsuperscript{186} Indeed, not all employer surveillance or monitoring is an unfair labor practice.\textsuperscript{187} However, an employer’s surveillance of union activity violates Section 8(a)(1) if it is “coercive, threatening or restraining in nature.”\textsuperscript{188} Moreover, the Board has held that, under certain circumstances, an employer may violate Section 8(a)(1) by creating the impression of surveillance.\textsuperscript{189}

\begin{footnotesize}
\begin{enumerate}
\item Mathiason et al., supra note 6, at 42 (“[BYOD] [m]onitoring may take the form of reviewing applications employees install on their dual-use devices to prevent the installation of insecure apps or monitoring the websites employees visit to ensure employees are adhering to other company policies.”).
\item \textit{Id}.
\item Other relevant federal laws, such as the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, are beyond the scope of this Note. See Corey A. Ciocchetti, \textit{The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring}, 48 \textit{Am. Bus. L.J.} 285, 291–92 (2011) (reviewing the relevant federal laws as applied to the private workplace).
\item Finkin, supra note 178, at 373.
\item See id. (“The difficulty is that an employer may not be able to avoid passive observation – a supervisor cannot close his or her eyes at the water cooler when a union activist hands a co-worker a piece of union literature; but the search for the ‘disloyal’ via computer screening of utterance is scarcely passive.”).
\item See Villa Maria Nursing & Rehab. Ctr., Inc., 355 N.L.R.B. 1345, 1350 (2001) (“An employer’s mere observation of open, public, union activity on or near its property does not constitute unlawful surveillance.”).
\item NLRB v. Gold Spot Dairy, Inc., 417 F.2d 761, 762 (10th Cir. 1969); see, e.g., Partyline Worldwide, Inc., 344 N.L.R.B. 1342, 1342 (2005) (finding unfair labor practice when “no less than eight high-ranking managers and supervisors stood at entrances to the employee parking lot watching [union representatives] give literature to employees as they entered and exited the parking lot during shift changes”); Loudon Steel, Inc., 340 N.L.R.B. 307, 307 (2003) (concluding that employer unlawfully engaged “in surveillance of employees’ union activities by approaching their vehicles as the Union attempted to distribute handbills . . . .”); Fred’s Wallace & Son, Inc., 331 N.L.R.B. 914, 915 (2000) (“[W]hile an employer can watch open union activity, if it . . . openly takes down names or videotapes that activity, it goes too far and unlawfully creates the impression of surveillance . . . .”).
\item See Lundy Packing Co., 223 N.L.R.B. 139, 147 (1976) (“[B]y creating the impression that union
\end{enumerate}
\end{footnotesize}
The idea behind finding “an impression of surveillance” as a violation of Section 8(a)(1) of the Act is that employees should be free to participate in union organizing campaigns without the fear that members of management are peering over their shoulders, taking note of who is involved in union activities, and in what particular ways.\footnote{Flexsteel Indus., 311 N.L.R.B. at 257.}

Moreover, soliciting employees to engage in surveillance to communicate anti-union statements to the employees or enlisting employees to conduct surveillance of union activities violates Section 8(a)(1) because employees cannot feel free to exercise their Section 7 rights under such circumstances.\footnote{Register-Guard, supra note 178, at 373.}

In a BYOD program, even though the employer may have a legitimate interest in monitoring the employee’s actions and communications, the employer must not create an impression of surveillance.\footnote{See Lundy Packing Co., 223 N.L.R.B. 139, 147 (1976) (“[B]y creating the impression that union meetings were under company surveillance Respondent has violated Section 8(a)(1)”).} Given that most monitoring of a BYOD device will involve installing software onto the dual-device, and the fact that such a device will be expressly used by the employee for personal and work purposes, an impression of surveillance is almost sure to arise in a BYOD scenario. For example, a union steward utilizing a BYOD device may use the device to send communications soliciting union membership or distributing union literature. The employer’s monitoring of the BYOD device would catch such communications. An individual aware of such monitoring might refrain from sending such protected communications for fear of being targeted by the employer. Creating an impression of surveillance requires only that the employer to indicate that “it is closely monitoring the degree of an employee’s union involvement.”\footnote{Finkin, supra note 178, at 373.} Thus, the employer must be careful about when, what, and how they monitor employee’s electronic communications and actions. Moreover, the employer must not “single out union-related communications for application of”\footnote{Id.} a communications or electronic use policy “[since s]uch would be a discriminatory application of an otherwise neutral policy”\footnote{Id.} and, even under \textit{Register-Guard}, would violate the Act.

