Hofstra Labor & Employment Law Journal

Volume 34 | Issue 2 Article 7

3-1-2017

Not Every Cloud Has a Silver Lining: The Implications of Cloud-Based Computing and Bring Your Own Devices on Employee Monitoring and the Dynamic Shift in the Definition of the Workplace

Ashtyn Hemendinger
Maurice A. Deane School of Law at Hofstra University

Follow this and additional works at: https://scholarlycommons.law.hofstra.edu/hlelj

 Part of the Labor and Employment Law Commons

Recommended Citation
Hemendinger, Ashtyn (2017) "Not Every Cloud Has a Silver Lining: The Implications of Cloud-Based Computing and Bring Your Own Devices on Employee Monitoring and the Dynamic Shift in the Definition of the Workplace," *Hofstra Labor & Employment Law Journal*: Vol. 34: Iss. 2, Article 7.
Available at: https://scholarlycommons.law.hofstra.edu/hlelj/vol34/iss2/7

This document is brought to you for free and open access by Scholarship @ Hofstra Law. It has been accepted for inclusion in Hofstra Labor & Employment Law Journal by an authorized administrator of Scholarship @ Hofstra Law. For more information, please contact lawscholarlycommons@hofstra.edu.

NOTES

NOT EVERY CLOUD HAS A SILVER LINING: THE IMPLICATIONS OF CLOUD-BASED COMPUTING AND BRING YOUR OWN DEVICES ON EMPLOYEE MONITORING AND THE DYNAMIC SHIFT IN THE DEFINITION OF THE WORKPLACE

I. INTRODUCTION

The Cloud is a nebulous subject matter for many. It may boggle the mind to think that something so intangible can hold such vast amounts of information.[1] Simply put, however, this mystical force is a way of accessing data stored not on the internal databases of the computer, but through external databases such as the Internet.[2] An instance of Cloud-based software, commonly used in the workplace, involves external applications on the Internet that companies use and input information into.[3] In much the same way as you would visit a website, you access these applications through a web browser like Internet Explorer, Firefox, Safari, or Google Chrome.[4] All information that you type into the software, and any files that you create, are saved on the website and protected with a unique user name and password.[5] More and more companies are switching to Cloud-based technology systems for daily tasks and to streamline work product.[6] In fact, "several [C]loud computing applications, such [as] web email, wiki applications, and online tax preparation," have become common uses for work and

1. DropBox, Google Drive, One Drive, and Box are examples of online cloud storage systems. *See, e.g.*, Michael Muchmore, *The Best Cloud Storage and File-Sharing Services of 2017*, PCMAG UK (Mar. 31, 2017), http://uk.pcmag.com/storage-devices-reviews/3682/guide/the-best-cloud-storage-and-file-sharing-services-of-2017.

2. Melanie Pinola, *What Is Cloud Computing?*, LIFEWIRE (Oct. 21, 2016), https://www.lifewire.com/what-is-cloud-computing-2378249.

3. *See id.* (common examples might include Facebook, Gmail, and financial apps like PNC Bank).

4. *See id.*

5. *See id.*

6. *See The 2016 Gartner CIO Agenda*, GARTNER, https://web.archive.org/web/20151010084735/http://www.gartner.com:80/technology/cio-trends/cio-agenda/ (last visited May 4, 2017).

Published by Scholarship @ Hofstra Law, 2017

personal experiences.[7] For instance, when an employee buys items for the sales department on Amazon, the financial information goes into the Cloud for others at the company to use.[8]

Supporters of the switch to Cloud computing contend that it is cheaper, faster, and more secure than traditional data storage.[9] Traditional storage users, on the other hand, object to Cloud computing because they believe they are "hand[ing] over their valuable proprietary information to third parties."[10] Without adequate controls in place, Cloud-based software can raise security issues, such as data loss and theft.[11] Some privacy scholars go so far as to say that "the vast majority of [C]loud computing services is, by default, insecure."[12] One successful corporation recently had such a privacy issue with the Cloud where a procurement employee redeemed the company's points on a retail website to go on an all-expense paid vacation.[13] This not only went against company policies, but it also violated the employee's fiduciary duty as an agent of the company.[14]

In situations like this, it seems obvious that legal security measures need to be implemented to protect the employer's interests. Such measures may include working with the Human Resources ("HR") and Information Technology ("IT") departments in order to create new policies, as well as searching work devices on which employees store company information.[15] However, when dealing with companies, one

7. *Cloud Computing*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/cloudcomputing/ (last visited May 4, 2017).

8. *See* Rich Miller, *Inside Amazon's Cloud Computing Infrastructure*, DATA CTR. FRONTIER (Sept. 23, 2015), http://datacenterfrontier.com/inside-amazon-cloud-computing-infrastructure/.

9. *See* Pinola, *supra* note 2.

10. Elana A. Bertram, *How to Keep Your Invention Patentable While It is Stored in the Cloud: A Guide for Small Inventors*, 21 FED. CIR. B.J. 389 (2012).

11. *See* Vangie Beal, *Cloud Computing Security Challenges*, WEBOPEDIA (Apr. 15, 2011), http://www.webopedia.com/DidYouKnow/Hardware_Software/cloud_computing_security_challenges.html. The issue of cloud computing and privacy is especially prevalent at law firms, where attorneys are handling privileged client information. There is a risk of the information coming into the hands of unintended recipients when transmitting information relating to the representation. Therefore, attorneys must proactively confirm that the cloud computing is up to date and extremely secure. James T. Townsend, *Professional Responsibility*, 62 SYRACUSE L. REV. (2010-2011 Survey of New York Law) 763, 775 (2012).

12. Bertram, *supra* note 10, at 400 (internal quotations and citations omitted).

13. The corporation discussed throughout this section has asked to remain anonymous. The facts and circumstances explained are specific to that corporation.

14. RESTATEMENT (THIRD) AGENCY § 8.01 (AM. LAW INST. 2005).

15. *See InfoLawGroup LLP, The Security, Privacy and Legal Implications of BYOD (Bring Your Own Device)*, INFO. L. GROUP (Mar. 28, 2012), http://www.infolawgroup.com/2012/03/articles/byod/the-security-privacy-and-legal-implications-of-byod-bring-your-own-device/.

has to consider both the employer's interest in security and the employees' needs and rights. With the Cloud comes the ability to access personal and work information anytime and anywhere, that is, as long as you have an electronic device (e.g. your personal smartphone or computer).[16] When the electronic work and personal life boundary is blurred, legal issues arise involving the Fourth Amendment, legislative statutes, and an employee's right to privacy.[17]

In 2010, the Supreme Court addressed the issue of employees' privacy in the public and governmental sector in *City of Ontario v. Quon*.[18] While stating that Quon had a reasonable expectation of privacy in his use of his company-owned cellphone, the Supreme Court refused to define what a reasonable expectation of privacy was in the workplace.[19] With an ambiguous Supreme Court decision, the working world is now left with unanswered questions of how to address the complex interplay between privacy and technology in the workplace.[20]

This Note addresses the conflicting ideals of the workplace: an employee's right to privacy and the employer's duty to ensure that the company's best interests and fiduciary obligations are met.[21] Even in the age of technological innovation, this issue is still too novel to have been "extensively litigated."[22] As a result, the different principles will be examined objectively by comparing an employee's right to privacy on work and personal devices against the employer's right to search these devices.[23] However, unlike other scholarly pieces, which only discuss

16. *See What is the Cloud?*, GCFLEARNFREE.ORG, https://www.gcflearnfree.org/computerbasics/understanding-the-cloud/1/ (last visited May 4, 2017).

17. *See* Diane Vaksdal Smith & Jacob Burg, *What are the Limits of Employee Privacy?*, GP SOLO (Privacy and Confidentiality, A Publication of the American Bar Association), Nov./Dec. 2012, http://www.americanbar.org/publications/gp_solo/2012/november_december2012privacyandconfidentiality/what_are_limits_employee_privacy.html.

18. *See* City of Ontario v. Quon, 560 U.S. 746, 763 (2010) (finding that search was permissible in its scope because reviewing the transcripts was reasonable since it was an efficient and expedient way to determine whether the employee's overages were the result of work-related messaging or personal use); *see also infra* Section V.B.

19. *See id.* at 764-65.

20. *See* Rehberg v. Paulk, 611 F.3d 828, 847 (11th Cir. 2010). After Quon, *Rehberg v. Paulk* continued to skirt the technology and privacy issue. *See id.* It seems as if courts are skirting the issue and pushing it off for some other generation. However, as technology becomes more and more an integral part of our lives, regulations and rules need to be established on technology privacy.

21. *See infra* Sections III.A., III.B., III.C., IV.

22. Bertram, *supra* note 10, at 389.

23. *See infra* Sections III.A., III.B., III.C., IV.

an employee's right to privacy as the overruling factor,[24] this Note also examines the importance of the employee's fiduciary duty, and, therefore, suggests a policy leaning in favor of the employer.[25]

Throughout the analysis, this Note will clarify what is meant by the phrase "reasonable expectation of privacy."[26] Section II of this Note begins by briefly discussing the topic of Cloud computing.[27] Section III then provides an analysis of the apportioned rights of the Fourth Amendment, alongside administrative rulings and state-specific privacy and search and seizure statutes.[28] Section IV addresses the current relationship between technology and the Fourth Amendment, administrative rulings, and statutes and legislation.[29] Section V then discusses the development of the current standard used to evaluate employee monitoring.[30] After objectively exploring the conflicting ideals, Section VI suggests several solutions to clear away the overcast engulfing the issues of the Cloud, Bring Your Own Device ("BYOD") policies, and employee monitoring.[31]

II. CLOUD COMPUTING: THE BASICS

The Cloud is what technologists like to call "computing on demand."[32] It is a way of delivering computing power to a user, wherever and whenever they need it, through digital devices such as a computer or cellphone.[33] Cloud computing can take different forms,

---

24. *See, e.g.*, Marissa A. Lalli, Note, *Spicy Little Conversations: Technology in the Workplace and a Call for a New Cross-Doctrinal Jurisprudence,* 48 AM. CRIM. L. REV. 243, 244 (2011) (discussing several cases that dealt with employee privacy as the central issue).

25. The laws of agency and corporations will be used to further this argument. *See* RESTATEMENT (THIRD) AGENCY § 8.01 (AM. LAW INST. 2006).

26. At the moment, a reasonable expectation of privacy is determined by the following: "(1) the individual exhibited an actual expectation of privacy in the location searched (the subjective prong); and (2) that expectation is one that society is prepared to accept as reasonable (the objective prong)." Although arguably clearer than just stating a "reasonable expectation of privacy," this still lacks a clear definition of what this phrase means. Mary Graw Leary, *The Supreme Digital Divide*, 48 TEX. TECH L. REV. 65, 68 (2015).

27. *See infra* Section II.

28. *See infra* Sections III.A., III.B., III.C.

29. *See infra* Section IV.

30. *See infra* Sections V.A., V.B.

31. *See infra* Sections VI.A., VI.B., VI.C., VI.D.

32. Jeffrey F. Rayport and Andrew Heyward, *Envisioning the Cloud: The Next Computer Paradigm,* MARKETSPACENEXT, https://web.archive.org/web/20150410001016/http://marketspacenext.com/inthemedia/envisioning-the-cloud/ (last visited May 4, 2017) (best accessed via the wayback machine as original URL no longer exists).