\footnote{Mohawk Indus. Inc., 334 N.L.R.B. 1170, 1171 (2001) (telling employees that the employer had a list of union supporters creates an unlawful impression of surveillance of employees’ union activities).  
191. See Metro One Loss Prevention Servs. Grp. (Guard Div. NY), Inc., 356 N.L.R.B. No. 20, *2 (Nov. 8, 2010) (holding that the employer violates NLRA by requesting an employee to spy on another employee’s union activities and report back to the employer); Marhoefer Baking Co., Inc., 258 N.L.R.B. 511, 514 (1981) (noting that there is an NLRA violation when an employer engages in “soliciting employee grievances, in proposing an employer-employee committee to resolve employee grievances in place of the Union, and in threatening to discontinue the operation in retaliation if the employees chose to be represented by the Teamsters . . . “)).  
192. See Flexsteel Indus., 311 N.L.R.B. at 257.  
193. Flexsteel Indus., 311 N.L.R.B. at 257.  
194. Finkin, supra note 178, at 373.  
195. Id.
C. BYOD Policies Are Mandatory Subjects of Bargaining

Section 158(a)(5) of the Act makes it an unfair labor practice for an employer “to refuse to bargain collectively with the representatives of his employees . . . “196 Section 158(d) defines collective bargaining as follows:

For the purposes of this section, to bargain collectively is the performance of the mutual obligation of the employer and the representative of the employees to meet at reasonable times and confer in good faith with respect to wages, hours, and other terms and conditions of employment, or the negotiation of an agreement, or any question arising thereunder, and the execution of a written contract incorporating any agreement reached if requested by either party, but such obligation does not compel either party to agree to a proposal or require the making of a concession . . .197

In sum, both the employer and the employee bargaining representative have an obligation to bargain in good faith regarding, and only regarding, mandatory bargaining subjects. 198 Mandatory bargaining subjects are “wages, hours, and other terms and conditions of employment.”199 The question presented is whether the specific components of an employer’s BYOD policy—including MDM software and remote device wiping policies—are mandatory bargaining subjects.

While “wages” and “hours” are relatively clear bargaining topics, the phrase “other terms and conditions of employment” is considerably more elusive.200 There is no statutory definition on point and the Supreme Court has primarily left it to the Board to decide whether a given topic is a mandatory bargaining subject.201 The Board in turn has proceeded to define the concept through case-by-case adjudication.202 Consequently, the Board has decided that a myriad of topics are mandatory bargaining subjects.203 Some

197. 29 U.S.C § 158(d) (2012).
198. Id.
199. Id.
201. Id at 495.
202. See id. at 495.
203. Id.
representative topics are: in-plant food prices and services, freedom from discriminatory discharge, seniority rights, the imposition of a compulsory retirement age, work rules, and use of bulletin boards.

The Supreme Court has provided some guidance on the question of what constitutes a "term and condition of employment." In *Fibreboard*, the Court adopted the notion that "managerial decisions, which lie at the core of entrepreneurial control," are not mandatory bargaining subjects. In *First National Maintenance*—which concerned a company that closed one of its facilities and terminated all of its workers there three weeks after the union attempted to bargain with the company—the Court identified three types of management decisions: (1) those that "have only an indirect and attenuated impact on the employment relationship," such as decisions regarding advertising and financing; (2) those that "are almost exclusively 'an aspect of the relationship' between employer and employee," such as decisions related to production quotas and work rules; and (3) those that have "a direct impact on employment . . . but [have] as [their] focus only the economic profitability

the Senate and now appearing in § 8(d).

204. *Id.* at 497.


The contracts . . . were the means adopted to ‘eliminate the Union as the collective bargaining agency of its employees’ . . . [B]y their terms they imposed illegal restraints upon the employees’ rights to organize the bargain collectively guaranteed by §§ 7 and 8 of the Act . . . . This provision foreclosed the employee from bargaining for a closed shop or a signed agreement with the employer, frequent subjects of negotiation between employers and employees . . . . The Board . . . prote[es] the ‘exercise by workers of full freedom of association, self-organization, and designation of representatives of their own choosing, for the purpose of negotiating the terms and conditions of their employment . . . .’

206. See Indus. Union of Marine & Shipbuilding Workers of Am., AFL-CIO v. NLRB, 320 F.2d 615, 620 (3d Cir. 1963) ("We agree with the Board that both seniority rights and a grievance procedure are within the phrase 'wages, hours, and other terms and conditions of employment' and hence are mandatory bargaining subjects.").

207. See Inland Steel Co. v. NLRB, 170 F.2d 247, 252 (7th Cir. 1948).

The Company’s position that the age of retirement is not a matter for bargaining leads to the incongruous result that a proper bargaining matter is presented if an employee is suddenly discharged on the day before he reaches the age of 65, but that the next day, when he is subject to compulsory retirement, his Union is without right to bargain concerning such retirement.


Despite the deliberate open-endedness of the statutory language, there is an undeniable limit to the subjects about which bargaining must take place: "Section 8(a) of the Act, of course, does not immutably fix a list of subjects for mandatory bargaining . . . . But it does establish a limitation against which proposed topics must be measured. In general terms, the limitation includes only issues that settle an aspect of the relationship between the employer and the employees." . . . Other management decisions, such as the order of succession of layoffs and recalls, production quotas, and work rules, are almost exclusively ‘an aspect of the relationship’ between employer and employee.

209. NLRB v. Proof Co., 242 F.2d 560, 562 (7th Cir. 1957).


212. *Id.*


214. *Id.* at 677.

of” the business. The Court concluded that the employer’s decision to close part of its business belonged in the third category. Such decisions require mandatory bargaining, the Court reasoned, “only if the benefit, for labor-management relations and the collective-bargaining process, outweighs the burden placed on the conduct of the business.” Applying this balancing test, the Court held that the company did not have an obligation to bargain before closing part of its business for purely economic reasons.

Applying Supreme Court precedent, the Board has adopted the Ford Motor test for assessing whether a particular issue is a mandatory bargaining subject. Under Ford Motor there are two prongs of inquiry: first, whether the subject at issue is germane to the working environment, or, whether the subject will “settle an aspect of the relationship between the employer and employees.” The second prong is whether the subject at issue lies at the core of entrepreneurial control. While the Board has yet to rule on whether a BYOD policy is a mandatory subject of bargaining, the following analysis suggests that it would be.

In a series of cases pre-dating the widespread use of new technologies in the workplace, the Board appeared to view most workplace technologies of the time as mandatory subjects of bargaining. Conceiving a BYOD program in general terms—the ability of an employee to utilize her own device at work for work purposes—such a program would clearly be germane to the working environment, as it would fundamentally alter the means by which an employee works on a daily basis. It is also likely that such a policy would not lie at the core of entrepreneurial control. In Fibreboard, Justice Stewart (whose formulation of the standard was adopted in Ford Motor) described the kinds of management decisions that are beyond the ken of collective bargaining: “[d]ecisions concerning the volume and kind of advertising expenditures, product design, the manner of financing, and sales, all may bear upon the