33. *See What is Cloud Computing*, QUEEN MARY U. OF LONDON SCH. OF L.,

with varying ranges of privacy.[34] For instance, companies have the option to choose between using a private cloud, public cloud, or hybrid cloud security system.[35] In a private cloud forum, most websites and information remain within the corporate firewall.[36] In these cases, system administrators from the IT department can manually control security.[37] Another option is a public cloud forum, in which a company relies on a third-party cloud service provider for services such as servers, data storage, and applications.[38] The system recommended for most companies is a hybrid cloud forum, which is a combination of both public and private forums.[39] With hybrid cloud forums, enterprises are able to mix and match cloud storage resources.[40]

In the workplace the cloud computing software model known as "Software as a Service" ("SaaS") has grown in popularity.[41] Using SaaS is much like someone using Gmail or Yahoo mail services, except SaaS goes further.[42] Instead of employees having their data saved on their individual computer, SaaS is accessed via a web browser and data is stored in the vendor of the SaaS's data center.[43] This is very appealing to companies.[44] Because the Cloud uses "shared resources, including software and servers, to deliver information and services to the end

---

http://www.cloudlegal.ccls.qmul.ac.uk/what/index.html (last visited May 4, 2017).

34. *See* Beal, *supra* note 11; *see also* Eric Knorr, *What Cloud Computing Really Means*, INFOWORLD (Apr. 7, 2008), http://www.infoworld.com/article/2683784/cloud-computing/what-cloud-computing-really-means.html.

35. *See* Knorr, *supra* note 34 (such as SaaS, MSP, or a hybrid of the two).

36. Vangie Beal, *Private Cloud,* WEBOPEDIA, http://www.webopedia.com/TERM/P/private_cloud.html (last visited May 4, 2017).

37. *See id.*

38. Forrest Stroud, *Public Cloud,* WEBOPEDIA, http://www.webopedia.com/TERM/P/public_cloud.html (last visited May 4, 2017).

39. Vangie Beal, *Hybrid Cloud Storage,* WEBOPEDIA, http://www.webopedia.com/TERM/H/hybrid_cloud_storage.html (last visited May 4, 2017) [hereinafter Beal, *Hybrid*]. Hybrid cloud forums are typically used in private corporations that do business with outside companies. *See* Knorr, *supra* note 35.

40. Beal, *Hybrid*, *supra* note 39.

41. *See Cloud Computing/Software as a Service for Lawyers*, ABA L. PRAC. DIVISION, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/saas.html (last visited May 4, 2017. An example of SaaS is Concur Technologies (provides travel and expense management for companies). *See Top 10 Software as a Service (SaaS) Companies*, ZEENDO (Mar. 8, 2013), http://zeendo.com/info/top-10-software-as-a-service-saas-companies/.

42. Paul Gil, *What is 'SaaS' (Software as a Service)?*, LIFEWIRE (http://netforbeginners.about.com/od/s/f/what_is_SaaS_software_as_a_service.htm (last updated Mar. 23, 2017).

43. *Cloud Computing/Software as a Service for Lawyers*, *supra* note 41.

44. *See id.* (discussing advantages such as automatic updates and subscription model packaging).

user", the service is inherently efficient.[45] Further, companies are drawn to the cloud by its lower costs, since the end user "is no longer burdened with the expense of maintaining and updating servers, data centers, and software."[46]

III. THE FOURTH AMENDMENT, ADMINISTRATIVE RULINGS, AND STATUTES AND LEGISLATION: IS THERE A RIGHT TO PRIVACY IN THE WORKPLACE?

Although the Constitution does not explicitly state that people have a right to privacy, the right is deemed inherent under the Fourth Amendment.[47] Whether or not this right extends into the workplace typically depends on whether the workplace is public or private.[48] Yet, even if the Fourth Amendment does not extend to nonpublic workplaces, recent administrative rulings and state privacy statutes have established that private and public employees do have a reasonable expectation to privacy in the workplace.[49]

A. The Fourth Amendment

The Fourth Amendment concerns the right of people to be safeguarded from "unreasonable searches and seizures."[50] In the past, the Supreme Court deemed searches conducted outside the judicial process to be unreasonable.[51] These unreasonable searches are subject to a few specific and well-established exceptions.[52] Before delving further

45. Nicole A. Black, *Global Cloud Survey Report 2012*, 2012 LEGAL IT PROFESSIONALS 4, https://www.legalitprofessionals.com/wpcs/cloudsurvey2012.pdf.

46. *Id.* at 5; *see also Cloud Computing*, *supra* note 7. Instead, the cloud-computing provider assumes these IT costs, while businesses simply pay a low monthly subscription fee. If the user needs temporary additional space, he can simply tell the cloud service provider to up his quota for the time being, rather than purchase additional physical capacity which would only be needed for a short period and then left idle. *Cloud Computing*, *supra* note 7.

47. *See* U.S. CONST. amend. IV.

48. *See id.*

49. Purple Comm'ns, Inc., 361 N.L.R.B. No. 126, 1 (Dec. 11, 2014); *see also* Ga. Code Ann. § 16-11-62 (2016).

50. U.S. CONST. amend. IV.

51. *See* City of Los Angeles, California v. Patel, 576 U.S. _, 135 S. Ct. 2443, 2452 (2015). "The Fourth Amendment proscribes all unreasonable searches and seizures, and it is a cardinal principle that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.'" Mincey v. Arizona, 437 U.S. 385 (1978) (emphasis in original) (quoting Katz v. United States, 389 U.S. 347, 357 (1967).

52. *See, e.g.*, *Mincey*, 437 U.S. at 390 (holding that the warrantless search of petitioner's

into the Fourth Amendment, it is important to address these exceptions to help define what is currently meant by the phrase "reasonable expectation of privacy."

In *Brigham City, Utah v. Stuart*, police officers responded to a three o'clock in the morning call regarding a loud party.[53] Hearing shouting outside, the police officers proceeded into the yard.[54] There, through the screen door and windows, they saw an altercation in the kitchen between four adults and a juvenile, who punched one of the adults, causing him to spit blood in a sink.[55] The officers opened the screen door and announced their presence.[56] When the fighting still continued, the officer entered the kitchen and again cried out, whereupon the altercation gradually subsided.[57] The officers arrested respondents and charged them with contributing to the delinquency of a minor and related offenses.[58] Defendants in this case motioned to suppress all evidence obtained after the officers entered the house, arguing that the warrantless entry violated the Fourth Amendment.[59]

While there are exceptions to a person's Fourth Amendment rights, limitations on those exceptions exist.[60] *United States v. Blok*, for example, discusses an employee, Peggy Jean Blok, was charged with petty larceny.[61] The police officers searched her desk without a warrant and discovered incriminating evidence.[62] Unlike *Brigham City*, the police search was not in response to an emergency.[63] The court held that

---

apartment as a homicide scene was permissible under the Fourth and Fourteenth Amendments and therefore fell under delineated exceptions). The Fourth Amendment protects the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. U.S. CONST. amend. IV. It further provides that no warrants shall issue, but upon probable cause. U.S. CONST. amend. IV. Based on this constitutional text, searches conducted outside the judicial process, without prior approval by a judge or a magistrate judge, are *per se* unreasonable subject only to a few specifically established and well-delineated exceptions. This rule applies to commercial premises as well as to homes. *City of Los Angeles*, 135 S. Ct. at 2456-57 (holding that hotels do not fall under this exception due to the regulations of the Constitution).

53. Brigham City v. Stuart, 547 U.S. 398, 400-01 (2006).

54. *Id.* at 401.

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.*

59. *See id.* at 401, 406-07.

60. *See* United States v. Blok, 188 F.2d 1019, 1020 (D.C. Cir. 1951).

61. *Id.*

62. *Id.*

63. *Compare id.* at 1019, 1020-21 (finding that combined operation of a government agency and enforcement of criminal law did not give a right to search beyond the scope of either in regards to defendant being arrested for petty larceny), *with Brigham City*, 547 U.S. 398, 406-07 (finding that Police officers' manner of warrantless entry into home was "reasonable," for Fourth

because Blok stored personal property in the desk and had the exclusive right to use it, the police officers had no right to search the desk without her permission.[64] Therefore, the United States Court of Appeals for the District of Columbia Circuit ruled that the search of the employee's desk was a violation of her right to privacy.[65]

The fundamental right of freedom from unreasonable searches and seizures is unique, in that it is one of the few provisions of the Bill of Rights that grew directly out of the experience of the colonials.[66] They had a good sense of what conduct was "unreasonable" since they experienced it first-hand under British rule.[67] Before the American Revolution, the British claimed the right to issue Writs of Assistance, which allowed British soldiers to enter a home for no specific reason other than to search for evidence of smuggling.[68] These Writs of Assistance were lambasted by colonists, who claimed they were being deprived of their essential English liberty.[69] With memories of the British "tyranny" still fresh in their minds, delegates to the ratification conventions demanded a Bill of Rights in the Constitution.[70] Included in the Bill of Rights would be the Fourth Amendment.[71]

After its introduction and ratification, the Fourth Amendment prohibited "broad, sweeping, arbitrary searches and seizures," while

---

Amendment purposes, where after observing ongoing physical altercation between occupants from outside, one officer opened the screen door of the home and yelled "police and when nobody responded, officers stepped inside and again announced their presence).

64. Her superiors may have reasonably searched the desk for official property needed for official use. *Blok*, 188 F.2d 1019, 1021. ("But as the Municipal Court of Appeals said, the search that was made was not 'an inspection or search by her superiors. It was precisely the kind of search by policemen for evidence of crime against which the constitutional prohibition was directed.' In the absence of a valid regulation to the contrary appellee was entitled to, and did, keep private property of a personal sort in her desk. Her superiors could not reasonably search the desk for her purse, her personal letters, or anything else that did not belong to the government and had no connection with the work of the office.").

65. *Id.* at 1021.

66. *See History,* JUSTIA US LAW, http://law.justia.com/constitution/us/amendment-04/01-search-and-seizure.html (last visited May 4, 2017).

67. Mike Maharrey, *Fourth Amendment: The History Behind "Unreasonable"*, TENTH AMEND. CTR., (Sept. 25, 2014, 1:03 AM), http://tenthamendmentcenter.com/2014/09/25/fourth-amendment-history-behind-unreasonable/.

68. *Id.*

69. Interestingly enough, Writs of Assistance were not considered proper in British legal tradition. *Id.* ("In 1604, Attorney General of England Sir Edward Coke held in Semayne's Case that the King did not have unlimited authority to enter a private dwelling. . . . Laying out the case, Coke eloquently upheld the sanctity of a person's home. 'The house of every one is to him as his castle and fortress, as well for his defen[s]e against injury and violence as for his repose.'").

70. *Id.*

71. *See id.*

requiring federal agents to first obtain a warrant before performing a search.[72] The Amendment eventually came to symbolize the right of privacy,[73] with a goal to uphold this right for both the public and private citizens of the United States.[74] However, whether the rights of public and private citizens are being fully upheld depends on how the U.S. Constitution is interpreted. If one interprets the Constitution narrowly, it seems that the Fourth Amendment only pertains to searches by the government.[75] In fact, some scholars argue that private intrusions are not covered under this Amendment.[76] Further, there is precedent to show that the Fourth Amendment does not extend to the privacy interests of non-public employees.[77] Employers at private corporations are restricted only "in rare situations where employees possess a 'reasonable expectation of privacy' in the workplace."[78]

However, gray areas emerge when considering devices used for work and pleasure, as well as personal work devices, which often go on external sites to complete transactions.[79] It is this area of technology in which the Fourth Amendment could possibly apply, since these items may have a greater expectation of privacy and may not be company-

72. *Id.* Each warrant must include specific descriptions of what agents are looking for and of the place they intend to search. *Id.*

73. *See id.*; *see also Fourth Amendment: An Overview*, LEGAL INFO. INST. (2015), https://www.law.cornell.edu/wex/Fourth_amendment (last visited May 5, 2017).

74. *See Fourth Amendment: An Overview*, *supra* note 73 (explaining "the ultimate goal of this provision is to protect people's right to privacy"); *see also* Oklahoma Press Publ'g. Co. v. Walling, 327 U.S. 186, 205-06 (1946) (noting that the Fourth Amendment has been applicable to corporations also).

75. *Fourth Amendment: An Overview*, *supra* note 73.