216. Id.
217. Id.
218. Id. at 679.
219. Id. at 686; see also United Food & Commercial Workers, Local 150-A v. NLRB, 1 F.3d 24 (D.C. Cir. 1993) (affirming the Board’s new standard for determining whether a decision to relocate bargaining unit work is a mandatory subject of bargaining).
220. See, e.g., Colgate Palmolive Co., 323 N.L.R.B. 515, 515–16 (1997) (holding that surveillance cameras were germane to the work environment, were not entrepreneurial in nature, and were thus a mandatory subject of bargaining); Johnson-Batenem Co., 295 N.L.R.B. 180, 182 (1989) (holding that drug and alcohol testing requirements were “both germane to the work environment and outside the scope of managerial decisions”); Medicenter, Mid-South Hosp., 221 N.L.R.B. 670, 676 (1975) (applying the standard as set out by Justice Stewart’s concurring opinion in Fibreboard to hold that polygraph testing was not a managerial decision that was at the core of entrepreneurial control).
security of the workers’ jobs . . . [but] such decisions [do not] so involve ‘conditions of employment’ that they must be negotiated with the employees’ bargaining representative.” In sum, Justice Stewart would exclude from bargaining “those management decisions which are fundamental to the basic direction of a corporate enterprise or which impinge only indirectly upon employment security . . . .” Applying this language, a BYOD program does implicate company finances but does not concern “the manner of financing,” and a BYOD program is not akin to product design or advertising. More importantly, as set forth below, a BYOD program does directly impinge upon the job security of employees since the monitoring of such devices can be evidence utilized in a discharge.

In *E.I. DuPont de Nemours & Co.*, the employer wished to produce a videotape expressing its new management principles and asked employees to participate in the video. The Board held that, because the employee’s participation was voluntary, participation in the video was not a mandatory subject of bargaining. However, the Board went on to suggest that the videotaping would have been a mandatory bargaining subject if participation was not voluntary or if the videotaping was part of the employee’s day-to-day responsibilities. In such a case, the videotaping would have become a term or condition of employment plainly germane to the working environment. However, BOYD monitoring is distinguishable and under *DuPont* would arguably be a mandatory subject of bargaining since such monitoring would “represent [a] change in an important facet of the daily lives of unit employees, [and would] impinge on their employment security.” This conclusion is supported by the Seventh Circuit’s ruling in *In re Amoco Petroleum Additives Co.* where the court, in dicta, noted that electronic surveillance and the degree of privacy available in the workplace is a “condition” of employment and an “ordinary subject of bargaining.”

The Board took up a similar issue—installation of surveillance cameras in the workplace, including restroom facilities—in *Colgate-Palmolive Co. v. Local 15, International Chemical Workers Union.* The Board held that installation of such surveillance was germane to the working environment. The Board analogized the cameras to other investigatory tools, such as drug and polygraph testing, and physical examinations, all of which were

226. *Id.*
227. *Id.*
229. *Id.* at 155.
230. *Id.* at 155–56.
231. *Id.*
232. *Id.*
233. *Id.* at 156.
236. *Id.*
238. *Austin-Berryhill, Inc.*, 246 N.L.R.B. 1139 (1979); *Medicenter, Mid-South Hospital*, 221 N.L.R.B.
found to be mandatory bargaining subjects. Moreover, the Board raised concerns about employee privacy due to the placement of cameras in the restrooms. Finally, the Board concluded that installation of the cameras was not an issue lying at the core of entrepreneurial control.

Electronic surveillance of the type discussed (i.e., hidden video cameras) is not entirely distinct from the type of monitoring that a BYOD policy would entail. Such monitoring would capture employee actions, decisions, and locations. Moreover, such monitoring could conceivably be used as an investigatory tool or basis for discharge. Finally, such monitoring is clearly germane to the working environment and lies beyond the core of entrepreneurial control. Consequently, even though the Board has yet to rule on this type of electronic surveillance, it is likely that the Board and the courts would find such monitoring to be a mandatory bargaining subject.

IV. RECOMMENDATION

Recall that in Register-Guard, the Board found that the employer did not violate Section 8(a)(1) of the NLRA by maintaining a policy prohibiting the use of the employer’s email system for all “non-job-related solicitations,” including Section 7 activity. The basis for the decision was that an employer’s email system is company property and employees have no statutory right to use an employer’s email system for Section 7 purposes.

The first issue is the tension between Register-Guard and Board precedent. In Register-Guard, the Board condoned employer restriction of email because there were alternative means of communication between employees, such as face-to-face communication and physical distribution of literature. The Board thus inappropriately applied a nonemployee standard for real property access that followed Babcock & Wilcox and Lechmere.