76. *Id.* "Private intrusions not acting in the color of governmental authority are exempted from the Fourth Amendment." *Id.*

77. *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 115, 118-20 (1984) (finding that the search and seizure of the cocaine was reasonable and did not violate the Fourth Amendment because the package had already been opened by a private party to whom the Fourth Amendment did not apply); Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (holding that the provision of the Fourth Amendment forbidding unreasonable searches and seizures refers to governmental action).

78. Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 290 (2011).

79. Nicole Fallon, *4 Big Issues Affecting Tomorrow's Workplace*, BUS. NEWS DAILY (Apr. 22, 2015, 7:05 AM), http://www.businessnewsdaily.com/7930-4-big-issues-affecting-tomorrow-s-workplace.html.

> Today, most companies have some kind of BYOD (bring your own device) policy regarding the use of personal tech devices for work purposes. Several years ago, these policies primarily meant smartphones and laptops, but today, employees also have tablets, smart watches, fitness trackers and other Internet-enabled devices—all of which can connect to employer networks and access work data.

Id.

owned.[80] Nonpublic employees need to argue that although they are in the private sector, their personal items, including their Bring Your Own Devices ("BYOD") as well as their private office desks, have a reasonable expectation of privacy and therefore are protected under the Fourth Amendment.[81] Further, specific federal and state statutes on employment law and privacy, as well as administrative rulings, could also provide privacy protection in the private workplace.[82]

In order for the reasonable expectation of privacy to exist, however, one must establish: "(1) that he manifested 'a subjective expectation of privacy' in the item searched or seized, and (2) a willingness by society 'to recognize that expectation as legitimate.'"[83]

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[84]

Arguably, emails, text messages, and information sent through the Cloud fall under this category.[85] This information can be sent to a receiver, who could then pass the information on to a third party, whether by mistake or on purpose.[86] Although there are few Circuit Court decisions that address the issue of Fourth Amendment protection of this kind of information, these decisions hold that there are no Fourth Amendment rights.[87]

---

80. One example of Fourth Amendment rights covering nonpublic companies is California's state constitution. Porten v. Univ. of San Francisco, 64 Cal. App. 3d 825, 829 (Cal. Ct. App. 1976) (holding that the "constitutional provision [Article I, Section I] . . . confers a judicial right of action on all Californians" and "is considered an inalienable right which may not be violated by anyone."). Further, common law provides small measures of protection against excessive monitoring. *Ciocchetti*, *supra* note 78, at 299.

81. *See* James v. Hampton, 592 F. App'x 449, 451, 456-57, 459, 463 (6th Cir. 2015) (holding that former Michigan state court judge's Fourth Amendment rights were violated by a search of her personal safe were sufficient because she had a reasonable expectation of privacy in it, it was not a workplace item, and there was no warrant, probable cause, or exception shown).

82. *See infra* Section III.B. and III.C.

83. Rehberg v. Paulk, 611 F.3d 828, 842 (11th Cir. 2010) (citations omitted).

84. *Id.* at 842-43 (citations omitted).

85. *See id.* at 843-44.

86. *See id.* at 843 ("Here, Rehberg lacked a legitimate expectation of privacy in the phone and fax numbers he dialed.").

87. *See* United States v. King, 55 F.3d 1193, 1195-96 (11th Cir. 1995) (finding that the Fourth Amendment did not protect the defendant because the government received the letter from a private

Brigham City, *Blok*, and the other cases noted in this Part set important guidelines for rights that can subsequently be applied to privacy in the workplace.[88] The exceptions and limitations of the Fourth Amendment may be clearly stated, but when integrated with legislation and administrative decisions, the boundaries of employee monitoring grow blurry.

B. *Administrative Decisions*[89]

"The National Labor Relations Board (NLRB) is an independent federal agency vested with the power to safeguard employees' rights to organize and to determine whether to have unions as their bargaining representative."[90] One issue relevant to privacy in the workplace is concerted activity.[91] The NLRB has consistently held that an employer interferes with its employees' section 7 rights when it prohibits employees from discussing wages with or disclosing wage rates to each other.[92] Issues surrounding electronic communication between employees are prevalent in the workforce, especially matters concerning whether employees can participate in concerted activity through email, and whether employers can monitor these emails.[93] In general, employer monitoring of an employee emails and other electronic devices is "not only legal but also practical, given the nature and reach of electronic

individual). "The Sixth Circuit reasoned that a person would lose a legitimate expectation of privacy in a sent email that had already reached its recipient, analogizing an emailer to a letter-writer, whose expectation of privacy ordinarily terminates upon delivery of a letter." *Rehberg*, 611 F.3d at 843-44, 847 (internal quotations and citations omitted) (holding that plaintiff did not have a privacy right to the phone records requested from his phone service providers and the law regarding his e-mails transmitted over the internet and maintained by a third-party provider was not clearly established).

88. *See supra* Section III.A.

89. Although labor and employment law are often discussed separately, these NLRB administrative cases are used to discuss, on an administrative level, what rights employees' have regarding emails and Internet use. The issue of union organization will not be discussed in depth.

90. *What We Do*, NLRB, https://www.nlrb.gov/what-we-do (last visited May 5, 2017).

91. Concerted activity is defined as activity involving "two or more employees [who] take action for their mutual aid or protection regarding terms and conditions of employment." *Employee Rights*, NLRB, https://www.nlrb.gov/rights-we-protect/employee-rights (last visited May 5, 2017).

92. *See, e.g.*, Koronis Parts, Inc., 324 N.L.R.B. 675, 694 (Oct. 10, 1997); Wilson Trophy Co., 307 N.L.R.B. 509, 512 (May 13, 1992). Section 7 of the NLRA (section 157 of the United States Code) states: "Employees 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 . . . ." National Labor Relations Act, 29 U.S.C. § 157 (2012).

93. *See* RICHARD CARLSON & SCOTT A. MOSS, EMPLOYMENT LAW 259 (Aspen Publishers 3d ed. 2013).

communications."[94] Some scholars argue that an employer can monitor employees' email and website usage because the employer owns the hardware that is being used for communications as well as the network access on which the email has been sent and received.[95] However, these scholars are not considering employees' personal electronic devices, which also can be and frequently are used for emails and other work-related matters.

Recently, the NLRB decided a matter regarding an employee's right to privacy in emails.[96] On December 11, 2014, the NLRB made an unprecedented ruling allowing employees to engage in protected concerted activity on their employer email systems, during off time, absent "special circumstances."[97] This case involved Purple Communications, a company which provides sign-language interpretation services through a video computer call.[98] Employees at Purple Communications had access to the employer's intranet system and various work programs, but the computers had limited, if any, access to the Internet and non-work programs.[99] Each employee was assigned an email account, which he or she had access to at his or her workstations as well as from his or her home computers and smart phones,[100] and "[e]mployees routinely used the work email system to communicate with each other."[101] At some of the company's facilities, there were shared computers in common areas the Internet and non-work programs could be accessed.[102] Since June 2012, the company maintained an employee handbook that contained the company's

94. Jeffrey A. Mello, *Social Media, Employee Privacy and Concerted Activity: Brave New World or Big Brother?*, 63 LAB. L.J. 165, 167 (2012) ("E-mail monitoring has not been found to be unlawful regardless of whether or not employees had been informed of company policy, mainly because the employer usually owns the hardware that is being used for communications as well the network access on which the e-mail has been sent and received."). Employers believe that because employees are being paid by employers to work, employers have the right to make sure they are spending their time efficiently and in a way that is best for the company. *Id.*

95. *See id.*

96. *See* Purple Commc'ns, Inc., 361 N.L.R.B. No. 126, at 1 (Dec. 11, 2014).

97. *See Purple Commc'ns*, 361 N.L.R.B. No. 126, at 5 ("[W]e adopt a presumption that employees who have been given access to the employer's email system to engage in statutorily protected discussions about their terms and conditions of employment while on nonworking time, absent a showing by the employer of special circumstances that justify specific restrictions.").

98. *Id.* at 2. "The Employer's video relay interpreters 'process' calls using company-provided computers located at their workstations." *Id.* at 62.

99. *Id.* at 2-3.

100. *Id.* at 3.

101. *Id.* at 62.

102. *Id.*

electronic communications policy.[103] The union, Communications Workers of America, brought a charge against Purple Communications for committing unfair labor practices by "maintaining rules that unlawfully interfered with employees' rights to engage in protected concerted activity."[104] The Board decided its precedent cases in this area were incorrect in their analysis of an employee's right to protected email communication.[105] The Board found that in certain circumstances, such as discussing union matters, employees had a "reasonable expectation of privacy."[106] Overall, however, the Board found that under the National Labor Relations Act ("NLRA"), employers were allowed to monitor employees' emails.[107]

Another hot topic in the world of labor and employment relations and the NLRB involves employees' use of websites, such as social media platforms like Facebook, to discuss work-related matter outside of working hours, and whether employers are violating employees' right to privacy by monitoring employees' email and website use.[108] This is an

---

103. *Id.* The Court held that this policy restricted employees from concerted activities, including discussion with other employees about salary as well as discussion of the company on social media and other websites. The policy stated the following:

> Computers, laptops, internet access, voicemail, electronic mail (email), Blackberry, cellular telephones and/or other Company equipment is provided and maintained by the. . . Company business. All information and messages stored, sent, and received on these systems are the sole and exclusive property of the Company, regardless of the author or recipient. . . . Employees are strictly prohibited from using the computer, internet, voicemail and email systems, and other Company equipment in connection with any of the following activities. . . . Engaging in activities on behalf of organizations or persons with no professional or business affiliation with the Company. . . . Sending uninvited email of a personal nature.

Id.

104. *See id.* at 61. The charge against Purple Communications also accused Purple Communications of violating section 7 of the NLRA, which discusses the right to organize a union. *Id.* This other charge regarding labor organization is outside the scope of this Note.

105. *Id.* at 1. "By focusing too much on employers' property rights and too little on the importance of email as a means of workplace communication, the Board failed to adequately protect employees' rights under the Act and abdicated its responsibility 'to adapt the Act to the changing patterns of industrial life.'" *Id.*

106. *See id.* at 62.

107. *See id.* at 16. ("An employer's monitoring of electronic communications on its email system will similarly be lawful so long as the employer does nothing out of the ordinary, such as increasing its monitoring during an organizational campaign or focusing its monitoring efforts on protected conduct or union activists. Nor is an employer ordinarily prevented from notifying its employees, as many employers also do already, that it monitors (or reserves the right to monitor) computer and email use for legitimate management reasons and that employees may have no expectation of privacy in their use of the employer's email system.").

108. *See, e.g.*, Three D, LLC v. NLRB, 629 F. App'x. 33, 36 (2d Cir. 2015) ("The Board declined to hold [them] . . . responsible for any other statement posted in the Facebook

issue because monitoring has the possibility of stifling concerted activity, an important employee right, in and outside of the workplace.[109] *Three D, LLC v. NLRB* addresses the issue of concerted activity, social media, and employee monitoring.[110] The case involves a sports bar employer, Triple Play Sports Bar and Grille, who fired employees "after one commented on Facebook that the company mismanaged payroll tax withholding and a second employee added a Facebook 'like' to the posting."[111] The employer claimed it had a right to monitor employees' social media use and that the firings were legal since the posts publicly embarrassed the employer and were detrimental to the company's image.[112] The Board "rejected the employer's claim that the workers' use of obscenities cost them the protection of the federal labor law," and found that the "employees were engaged in a work-related discussion that was protected by the [NLRA]." [113] The Board further held that the firings were unlawful, and the Second Circuit noted that the holding "accords with the reality of modern-day social media use."[114]

The ruling in *Three D, LLC v. NLRB* is crucial because it sets an important boundary in employer monitoring of employee's electronic devices. Employees have little privacy when it comes to the workplace, especially in non-public workplaces.[115] However, even if employers are entitled to monitor employee's emails and website use, they are not allowed to punish employees for concerted activities involving the discussion of their employer and other work-related matters.[116] This protects employees and encourages them to invoke their section 7 rights under of the NLRA.[117] As author Jeffery A. Mello states: "Regardless of whether a workplace is unionized or non-union[ized], [public or non-public,] any employer policy which attempts to impede employees'

discussion . . . .).