670 (1975).
240. Colgate, 323 N.L.R.B. at 515.
241. Id.
242. Id.; see also Brewers & Maltsters, Local Union No. 6 v. NLRB, 414 F.3d 36, 45 (D.C. Cir. 2005) (affirming the Board’s ruling that “use of hidden surveillance cameras in the workplace is a mandatory subject of bargaining”); Nat’l Steel Corp. v. NLRB, 324 F.3d 928, 931–33 (7th Cir. 2003) (affirming Colgate-Palmolive and holding that use of hidden surveillance cameras is a mandatory subject of bargaining because use of such devices to discover misconduct has implications for an employee’s job security).
244. Register-Guard I, supra note 13, at 1115.
245. Id.
246. Id. at 1115–16.
248. NLRB v. Babcock & Wilcox Co., 351 U.S. 105, 112–13 (1956) (ruling that no obligation is owed to allow nonemployee organizers to distribute or solicit on the employer’s property except where “the location of the plant and the living quarters of the employees place the employees beyond the reach of reasonable union efforts to communicate with them”).
249. Jean Country, 291 N.L.R.B. 11, 22 (1988) (setting forth a three-pronged balancing test in attempt to follow the dictate of Babcock & Wilcox that accommodation between employees’ Section 7 rights and
rather than applying the employee standard for real property access that follows *Republic Aviation*.

Thus, the case was predicated on a fallacious application of legal precedent.

The second and larger issue in *Register-Guard* was the Board’s approach to email and the workplace. As previously mentioned, the Board analogized email systems to other traditional communication systems, such as bulletin boards and telephones despite the obvious dissimilarity. Specifically, the Board did not give consideration to the collapsed distinction between solicitation and distribution in electronic communications, nor did the Board fully consider the complicated network of ownership rights over an email system. Finally, the Board decision turned a blind eye to the realities of the modern workplace wherein many employees work remotely using personal servers in traditionally nonwork areas. *How Register-Guard* would apply to remote workers, cyberworkers, or an employee working off of a BYOD device is patently unclear from the Board’s decision.

Given that *Register-Guard* confirms the Board as “the Rip Van Winkle of administrative agencies”—ignoring the unique features of the modern workplace and attempting to apply anachronistic standards to a completely new problem—it is clear that the Board must update its approach by adapting the NLRA and Board precedent to the dictates of the future. Overturning *Register-Guard* would be an effective beginning. If the Board were to overturn *Register-Guard*, it would be advantageous for the Board to clearly state that email is not a traditional mode of communication and requires a distinct standard of legal analysis and a BYOD program is a mandatory bargaining subject. Perhaps most importantly, the Board should take the opportunity to update and adapt the NLRA to the unique issues of a technologized workplace and workforce. Returning to the rule set forth in *Republic Aviation* is the most logical choice for the Board to make.

Given that employer monitoring of employee’s electronic communications and activity has the potential to create the impression of surveillance and impede employees’ Section 7 rights, the employer should have a policy in place, be clear and forthright with their intention to monitor.

employers’ property rights “must be obtained with as little destruction of the one as is consistent with the maintenance of the other.”).


253. See id. at 1121 (exemplifying an example of when the dissent quotes NLRB v. Thill, Inc., 980 F.2d 1137, 1142 (7th Cir. 1992)).

254. Though interestingly, when the Board called for briefs, the list of questions it presented included whether or not to apply a traditional or a new standard to the modern workplace. Id. at 1110.

255. While somewhat dated, a good example of a corporate policy governing employees’ use of the internet and email—including commentary on employees’ personal use of the internet and email—can be found in DAVID M. DOUBLET & VINCENT I. POLLEY, *EMPLOYEE USE OF THE INTERNET AND E-MAIL: A MODEL CORPORATE POLICY WITH COMMENTARY ON ITS USE IN THE U.S. AND OTHER COUNTRIES* 1–17 (2002). A more recent corporate policy focusing on employee use of mobile devices suggests that: An employee mobile device policy should address the following:
the BYOD devices, and should have employees sign agreements of understanding to that effect. While it is true that at least one court has found email monitoring lawful, despite employees not having been informed of the company policy, the rationale was predicated on the employer’s ownership of the hardware and the network on which the email has been sent—a premise not necessarily true in a BYOD setting. Having employees sign consent forms permits employees to consider their electronic communications and actions and change their behavior accordingly. Thus, obtaining consent is an important form of notification, and notification of when an employer is monitoring electronic communications is statutorily required in several states, including Connecticut and Delaware.