109. *See id.* at 36-37.

110. *Id.*

111. *Second Circuit Backs NLRB on Facebook Firings*, BLOOMBERG BNA (Oct. 22, 2015), https://www.bna.com/second-circuit-backs-n57982062581/.

112. *Id.* (Triple Play argued "that airing complaints on an online resource like Facebook was akin to yelling at a manager in front of customers.").

113. *Id.*

114. *Id.* (internal quotations omitted).

115. Mello, *supra* note 94, at 167-68.

116. Protected concerted activity could include online discussion boards, an email between employees who discuss issues related to supervision, and even Facebook postings. *See* Three D, LLC v. NLRB, 629 F. App'x. 33, 35 (warning that too much employer monitoring "could lead to the undesirable result of chilling virtually all employee speech online"); Mello, *supra* note 94, at 170 (discussing that an online bulletin qualified as protected concerted activity).

117. *See* National Labor Relations Act, 29 U.S.C. § 157 (2012); *see also* CARLSON & MOSS, *supra* note 93, at 257.

abilities and rights to communicate outside of the workplace regarding wages, hours, supervision or working conditions would be subject to a [s]ection 7 challenge."[118]

As with the Fourth Amendment, employees have limited rights to privacy (i.e., a "reasonable expectation of privacy") based on court and administrative rulings.[119] These decisions seem to specify a "reasonable expectation of privacy."[120] However, this still does not fully answer one question: To what extent can employers monitor employee's Internet and external digital application use? State and federal privacy statutes must be considered next in order to continue the development of the definition.

C. Statutes and Legislation

Along with the Fourth Amendment and various court decisions, state and federal statutes are used to explore and define the privacy rights of employees.[121] According to Darby and Keller, "[w]hile a number of state and federal statutes may apply to certain monitoring practices, there is no comprehensive privacy legislation tailored to the workplace [on a federal or a state level]. Thus, courts are continuing to develop the law through statutory interpretation and decisions under common law privacy principles."[122] As a result, courts and administrative bodies use "certain laws and causes of actions intended for other purposes to evaluate certain aspects of employee privacy."[123] For instance, some federal statutes, such as the Electronic Communications Privacy Act ("ECPA") and the Computer Fraud and Abuse Act (CFAA), which discuss the intent to prevent wiretapping or hacking of a computer system, have been applied to employee privacy

118. Mello, *supra* note 94, at 172.

119. *See Workplace Privacy and Employee Monitoring*, PRIVACY RTS. CLEARINGHOUSE, https://www.privacyrights.org/workplace-privacy-and-employee-monitoring (last visited May 7, 2017) ("Courts often have found that when employees are using an employer's equipment, their expectation of privacy is limited.").

120. *See, e.g., id.* (discussing a history of decisions discussing limited rights of privacy).

121. *See, e.g.*, 18 U.S.C. § 2510 (2012); 18 U.S.C. § 2707 (2012); N.Y. PENAL LAW § 250.05 (2000).

122. TIMOTHY J. DARBY & WILLIAM L. KELLER, INTERNATIONAL LABOR AND EMPLOYMENT LAWS (4th ed. Cumulative Supplement, Bloomberg BNA 2017). State statutes regarding privacy in the workplace are lacking. However, legislative bills have been proposed and are in discussion. *Id.*

123. Kara Lyons, *Corporate Reputation Management vs. Employee Privacy*, LAW360 (July 29, 2015, 12:39 PM), http://www.law360.com/articles/684280/corporate-reputation-management-vs-employee-privacy.

cases.[124] However, these federal statutes have not proven to be steadfast protections for employees.[125]

Some state constitutions carve out the individual right to privacy, and even those that do not include statutory or constitutional privacy

---

124. *See Electronic Communications Privacy Act (ECPA)*, ELECTRONIC PRIVACY INFO. CTR. https://epic.org/privacy/ecpa/#background (last visited May 7, 2017). "The [ECPA] was passed in 1986 to expand and revise federal wiretapping and electronic eavesdropping provisions." *Id.* It was envisioned to create a fair balance between "the privacy expectations of citizens and the legitimate needs of law enforcement." *Id.* (internal quotations omitted). The ECPA contains the Stored Communications Act, which in the modern context, primarily refers to stored e-mails. *Id.*

> The Act makes it unlawful to intentionally access a facility in which electronic communication services are provided and obtain, alter, or prevent unauthorized access to a wire or electronic communication while it is in electronic storage in such system. . . . Under [the] ECPA, an employer is generally forbidden from accessing an employee's private e-mails.

Id. However, if consent is given in the form of employment policies and an employment contract "that explicitly authorizes the employer to access e-mails, it may be lawful under ECPA for him to do so." *Id.*

> The [CFAA] appears to create criminal liability for an employer who attempts to gain unauthorized access to an employee's personal electronic device and provides for civil liability as well when the unauthorized access causes damages exceeding $–5,000. The law was originally designed to respond to juvenile hackers by prohibiting them from attacking the federal government's computers.

Michael Z. Green, *Against Employer Dumpster-Diving for Email*, 64 S.C. L. REV. 323, 347 (2012).

125. It seems that in today's society of technological innovations, the ECPA is outdated:

> The adoption of cloud computing, while offering many benefits (such as convenience and ease of access), makes the need for ECPA reform more urgent. Whereas an e-mail stored on a home computer would be fully protected by the 4th Amendment warrant requirement, only the Sixth Circuit has ruled that all e-mail stored on a remote, cloud computing server is protected. More and more information, including documents, e-mails, pictures, personal calendars, and locational data is being stored in the cloud. Much of this data has little or no protection under current law. Protections for locational data, in particular, have been widely discussed, but, to date, have not been added.

Electronic Communications Privacy Act (ECPA), *supra* note 124.

> In the employment context, claims under the ECPA have not been widely successful because the law provides a specific exception for interception of communications when the company has a legitimate business interest in monitoring the communications. The Stored Communications Act prohibits an employer from intentionally obtaining, altering, or preventing authorized access to certain stored communications. At least one court has found that an employer violated the Stored Communications Act by firing employees for comments posted on a password-protected MySpace page after the employer obtained, th[r]ough the apparent coercion of one employee, the login and password information for the MySpace page.

Lyons, *supra* note 123. Further, the ECPA, the Stored Communications Act, and the Computer Fraud and Abuse Act can also serve as "hurdles for an employer seeking to view the social media activity of its employees." *Id.*

provisions "recognize the common law tort of invasion of privacy."[126] For example, California has been fairly liberal in its development of privacy laws, giving a constitutional right of privacy for both public and private business entities.[127] "Several states, including Colorado [and New York,] have statutes prohibiting employers from taking any job-related action against an employee based on that employee's lawful conduct off the job."[128] These statutes are known as lifestyle discrimination statutes, and they "typically protect employees who smoke, drink alcohol, consume 'lawful products,' or participate in 'lawful conduct' off-duty and off the employer's premises."[129] They are further used to better protect private employees from discrimination.[130]

Some states have passed laws barring employers from "asking employees or applicants for employment to disclose social media passwords or requiring employees or applicants to allow an employer access to nonpublic information posted through social media."[131] New York's labor law statutes deem surveillance of employees to be an unfair labor practice for an employer, but they do not elaborate on what exactly surveillance means.[132] However, as previously stated,[133] many state statutes vary across the country. Some states have invoked laws that, when interpreted under employment law terms, allow employers to search emails and employees' computers for the "legitimate purpose of the business."[134] Additional differences between state privacy laws

126. Lyons, *supra* note 125.

127. CAL. CIV. CODE § 1798.82(a)-(b) (West 2010) (using the broad term "any").

128. Lyons, *supra* note 123.

129. Jean M. Roche, Note,*Why Can't We Be Friends?: Why California Needs a Lifestyle Discrimination Statute to Protect Employees from Employment Actions Based on Their Off-Duty Behavior*, 7 HASTINGS BUS. L.J. 187, 198 (2011) (citations omitted). If there is no lifestyle discrimination statute in a state, and if an employer finds out "information about any employee's lifestyle that does not precisely comport with the image of the company, the employer can generally fire the employee so long as it does not violate another federal or state discrimination statute." *Id.* at 199.

130. *See id.*

131. Lyons, *supra* note 123; *see also* Julie A. Totten & Melissa C. Hammock, *Personal Devices in the Workplace: Balancing Interests in a BYOD World*, 30 ABA J. LAB. & EMP. LAW 27, 34 (2014). As of August 5, 2014, seventeen states—Arkansas, California, Colorado, Illinois, Louisiana, Maryland, Michigan, New Jersey, New Mexico, Nevada, Oklahoma, Oregon, Rhode Island, Tennessee, Utah, Washington, and Wisconsin—have enacted some type of password protection law. *Id.* at 34 n. 40.

132. *See* N.Y. LAB. LAW § 704 (McKinney 2015).

133. *Infra* Section III.C.

134. *See, e.g.*, ARK. CODE ANN. § 4-110-103(1)(B) (2016). ("'Breach of the security of the system' does not include the good faith acquisition of personal information by an employee or agent of the person or business for the legitimate purposes of the person or business if the personal information is not otherwise used or subject to further unauthorized disclosure.").

include the right of employees to be informed that their email and website use is being monitored.[135]

While there is not one specific bright line rule for workplace privacy laws, uniformity of workplace privacy laws may not be necessary.[136] It is troubling that there is little specification by many of these state statutes as to what surveillance entails and what type of employer monitoring is permissible. The laws either ignore the rights of individual employees or they place heavy restrictions on the employer.[137]

Generally speaking, a constitutional, statutory or common law right to privacy prevents employers from unreasonably intruding into the "seclusion" of their employees. The determination of whether an employer's monitoring of an employee's social media page or email violates the employee's right to privacy will often turn on whether the employee has a "reasonable expectation of privacy."[138]

Before that can happen, one must understand the privacy rights and technology currently available in the workplace, as well as the stance of both employers and employees.

IV. PRIVACY RIGHTS AND TECHNOLOGY IN THE WORKPLACE

"Businesses rely on technology on a daily basis for all manner of work purposes," but now companies are starting to use that technology to create the most efficient products and workplace environments.[139] It

---

135. *See Workplace Privacy and Employee Monitoring, supra* note 120.

> If an e-mail system is used at a company, the employer owns it and is allowed to review its contents. Messages sent within the company as well as those that are sent from your terminal to another company or from another company to you can be subject to monitoring by your employer. This may include Internet-based email accounts such as Gmail and Yahoo as well as instant messages. . . . [E]mployers may monitor calls with clients or customers for reasons of quality control. However, when the parties to the call are all in California, state law requires that they be informed that the conversation is recorded or monitored by either putting a beep tone on the line or playing a recorded message.

Id.

136. *Infra* Section VI.

137. *See* Roche, *supra* note 129, at 190, 194.

138. Lyons, *supra* note 125.

139. Ben Rossi, *Technology and the Workplace of the Future*, INFO. AGE (June 15, 2015), http://www.information-age.com/it-management/strategy-and-innovation/123459663/technology-and-workplace-future; Lisa Sullivan, *The Pros and Cons of Allowing Personal Devices in the Workplace*, THE ARMADA GROUP (Sept. 21, 2014), http://www.thearmadagroup.com/it-infrastructure/the-pros-and-cons-of-allowing-personal-devices-in-the-workplace (Along with

seems as if Cloud computing technology amplifies the battle between employers and employees over the right to privacy. However, in the corporate workplace, "traditional Fourth Amendment protections are frequently not invoked."[140] In some cases, even privacy protections that do exist under the Fourth Amendment are becoming decreasingly robust.[141]

Employers believe all devices should be open for search since some employees use both work and personal devices for work-related transactions and matters. They argue that the monitoring of employees aids in solving the employee disengagement problem.[142] On the other hand, some state privacy laws provide broader privacy rights for employees.[143] For instance, a New York bill requires employers to give employees notice of electronic monitoring.[144] The employees believe that an employer searching through their devices that are used for both work and personal use is a violation of their rights, and the device should therefore be exempt from company searches.[145]

In the public or private sectors, there is some leeway to state that employees have a right to privacy.[146] Such leeway includes "areas set aside for an employee's exclusive use, such as an employee's individual office."[147] However, this leeway is limited.[148] An employee may not have an expectation to privacy in areas "where he or she does not normally work, even if that area contains documents that he or she has

---

efficiency, technology in the workplace "has been linked to the consumerization of IT — an emerging process that's helping to connect companies with customers, develop stronger consumer relations, and increase employee participation and job satisfaction.").

140. *See* Sarah Plotkin Paul, *Dawn Raids Here At Home? The Danger of Vanishing Privacy Expectations for Corporate Employees*, 17 ST. THOMAS L. REV. 265, 265 (2004).

141. *Id.*

142. Karen Higginbottom, *HR Technology Trends in the Workplace in 2015*, FORBES (Jan. 6, 2015, 2:04 PM), http://www.forbes.com/sites/karenhigginbottom/2015/01/06/hr-technology-trends-in-the-workplace-in-2015/ ("Disengaged employees cost the US economy $500 billion per year in lost productivity.").

143. *See State Social Media Privacy Laws*, NCSL (May 5, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx.

144. S. 995, 2015 Reg. Sess. (N.Y. 2015).

145. *See Privacy in the Workplace: Overview*, FINDLAW, http://employment.findlaw.com/workplace-privacy/privacy-in-the-workplace-overview.html (last visited May 7, 2017).

146. *See Privacy in the Workplace: Overview of Privacy in the Workplace,* JUSTIA, https://www.justia.com/employment/privacy/ (last visited May 7, 2017).

147. Paul, *supra* note 140, at 273. This would be an area that "is likely to qualify as an area for which the employee has a privacy expectation." *Id.*

148. *See id.*

helped to prepare."[149] The changing boundaries of the workplace cause further issues in determining privacy rights for employees, as employer-issued laptops or smartphones are used to access social networks or exchange personal text messages.[150]

The Cloud, workplace technology, and BYOD policies plainly benefit both employees and employers. However, with these developments, new privacy and confidentiality issues arise in the workplace.[151] BYOD policies, workplace technology, and the Cloud bring about complications for employers.[152] Control is one important consideration.[153] While IT departments control what sites employees can access on company computers, it is more difficult for them to control what sites and applications employees use on their personal devices.[154] Further, with the use of the Cloud, it has become increasingly difficult for companies to manage what information is kept confidential and what information is released into the Cloud.[155] Employers invest a great deal of resources in developing their products,

149. *Id.* at 273-74.

150. *See* Lisa M. Durham Taylor, *The Times They Are a-Changin': Shifting Norms and Employee Privacy in the Technological Era*, 15 MINN. J.L. SCI. & TECH. 949, 952-53 (2014). "In the past twenty years, businesses and private citizens alike have embraced the use of computers, electronic communication devices, the Internet, and e-mail. As those and other forms of technology evolve, the line separating business from personal activities can easily blur." *Id.* at 953 n.7 (citations omitted).

151. *See* Black, *supra* note 45, at 16; *see also* William A. Herbert, *The Electronic Workplace: To Live Outside the Law You Must Be Honest*, 12 EMP. RTS. & EMP. POL'Y J. 49, 50 (2008) (describing the merger of personal and work-related electronic communications).

152. Ben DiPietro, *Employers Turn to Surveillance to Curb Employee Risk*, WALL STREET J. (Sep. 29, 2015, 10:44 AM), http://blogs.wsj.com/riskandcompliance/2015/09/29/employers-turn-to-surveillance-to-curb-employee-risk/. These complications have led employers to increase resources and efforts towards employee monitoring: "With businesses having to worry about threats encompassing everything from executive misconduct and regulatory noncompliance to workplace violence and insider espionage, more emphasis is being paid to keeping track of what employees are saying and doing when they are on the job and out of the office." *Id.*

153. *See* Black, *supra* note 45, at 17 (One correspondent to the Global Cloud Survey Report 2012 stated: "My basic premise at the moment is if you rely on something totally you need total control so the cloud is not suitable." This perhaps points out a key limitation to cloud adaptation.); *see also The Security, Privacy and Legal Implications of BYOD (Bring Your Own Device)*, *supra* note 16; Sullivan, *supra* note 139.

154. Tony Bradley, *Pros and Cons of Bring Your Own Device to Work*, PCWORLD (Dec. 20, 2011, 10:42 PM), http://www.pcworld.com/article/246760/pros_and_cons_of_byod_bring_your_own_device_.html. "Company-issued IT typically comes with an acceptable use policy, and it is protected by company-issued security that is managed and updated by the IT department." *Id.* BYOD devices are trickier to manage.

155. Black, *supra* note 45, at 19. In the Global Cloud Survey Report 2012, "19% of lawyers surveyed . . . admitted to using public cloud services without the knowledge or approval of their firm." *Id.* at 16. This represents a significant risk for a breach in confidentiality.

services, processes, systems, and methods.[156] "The resulting confidential information often is extremely valuable to the business, and it can be financially devastating if the information is revealed to a competitor or the public."[157] With many of the incidents involving inadvertent disclosures and thefts of confidential information involving company employees, employers believe they are justified in monitoring employee communication on the Internet.[158]

In the past, employers would block certain websites from the workplace, as their use could cause privacy issues and breach client confidentiality.[159] However, as information is sent through the Cloud and employers continue to allow employees to use BYODs, there is less control over what sites and applications are blocked.[160] Control is further decreased with larger companies which have a number of offices in different jurisdictions.[161] This arises both during an employee's time at the company and afterwards.[162] For instance, when an employee is let go, or leaves the company of their own choice, "segregating and retrieving company data [from their BYODs and work-assigned devices] can be a problem."[163]

Employers raise the issue that BYODs cause an increase in employees' usage of devices for personal use during working hours, leading to inefficiency and "worker laziness."[164] Employers justify

156. Tanya E. Milligan, *Virtual Performance: Employment Issues in the Electronic Age*, 38 COLO.LAW., 29, 29 (2009).

157. *Id.*

158. *Id.* For example, to protect their confidential information, Google monitors its employees' electronic activities. In fact, Google "fired an employee after just eleven days of employment for allegedly blogging on the employee's personal website about . . .' 'vague financial-related things.'" *Id.*

159. *See* Black, *supra* note 45, at 17.

160. *See id.* at 12.

161. *See id.* at 20.

162. *See* Bradley, *supra* note 154.

163. *Id.* Retrieving company data is made more difficult by disgruntled employees. Mello, *supra* note 94, at 166-167. "Employers need to ensure that confidential documents, files, information and/or trade secrets are not disseminated to those outside of the organization who have no legitimate business interests in accessing such information." *Id.*

164. *See, e.g.*, Victoria Vessella, *6 Benefits of Employee Monitoring,* BUS. 2 COMMUNITY (Oct. 12, 2015), http://www.business2community.com/human-resources/6-benefits-of-employee-monitoring-01347304#4KGgMvuyb2J0pjKK.97 ("Without a means of tracking their activities, managers are forced to do a lot of guessing about what employees are doing throughout the course of a day."); *see also Bosses Use Tech Tools Track, Manage Workers' Time*, SEATTLE TIMES, http://www.seattletimes.com/business/bosses-use-tech-tools-to-track-manage-workers-time/ (last updated Aug. 18, 2015, 2:39 PM). Employees use employers' computers and other devices to "pay bills, e-mail family and friends, shop for gifts or other personal items, or chat with office colleagues." Milligan, *supra* note 156, at 30. "According to a survey by America Online and

employee monitoring as a way to determine whether employees are actually doing their jobs during work hours.[165] Regardless of the personal information that is caught in the cross fire, employers argue that they should have the ability to monitor all devices that employees use for work-related purposes.[166]

Issues arising for employees typically involve privacy rights and unlawful monitoring.[167] BYODs allow employees to use their own PCs and mobile devices at work, which increases worker satisfaction and decreases operating costs for companies.[168] In addition, many employers expect or at least tolerate personal use on BYODs or on workplace devices by employees because worker efficiency is sometimes increased.[169] While there are some benefits for companies and employees to use BYOD devices, some complications arise.[170] Employees can view this monitoring as an invasion of privacy.[171] This mistrust between employees and employers can have "detrimental effects on employee morale, commitment, performance, retention, and self-esteem."[172] BYOD devices and the public Cloud allow employees to continue their work at home since they are no longer tethered to a

---

salary.com, the average worker admits to wasting more than two hours per eight-hour workday . . . ." on their electronic devices. *Id.*

165. Mello, *supra* note 94, at 166; *see, e.g.,* William P. Smith and Filiz Tabak, *Monitoring Employee E-mails: Is There Any Room for Privacy?* 23 ACAD, OF MGMT. PERSP., 33, 33-35 (2009).

166. *See id.* at 34.

167. *See* David Streitfeld, *New Technologies Track and Assess Employees, But How much is Too Much?*, SYDNEY MORNING HERALD (Aug. 19, 2015, 12:09 PM), http://www.smh.com.au/business/workplace-relations/new-technologies-track-and-assess-employees-but-how-much-is-too-much-20150819-gj2fzm.html (explaining an instance where a woman was required to download an app that tracked all her whereabouts).

168. *See* Bradley, *supra* note 154 ("With the worker paying for most, or all of the costs . . . companies save a lot of money—as much as $80 per month per user. . . . [Employees would] rather use the devices they love rather than being stuck with . . . [the] devices that are selected and issued by the IT department."). *Id.*

169. *See* Brief for Elec. Frontier Found. et al. as Amici Curiae in Support of Respondents at 16-17, City of Ontario v. Quon, 560 U.S. 746 (2010) (No. 08-1332). *But see* Vessella, *supra* note 164 (explaining instead that employers want more efficiency instead of personal use).

170. Bradley, *supra* note 154.

171. Mello, *supra* note 94, at 167. ("Employees can often view electronic monitoring by employers as an invasion of their privacy which serves to erode any trust relationship which exists between employees and employers.").

172. *Id.*; *see, e.g.*, Mia Shopis, *Employee Monitoring: Is Big Brother a Bad Idea?*, SEARCHSECURITY (Dec. 9, 2003), http://searchsecurity.techtarget.com/news/940369/Employee-monitoring-Is-Big-Brother-a-bad-idea (The article is quoting an expert in electronic monitoring who stated that "[e]mployee monitoring is a bad idea . . . when it's used for Big Brother and micromanagement purposes. Organizations would be better off not doing it if they're going to scrutinize their employees' every move. If it creates a morale problem (and it will if it's not handled properly) all of its value is diminished.").

strictly internal work-based network.[173] Besides work-related material on employees' BYOD devices and in the Cloud, employers would have be able to monitor employees' personal activity and have access to employees' photos, footage, and emails.[174] This Orwell-like era of technology may cause many to say employers are crossing the line in terms of privacy.[175]

One such incident involves Amazon and their employee monitoring tactics through BYODs and the Cloud.[176] For instance, investigations show that the company tethers employees to the office outside of normal business hours, be it late night emails or calling in for a meeting on the weekend, which inevitably blurred the line between an employee's work and personal life.[177] Amazon's monitoring technologies "track the minute-by-minute movements and performance of employees . . . ."[178] While Amazon executives tout buzzwords such as "trust," "care for the customer," and "worker efficiency," it seems that the few employee privacy rights which remain are vanishing into thin air.[179] Amazon is not alone in its monitoring tactics.[180] Workplace technology developments now allow white-collar jobs to be "tracked, tweaked, and managed."[181]

---

173. *See* Stuart Dredge, *Why the Workplace of 2016 Could Echo Orwell's* 1984, THEGUARDIAN (Aug. 22, 2015, 7:04 PM), http://www.theguardian.com/technology/2015/aug/23/data-and-tracking-devices-in-the-workplace-amazon. BYOD and the public cloud extend the workplace boundaries. *Id.* However, this is not always a positive: "One of the *worst* things about workplace technology also comes outside the workplace, because all this flexibility often erodes your work/life balance." *Id.* The line between when one is acting as a company's employee and when one is acting as an individual is blurred. *See id.*

174. *See id.* Such employer activities include, monitoring when employees are logged on to their computer, the personal emails sent out, items downloaded, and text messages. *Id.*

175. *See id.*

176. *See Bosses Use Tech Tools to Track, Manage Workers' Time*, *supra* note 164.