Second, given that the implementation of a BYOD program would likely be construed as a mandatory bargaining subject by a court, the employer should err on the side of caution by bargaining in good faith with the union about the new program, though the employer need not make any concessions as to the specific policies surrounding the program. The duty of an

- Specify which mobile communications devices employers may use.
- Require employees to sign a waiver or release form.
- Determine when employer policies will be audited, assessed, and enforced in relation to the devices.
- Consider whether employees will be reimbursed for employer-specific use of a personal device.
- Restrict or limit software applications that employees may download.
- Determine the types of employer-related resources employees may access on their devices.
- Instruct employees on appropriate security procedures and enable them to separate the employer’s information from personal information on the device.
- Require employees to load approved security-related software for access to the employer’s systems and servers.
- Determine the IT support the organization will provide for the device or its applications.
- Create a procedure for retrieval of the employer’s data when a personally owned device user’s employment is terminated or the device is lost or stolen.
- Create a procedure for retrieval of the personal data of its device if it is needed for data collection and preservation in association with a legal hold order.


256. McLaren v. Microsoft, No. 05-97-00824-CV, 1999 WL 339015, at *4 (Tex. Ct. App. May 28, 1999) (ruling that the employer’s ownership of the computer and the network preempted any presumption or expectation of privacy on the part of the employee). See, e.g., Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (“[W]e do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system”); see also Tanya E. Milligan, Virtual Performance: Employment Issues in the Electronic Age, 38 COLO. LAWYER 2, 29–36 (2009) (finding that employees do not generally have an expectation of privacy regarding online communications). However, seventy-one percent of employers monitoring employees email notify such employees prior to any monitoring. See AMA/J/D POLICY INST. RES., supra note 176, at 5 (stating that eleven percent of employers do not notify employees while another eighteen percent do not know whether email monitoring took place).

257. The ECPA also contains a consent exception to employer monitoring. 18 U.S.C. § 2511 (2d ed.) (2002); see also Employers Must Obtain Employee Consent for BYOD Programs, LAW 360 (May 24, 2013, 11:12 AM), http://www.cov.com/files/Publication/cf92c70-1ddd-4ce0-9a88-25ec908324df/Presentation/PublicationAttachment/f2476f96-c4d4-4dd3-b575-28614fc43ef1/Employers_Must_Obtain_Employee_Consent_for_BYOD_Programs.pdf (focusing on the Computer Fraud and Abuse Act and suggesting that employers require all employees to give affirmative consent to a BYOD policy).


259. Supra Part III.C.

employer to bargain in good faith, imposed by Section 8(a)(5),\textsuperscript{261} means that an employer’s unilateral implementation of a BYOD program (i.e., implementation without negotiating with the union) will constitute an unfair labor practice.\textsuperscript{262}

V. CONCLUSION

As the consumerization of technology continues to expand IT innovation and drive technology decision-making in the employment context, it is important that employers remain cognizant of their statutory obligations and employees’ statutory rights. The BYOD movement is just beginning to receive widespread recognition and while some impediments to implementation have been resolved (e.g., by MDMs), as BYOD programs become more ubiquitous more problems will arise. As of yet the Board and the courts have not had the opportunity to interrogate the labor and employment issues that potentially arise in a BYOD setting. This creates some ambiguity around what is permissible—for example what level of employer monitoring of a BYOD device is a fair labor practice—but an employer can easily avoid becoming a landmark defendant by carefully, perhaps overzealously, following the dictates of the NLRA and ensuring that any BYOD policies are fully discussed and negotiated with the union. Technology will often make the workplace a more cost efficient and effective enterprise, but this does not mean that we have to jeopardize or disregard the rights of employees in the process.

\textsuperscript{261} Register-Guard I, \textit{supra} note 13, at 1111.