177. *See id.* ("Nearly a third of workers in a Gallup poll last year said they were expected to 'check email and stay in touch [on their personal computers or smartphones]' when they were not [at work].")

178. Simon Head, *Worse than Wal-Mart: Amazon's Sick Brutality and Secret History of Ruthlessly Intimidating Workers*, SALON (Feb. 23, 2014, 10:59 AM), http://www.salon.com/2014/02/23/worse_than_wal_mart_amazons_sick_brutality_and_secret_history_of_ruthlessly_intimidating_workers/.

179. *See id.* ("Amazon's system of employee monitoring is the most oppressive I have ever come across and combines state-of-the-art surveillance technology with the system of 'functional foreman,' introduced by Taylor in the workshops of the Pennsylvania machine-tool industry in the 1890s.").

180. Intermex, a money-transfer company based in Miami, requires employees to download an app on their cellphone that tracks their whereabouts 24 hours a day. *Bosses Use Tech Tools to Track, Manage Workers' Time*, *supra* note 164. Additionally, Infobeans, an Indian company headquartered in the United States, began to use a software system called Buddy which monitored the data used by employees. Streitfeld, *supra* note 167.

181. *Bosses Use Tech Tools to Track, Manage Workers' Time*, *supra* note 164.

According to a recent study, this monitoring takes many forms.[182] Regardless of the form of monitoring, "[m]ore than one fourth of employers have fired workers for misusing e-mail and nearly one third have fired employees for misusing the Internet."[183] This makes it even more important for employers to be limited in their searches of employees' devices, since some information is personal and should not be a cause of termination.

Considering both sides, one wonders where to draw the line in employee monitoring. Should different standards be used for different occupations, or should one general monitoring standard control both the public and private workplaces? The determining factor lies on what standard of evaluation is used regarding privacy rights in the workplace.

V. EVALUATION STANDARDS FOR PRIVACY RIGHTS IN THE WORKPLACE

It has been argued that employees only have an expectation of privacy within the boundaries of the "operational realities of the workplace."[184] Without much precedent in regards to Cloud-based software privacy or email privacy, one must look at cases that examine basic privacy issues and privacy issues involving digital devices, such as cellphones.[185]

A. Standard of Reasonableness: O'Connor v. Ortega

O'Connor v. Ortega, a case whose standard is still used in many state and federal courts, involves rights in the workplace under the Fourth Amendment.[186] Officials at a hospital, including Dr. O'Connor, conducted a search of petitioner's, Dr. Ortega's, office because they

182. *See The Latest on Workplace Monitoring and Surveillance*, AMANET, http://www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx (last visited May 7, 2017) ("Computer monitoring takes many forms: [forty-five percent] of employers tracking content, keystrokes, and time spent at the keyboard[;] [forty-three percent] store and review computer files[;] [twelve percent] monitor the blogosphere to see what is being written about the company[;] and [ten percent] monitor social networking sites. Of the [forty-three percent] of companies that monitor e-mail, [seventy-three percent] use technology tools to automatically monitor e-mail and [forty percent] assign an individual to manually read and review e-mail.").

183. *Id.*

184. *See* O'Connor v. Ortega, 480 U.S. 709, 710, 717 (1987).

185. City of Ontario v. Quon, 560 U.S. 746, 750 (2010); *see also* Rehberg v. Paulk, 611 F.3d 828, 835, 839 (11th Cir. 2010).

186. *See O'Connor*, 480 U.S. at 711-12.

suspected him of mismanagement of a residency program.[187] The issue was whether the search violated Dr. Ortega's "reasonable expectation of privacy" guaranteed by the Fourth Amendment.[188] The Supreme Court reversed the lower court, which granted O'Connor's motion for summary judgment, as there may have been a reasonable expectation for the search.[189] Justice O'Connor's view was that "the question whether an employee has a reasonable expectation of privacy [in their workplace] must be addressed on a case-by-case basis."[190] In this case, although hospital officials (representing the hospital) had a right to investigate Ortega's office, they did not have a right to search his desk and file cabinets, as Ortega had a reasonable expectation of privacy in regards to those items.[191] A case-by-case analysis as well as the standard of reasonableness presents a problem for both the courts and the workplace. Cloud-based computing privacy issues may present different issues, which would call for a case-by-case analysis as was used in the *City of Ontario v. Quon*.[192] However, going to court every time an issue like this arises is costly for employers and does not seem to be an effective use of the courts' resources.[193] On another note, while *O'Connor* discusses the right of privacy in the workplace, it does not involve digital devices, including devices for personal and work use.[194] The question of whether the "reasonable expectation of privacy" standard applied to digital devices was lightly addressed in *City of Ontario v. Quon*.[195]

187. *Id.* at 712.

188. *Id.* at 711-12 (As part of the investigation, hospital officials searched the doctor's office several times and seized personal items as well as articles belonging to the state.) *Id.* at 713.

189. *Id.* at 729. Summary judgment was inappropriate in this case because there was evidence that the hospital officials might have had a reasonable belief that there was state property in the office that needed to be secured, and that the scope of the intrusion might have been reasonable in light of this justification. *Id.* at 727.

190. *Id.* at 718.

191. *Id.*

192. City of Ontario v. Quon, 560 U.S. 746, 756-57 (2010) (citations omitted); *see infra* Section V.B.

193. *See Taking Action: The Pros and Cons of Litigation*, THE CONTINUING LEGAL EDUC. SOC'Y OF BRITISH COLUMBIA (Oct. 2010), https://www.cle.bc.ca/PracticePoints/FAM/11-TakingAction.pdf.

194. *See O'Connor*, 480 U.S. at 711-14.

195. *Quon*, 560 U.S. at 758-60.

B. *City of Ontario v. Quon*[196]

In 2010, the Supreme Court ruled on the issue of technology and privacy rights in the workplace in the case *City of Ontario v. Quon*.[197] The case involved a police officer, Quon, who claimed that his Fourth Amendment rights were violated when the police department's chief viewed transcripts of his text messages on his employee-sanctioned alphanumeric pagers.[198] The police chief sought the transcripts to see why police department employees consistently exceeded the character limit on their pagers.[199] When reviewing the transcripts, the chief found that the text messages of two of his police officers, Quon and one other employee, were primarily not work-related.[200] The Supreme Court acknowledged that the case "touches issues of far-reaching significance."[201] The Supreme Court specifically noted that ongoing "[r]apid changes in the dynamics of communication and information transmission" caused similar rapid change "in what society accepts as proper behavior."[202] They therefore suggested prudence when ruling on privacy and technology issues.[203]

Unfortunately, this prudential approach resulted in a Supreme Court decision that was quite ambiguous.[204] The Supreme Court ruled that the City of Ontario police department did not violate Quon's Fourth Amendment rights because reviewing the transcripts was "an efficient and expedient way to determine whether the [employee's] overages were the result of work-related messaging or personal use."[205] Although ruling on the Fourth Amendment question, the Supreme Court refused to rule on the question regarding whether an employee has a reasonable

196. Although *Quon* and *O'Connor* deal with public employees, the analysis here will pertain to nonpublic employees based on the discussion regarding the Fourth Amendment. *See supra* Section III.A.

197. *Quon*, 560 U.S. at 765.

198. *Id.* at 750-53. The City of Ontario issued pagers, that were able to receive text messages, to the city's police department. The City's contract with its service provider limited the number of characters each pager could send or receive on a monthly basis. *Id.* at 750-51.

199. *Id.* at 752. From the facts of the decision, the police chief's primary intention of investigating was not to target certain police officers, but instead he wanted to do the search to see if the existing character limit was too low for officers, and whether overage charges were for work or just personal messages. *Id.*

200. *Id.* at 752-53.

201. *Id.* at 750.

202. *Id.* at 759.

203. *See id.* at 750, 759.

204. *See id.* at 765.

205. *Id.* at 761.

expectation of privacy in a message sent.[206] This decision "place[d] the ball firmly back into the hands of lower federal and state courts" where the *Ortega* precedent still applies.[207]

With the upholding of the *Ortega* precedent, control has been handed to the states to create legislation regarding employees' right to privacy.[208] This solution has not been conflict-free, as violations of privacy or abuses of a company's Cloud-based system are still rampant in the workplace.[209] The Supreme Court's approach has been to avoid "elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[210] The issue is further complicated by the fact that technology continues to develop at a rapid pace, as does society's dependence on it. We cannot keep waiting to enact privacy legislation just because of a possibility of emerging technological developments. In today's society, new technology is always emerging.

VI. SOLUTION: DEFINING A REASONABLE EXPECTATION OF PRIVACY

A. Employee-focused Definition versus Employer-focused Definition

In modifying employees' privacy rights in the workplace, there

206. *Id.* at 765.

207. Lalli, *supra* note 24, at 244-45 (Referring to Ortega's "operational realities of the workplace" standard).

208. One amicus brief points to some states requiring employers to notify employees when monitoring their electronic communications. *See* Brief for N.Y. Intellectual Prop. Law Ass'n as Amicus Curiae In Support of Respondents at 19-20, City of Ontario v. Quon, 560 U.S. 746 (2010) (No. 08-1332).

209. *See infra* Parts IV. & V.

210. *Quon*, 560 U.S. at 759. The reason for this thinking may also be due to the demographic of the Supreme Court, as Supreme Court Justice Elena Kagan stated in 2013, "[t]he justices are not necessarily the most technologically sophisticated people." Will Oremus, *Elena Kagan Admits Supreme Court Justices Haven't Quite Figured Out Email Yet*, SLATE, http://www.slate.com/blogs/future_tense/2013/08/20/elena_kagan_supreme_court_justices_haven_t_gotten_to_email_use_paper_memos.html (last updated Aug. 20, 2013) (internal quotations omitted). This is not to say that people over any certain age are unable to understand technological changes. Some of the justices, such as Alito and Sotomayer, have attempted to comment on the area of technology and the Fourth Amendment. Leary, *supra* note 26, at 71-72. Yet, it is concerning that the majority of people interpreting our laws do not have a full grasp on the concepts they are hearing. *See id.* at 72 ("Justice Alito calls for a legislative response to questions regarding digital surveillance, arguing that the legislature is indeed better equipped to measure societal expectations").

needs to be elucidation on the phrase "reasonable expectations of privacy." Solutions include creating a new standard of evaluation, enacting legislation, or leaving the defining to public and private corporations. By doing this, employees will have a better understanding of when their Fourth Amendment and other privacy rights are being violated.

In the past, courts have routinely found that employees have no reasonable expectation of privacy in their workplace computers when the employer has a policy clearly informing employees that company computers cannot be used for personal e-mail activity and that they will be monitored.[211] Recently, scholars, as well as courts, argue that there seems to be a shift in worker privacy policy.[212] Lisa M. Durham Taylor, in her article *The Times They Are a-Changin': Shifting Norms and Employee Privacy in the Technological Era*, attempts to prove this trend by using several cases, such as *Pure Power Boot Camp v. Warrior Fitness Boot Camp* ("*PPBC*").[213]

In *PPBC*, the court ruled that the defendant had a reasonable expectation of privacy in the workplace.[214] This case hinged on the fact that the defendant was not actually using employer's computer or e-mail system.[215] Instead, the defendant used third-party communication services, which allowed him to use a one-click access application (one of the many cloud-based applications).[216] The court recognized these privacy rights even though the employer's policy expressly negated any privacy rights or expectations in any e-mail that passes through the company's computer system.[217] Taylor argues that subsequent courts addressing employee privacy claims seem to follow in expanding common law protections of employees' technology-based privacy rights.[218]

---

211. *See* United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) ("Therefore, regardless of whether [employee] subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after [employer] notified him that it would be overseeing his Internet use.")

212. *See* Taylor, *supra* note 150, at 990; *see also* Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 561-62 (S.D.N.Y. 2008) (Ruling that the defendant reasonably expected privacy in the e-mail messages he sent, received, and stored on his personal accounts, even though he had accessed his accounts on employer equipment and saved his password, enabling a one-click account entry).

213. *See* Taylor, *supra* note 150, at 990.

214. *Pure Power Boot Camp*, 587 F. Supp. 2d at 561-62.

215. *See id.* at 571.

216. *Id.* at 561-62.

217. *Id.*

218. *See* Taylor, *supra* note 150, at 993; *see, e.g.*, Pietrylo v. Hillstone Rest. Grp., No. 06-5754,

Taylor is correct that privacy law in the workplace has changed over the course of the last decade, as technology now plays a more pervasive role.[219] It is also true that she provides some evidence in favor of a broader reasonable expectation of privacy in the workplace for employees.[220]

Ultimately, Taylor's argument, as well as similar arguments made by other scholars, falls short for two reasons.[221] First, Taylor just skims the surface of the issues in her analysis of privacy laws and the need for more guidance for employers and employees.[222] The cases she cites in her argument do not consider the "operational realities of the workplace," a requirement under the Supreme Court ruling in the *City of Ontario v. Quon*.[223] Her article leaves open the question of whether laws should be created in anticipation of changes or if the law should continue to be flexible and respond rapidly to the ever-changing technology. Further, her argument discussing a recent shift in privacy policy in favor of the employee is not necessarily true in regards to external Cloud-based systems.[224]

Taylor's second reason looks to the rules of agency, specifically the fiduciary duty owed by an employee to his or her employer.[225] Employees generally owe a fiduciary duty of loyalty, care, and good conduct to employers.[226] Therefore, while employed at a company, the

---

2008 WL 6085437, at *1, *6-*7 (D.N.J. July 25, 2008); Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010).

219. As technology is evolving, states are enacting new legislation addressed to specific privacy concerns. *See* Taylor, *supra* note 150, at 1025.

220. *See id.*

221. *See id.* at 956-58.

222. *See id.* at 957.

223. *See generally id.* (discussing cases that deal with these privacy issues); *see also* City of Ontario v. Quon, 560 U.S. 746, 756 (2010).

224. *See* Taylor, *supra* note 150, at 990-99. For instance, in 2012 "Google reduced safeguards for Gmail users, over the objections of many lawmakers and users, when it consolidated privacy policies across its various Internet services." *Google Transparency Report Reveals Risk of Cloud-based Computing*, ELECTRONIC PRIVACY INFO. CTR. (Nov. 14, 2012), https://epic.org/2012/11/google-transparency-report-rev.html.

225. *See* Taylor, *supra* note 150, at 957-58; RESTATEMENT (THIRD) AGENCY § 7.07 (AM. LAW INST. 2006). To determine whether or not an agent can be considered an "employee" in a principal-agent relationship, one must consider various factors. *Id.* For example, whether the principal and agent believe they are creating an employment relationship; whether the type of work done by the agent is customarily done under a principal's direction or without supervision; and whether the principal is or is not in business. *Id.*

226. RESTATEMENT (THIRD) AGENCY § 8.01 (2006). Agency is the fiduciary relationship that arises when one person (a "principal") manifests assent to another person (an "agent") that the agent shall act on the principal's behalf and subject to the principal's control, and the agent manifests assent or otherwise consents so to act. *Id.*; *see also id.* § 8.08, 8.10.

employee must follow certain guidelines, such as the duty not to compete or act for an adverse party.[227]

Furthermore, in terms of fiduciary duties, anything an employee does on the premises of his job (or in uniform) belongs to the employer.[228] These fiduciary duties extend not only to contracted employees, but at-will employees as well.[229] A parallel can be drawn back to the story of the employee at the beginning of this Note.[230] By abusing the company's internal and external Cloud-based system, the employee breached her fiduciary duty owed to her employer, and more specifically her fiduciary duty to the company.[231] Because of incidents like this, as well as incidents where employees use external sites to compete directly with their employer, employers must have the power to monitor what internal and external sites employees are using and what information is being entered or sent using these sites.[232]

An employer may argue that anything done on company devices or any work-related material done on BYODs, unless otherwise noted in the company's policies, is the property of the company.[233] Because of the fiduciary relationship owed to the employer, this means that work

227. EMPLOYMENT LITIGATION § 3.05 (Law Journal Press 2017) ("In the case of an agreement not to compete, the employee generally promises not to engage in or in any way be connected with a competing organization or product or service within a specified geographical area, and for a specified period of time."). "Typically containing time and space limitations, non-compete contracts prohibit employees from competing with their former employers after leaving their employment." T. Leigh Anenson, *Litigation Between Competitors With Mirror Restrictive Covenants: A Formula For Prosecution*, 10 STAN. J.L. BUS. & FIN. 1, 2 n.6 (2005).

228. *See* RESTATEMENT (THIRD) AGENCY § 8.01. This ambiguously includes anything physical or electronic (e.g. paper, brief, computer file, etc.). *Id.*

229. *See* RESTATEMENT (THIRD) AGENCY § 8.01 cmt. c. ("All who assent to act on behalf of another person and subject to that person's control are common-law agents as defined in [section] 1.01 and are subject to the general fiduciary principle stated in this section. Thus, the fiduciary principle is applicable to gratuitous agents as well as to agents who expect compensation for their services, and to employees as well as to nonemployee professionals, intermediaries, and others who act as agents.").

230. *See infra* Part I.

231. *See* RESTATEMENT (THIRD) AGENCY § 8.01, cmt. b.

232. *See* Miriam Schulman, *Little Brother is Watching You*, ISSUES IN ETHICS 100 BUS. & SOC'Y REV. 65, 66 (1998). Employers have legitimate concerns about employees' abusing cloud-based technology and stealing information: "according to the 'Handbook on White Collar Crime', [the use of e-mail in thefts of proprietary information] account for more than $2 billion in losses a year. The transfer of such information can be monitored by programs that search employee e-mails for suspect word strings or by employers simply going into the employee's hard drive and reading the messages." *Id.*

233. This also applies to companies receiving the information, regardless of "employer" status. *See Cloud Computing*, *supra* note 7 ("WebMD's Terms and Conditions of Use, state that information provided to them by e-mail, blog posting, uploading photos or video, or submitting information . . . this information becomes the property of WebMD.").

done either on BYODs or through the Cloud will also be owned by the employer.[234] Thus, the fiduciary relationship argument bolsters the employers' claim to a right to monitor BYOD devices as well as other personal work devices.[235]

B. A New Standard of Review

Still, there is a limit to an employer's monitoring of an employee's emails—that is, the "reasonable expectation of privacy." The most viable option for determining what the bounds are for a reasonable expectation of privacy is an adaptation of the four-part test referenced *In re Asia Global Crossing, Ltd*, a bankruptcy case, which dealt with privileged email communications.[236] The four-part test *In re Asia Global Crossing, Ltd.* was created to measure the employee's expectation of privacy in his computer files and email:

> (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use or monitoring policies?[237]

The objective reasonableness of an employee's intent that his or her personal communications will remain confidential depends on these four

234. *See, e.g.*, Circular 9, *Works Made for Hire*, U.S. COPYRIGHT OFFICE 2 (Sept. 2012), https://www.copyright.gov/circs/circ09.pdf (explaining a work for hire relationship).

235. RESTATEMENT (THIRD) OF AGENCY § 1.01 cmt. g (AM. LAW INST. 2005) ("However ministerial or routinized a work assignment may be, no agent, whether or not an employee, is simply a pair of hands, legs, or eyes. All are sentient and, capable of disloyal action, all have the duty to act loyally.")

236. In re Asia Global Crossing, Ltd., 322 B.R. 247, 257 (S.D.N.Y. 2005) (Finding that a privileged communication does not lose its privileged character for the sole reason that it was sent by e-mail or because persons necessary for the delivery or facilitation of the e-mail may have access to its content. Accordingly, the transmission of a privileged communication through unencrypted e-mail does not, without more, destroy the privilege). "[T]he aggrieved party must show a reasonable expectation of privacy.... [T]he person asserting the right must demonstrate that he has a 'subjective expectation of privacy ... that society accepts as objectively reasonable.' Similarly, one ... must show ... a subjective expectation of privacy and that the expectation is objectively reasonable." *Id.* at 256-57 (citations omitted).

237. *Id.* at 357. Although the case dealt with whether the attorney waived an attorney-client privilege, the four-factor test is still applicable because it still deals with privacy and confidentiality—topics of this Note.

factors.[238] At the same time, the four elements act as a balancing test that fairly considers the interests of both the employer and employee.[239] As opposed to just throwing around the ambiguous phrase "reasonable expectation of privacy," this four factor test,[240] combined with consideration for the operational realties of the workplace, such as size of the company, number of employees, type of business, and cost, can be used to determine whether the monitoring policies impinge on employees' privacy rights or leave employers' unprotected. To deal with BYODs and Cloud computing, a fifth factor needs to be added to define what constitutes reasonable monitoring policies. This fifth factor will compare the company's interest in preventing the "inappropriate and unprofessional" conduct with whether the detriment caused for not monitoring outweighs the alleged violation of employees' privacy rights.[241] In addition, the analysis would be heavily fact-based, so as to minimize the risk that an employer will abuse its monitoring practices.[242]

This four-part (sometimes five-part) test is just one solution for the Cloud-data problem.[243] The issue with this standard is that the Supreme Court refuses to make a decision until technology's place in society is determined.[244] As mentioned previously, technology continues to develop, and therefore its place in society is just that: a continual development. It is not something that should cause distress, but rather something that should be melded into our society's rules and regulations.

C. Legislative Action

The Supreme Court's present refusal to develop a bright-line test suggests that perhaps the best solution in removing the judicial digital divide between the law and technology is to take the burden away from the Supreme Court, and place it instead on the legislature.[245] The

238. *See id.*; *see also* In re Royce Homes, LP, 449 B.R. 709, 735 (S.D. Tex. 2011).

239. *See In re Royce Homes, LP*, 449 B.R. at 735.

240. *See id.*

241. The fifth factor is taken from the ruling in *Smyth v. Pillsbury Co.*, where the court attempted to weigh the interests of employers against the privacy rights of employees. *See* Smyth v. Pillsbury Co. 914 F. Supp. 97, 101 (E.D. Pa. 1996) (finding that Smyth had no "reasonable expectation of privacy" on his employer's system because the company's interest in preventing "inappropriate and unprofessional" conduct outweighed Smyth's privacy rights).

242. *See id.* There will have to be actual evidence or a good argument for what the detriment is so courts don't have employers using this test for trivial matters that don't qualify as a true detriment to the company.

243. *See* In Re Asia Global Crossing, Ltd., 322 B.R. 247, 257 (S.D.N.Y. 2005).

244. *See infra* Section V.B.

245. *See infra* Section V.B.

legislative branch of government is most able to assess privacy concerns and is the most equipped to understand the constrictions on local law enforcement.[246] In essence, legislatures are more likely to accurately measure a reasonable balance between the two.[247] The proposed legislation can protect employees from unnecessary monitoring of their electronic devices, while at the same time carving out exceptions for such monitoring that will help protect employers' legitimate workplace interests.

In regards to legislative rules dealing with Cloud computing and BYOD privacy in the workplace, the legislature can look to recently enacted state statutes that deal with password-protection for employees.[248] These laws protect employees from employer requests for social media usernames and passwords.[249] While these statutes are steps toward protecting the employee, one must not forget about the employer. These state statutes try to maintain a balance between employee and employer interests.[250] For instance, employers have the right and obligation to request an employee's personal social media passwords and postings if they reasonably believe it to be relevant "to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations, provided that the social media is used solely for purposes of that investigation or a related

246. *See* Riley v. California, 573 U.S. _, 134 S. Ct. 2473, 2497-98 (2014).

247. *Id.*

248. Brittanee L. Friedman, Note, *#PasswordProtection: Uncovering the Inefficiencies of, and Not-So-Urgent Need for, State Password-Protection Legislation*, 48 SUFFOLK U. L. REV. 461, 463 (2015).

249. *See* Alan Gutterman, *States Begin Push for Implementation of Employee Password Protection Laws*, LEGAL SOLUTIONS BLOG (Oct. 12, 2012), http://blog.legalsolutions.thomsonreuters.com/law-and-techology/states-begin-push-for-implementation-of-employee-password-protection-laws/ (Discussing California's recent implementation of legislation that prohibits employers "from requiring or requesting that an employee or applicant disclose a username or password for the purpose of accessing personal social media, to access personal social media in the presence of the employer or to divulge any personal social media."). "California, Delaware, Illinois, Maryland, Michigan, and New Jersey have passed laws prohibiting employers . . . from demanding access to social media accounts of employees . . . ." Michelle Poore, *A Call for Uncle Sam to Get Big Brother Out of Our Knickers: Protecting Privacy and Freedom of Speech Interests in Social Media Accounts*, 40 N. KY. L. REV. 507, 508 (2013); *see also* Daniel I. Prywes & Jena M. Valdetero, *Proceed at Your Peril: Questions Abound with New State Laws Restricting Employer Access to Employees' Personal Social Media Accounts*, BLOOMBERG BNA (June 10, 2013), http://www.bna.com/new-state-laws-restricting-employer-access-to-employees-personal-social-media-accounts/ (listing common features among state password-protection laws such as, a ban on employer requests or demands for passwords or access to social media accounts).

250. *See* Gutterman, *supra* note 249.

proceeding."[251] These statutes vary by state in inclusiveness and the balance they strike between employee-employer rights.[252]

As employers seek access to employees' social media usernames and passwords, they also want to be able to monitor employees' smartphones, emails, and other electronic devices, whether the devices are company-owned or personally-owned.[253] With some states enacting laws prohibiting employer-access to employees' social media and usernames, one may wonder whether these statutes signal a shift heavily in favor of employee privacy.[254] Does this mean that employers have no rights to monitoring employees' electronic devices? Arguably, the recent enactment applies only to social media, such as Facebook, Twitter, and other personal platforms, while still allowing for some employee monitoring of email and BYODs.[255] However, these password protection statutes are good starting points for creating employee monitoring legislation that protects the employee from abuse, but they are not so narrow that the employer cannot check emails or BYODs at all. In fact, several states' password protection statutes prohibit access to certain material through electronic communication devices, such as Smart Phones or Tablets.[256] Conceivably, federal or state legislators can enact statutes that allow for employers to monitor BYODs, but are only permitted to monitor work-based applications and employees' emails. This decreases ambiguity and brings society closer to striking an appropriate balance between employer needs and employee privacy.

Individual states can continue to enforce their own privacy regulations. Although the language of these state laws each aim to protect the same employer practices, the laws' inconsistencies create a hazy patchwork of laws of varying scopes.[257] Many of these laws assume a bright-line division between work and personal devices, and

251. *Id.*

252. Friedman, *supra* note 248, at 477 (For example, "Michigan addresses the issue by prohibiting employers from requiring an employee to 'allow observation of' his varied social media activity, whereas Oregon explicitly forbids shoulder-surfing activity and requiring employees to 'friend' employers.").

253. *See Workplace Privacy and Employee Monitoring*, *supra* note 119.

254. *See id.*

255. *See id.*

256. *See* Timothy J. Buckley, Note, *Password Protection Now: An Elakboration on the Need for Federal Password Protection Legislation and Suggestions on How to Draft It*, 31 CARDOZO ARTS & ENT. L.J. 875, 886 (2013).

257. *See* Woodrow Hartzog, *The Second Wave of Global Privacy Protection, Social Data*, 74 OHIO ST. L.J. 995, 1009 (2013) (arguing inconsistencies in social media laws across jurisdictions create difficulty in adequately responding to the issue).

each state may have different divisions.[258] Without a uniform model that includes identical terms and distinctions, these statutes make it "virtually impossible for a multi-state employer to establish a uniform policy."[259] In regards to BYODs and the Cloud, these state statutes are unsustainable in today's society where corporations exist in many states.[260]

Perhaps then, instead of state enacted statutes, Congress should take control and enact a federal statute, which incorporates the best of the reasonable prohibitions and exceptions found in the enacted state laws and bills.[261] The statute would need to clearly define what is protected and what is not, but also leave room for adjustments due to the ever-developing world of technology. This federal legislation can fill the gaps that the inconsistencies in state laws left unanswered.[262] For instance, a statute could prohibit employee monitoring of BYODs and personal devices with exceptions that allow access to electronic communication devices paid for in whole or in part by employers or educational institutions, accounts or services provided by employers or educational institutions, or obtained by virtue of the individual's relationship with the employer or the educational institution, and, in certain circumstances, information that is necessary to ensure compliance with laws, regulations, and prohibitions against work-related misconduct. However, issues may arise with interpretations of this statute in the different Circuit Courts. Without clear guidance from the Supreme Court, the Circuit Courts will be left to interpret whether the statute requires a broad or narrow application, once again leading to inconsistencies within multi-state corporations.[263] This is why it is paramount to include little to no ambiguity in the statute or have the Supreme Court interpret the statute.

D. Internal Regulations

Scholars argue that it is unlikely that Congress will pass an

258. *See id.*

259. *Id.* The parameters for privacy vary from state to state. *See, e.g.*, Buckley, *supra* note 256 ("Maryland and Illinois have prohibited employers, but not educational institutions, from requesting passwords. . . . In contrast, Delaware and New Jersey have prohibited institutions of higher education, but not employers, from requesting the passwords of students and applicants for admission").

260. *See* Hartzog, *supra* note 257, at 1009.

261. *See* Poore, *supra* note 249, at 509.

262. *See* Friedman, *supra* note 248, at 465.

263. *See* Lalli, *supra* note 24, at 245-46.

employee-friendly bill any time soon.[264] Legal indecision leads us to look inward within companies. It is crucial that employers create comprehensive and clear social media and monitoring policies. However, employees need remember their fiduciary duty to the company and make an effort to comply with these policies.

Companies can protect themselves by setting up internal regulations, thereby allowing for a more collaborative workplace environment. Employers will need to review technological security and confidentiality policies and procedures to ensure that company data is protected not only from outside attack, but also from disloyal employees.[265] As they review their polices or enact new policies, companies must be aware that as the traditional physical boundaries of the workplace are quickly becoming obsolete for many employers due to Cloud computing and BYOD, arrangements must be balanced against the potential legal implications of allowing employees to work remotely.[266] Employees will also need to be diligent in making sure the monitoring policies are not too intrusive. Limitations, such as the monitoring only of email and work-related applications and documents, should be emphasized. A company will need to revamp their Internet policies and have employees sign this new agreement so there is a uniform policy for the entire workplace.

Employers can require employees to install applications that require them to log on to their work server in order to be considered actually working (and subsequently in order to be paid). This will signal to the

264. *See* Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 294-304 (2002) (noting the failure of common law and statutory law in the United States to guarantee and adequately protect electronic privacy in the workplace); *see also* Michael Z. Green, *Reading Ricci and Pyett to Provide Racial Justice Through Union Arbitration*, 87 IND. L J. 367, 370 n.12 (2012) (describing initial efforts during President Barack Obama's administration to enact employee-friendly legislation and the unlikely prospects that such legislation will pass any time in the near future).

265. Currently, there is a growing split among federal appellate courts on whether employees with authorization and login credentials to the employer's computer system can be civilly liable for stealing information or breaking confidentiality. "Although five circuit courts of appeals have held that an employee misusing his/her access to information in violation of company policy constitutes 'exceeding authorized access,'" there is a growing minority of circuit courts holding that if an employee is authorized to access his employer's computer systems, that employee's taking of data in violation of company policy does not amount to a violation. *See* Alizah Z. Diamond, *United States: 16 Labor & Employment Resolutions For 2016*, MONDAQ, http://www.mondaq.com/unitedstates/x/455430/employee+rights+labour+relations/16+Labor+Employment+Resolutions+For+2016 (last updated Jan. 4, 2016). As of the publication of this Note, there is no change in the views of the majority.

266. *See* Lalli, *supra* note 25, at 248-49 ("Many market forces have conspired to create this business-personal elision").

employer that anything the employee does can be monitored. Employers can install other applications on employees' computers to impede employee unproductivity. These applications have the ability to block certain websites or applications for a certain amount of time.[267]

It is critical that transparency exists and employees have access to written rules and policies regarding privacy and monitoring of their personal devices.[268] By having these written policies in place, employers will be able to avoid costly lawsuits down the road. To provide a safeguard against superiors who may show bias against certain employees, the monitoring should not be done by the superior, but instead a collaboration between the IT and HR departments. Company executives will establish the guidelines and what the IT and HR coalition should look for in their monitoring.

VII. CONCLUSION

As it currently stands, governmental employees have a constitutionally protected reasonable expectation of privacy, and nonpublic employees find protection in common law as well as state privacy laws.[269] Despite these protections, employers need some kind of monitoring in order to protect the company's interest and especially its confidential information. This applies with equal force to public and private companies.[270] The ability to maintain confidentiality and to rely on the fiduciary duty that exists between a company and its employees are of the utmost priority in the working world.

With the fast-paced development of technology, and the use of BYODs and the Cloud in the workplace, it seems that society may turn

267. *See* SELF CONTROL APP, https://selfcontrolapp.com/ (last visited May 8,2017).

268. "[T]o monitor employee use of [BYODs] employers must . . . obtain employee consent to access content on dual-use devices and ensure that managers do not access private content employees may have stored in order to mitigate the risk of violating the Computer Fraud Abuse Act, the Stored Communications Act or related state laws." Diamond, *supra* note 265.

269. *See* Smith & Burg, *supra* note 18.

270. *See* DiPietro, *supra* note 152 (discussing how Real-Time Technology Group monitors more than 30,000 workers who work in public and private corporations). Even Hillary Clinton, as Secretary of State, was not immune to the duty to protect employer's (or in this case the country's) privacy: "Clinton did sign a Classified Information Nondisclosure Agreement, in which she pledged to safeguard classified information whether 'marked or unmarked classified information, including oral communications,'" but Clinton violated this nondisclosure agreement when she received classified emails on her home server, which were discovered when "the House Select Committee on Benghazi sought her emails at the time of the 2012 attacks and initially was told none could be found." Glenn Kessler, *How Did 'Top Secret' Emails End up on Hillary Clinton's Server?*, WASH. POST. (Feb. 4, 2016), https://www.washingtonpost.com/news/fact-checker/wp/2016/02/04/how-did-top-secret-emails-end-up-on-hillary-clintons-server/?utm_term=.0efb309732ce.

to Congress to enact specific federal regulations as opposed to waiting for the courts to decide. In the meantime, the issue of the legal system playing catch up with technology can be assuaged by companies and their employees working together to create their own privacy policies. The complex legal implications of BYOD and the cloud must be carefully considered using a multi-disciplinary approach (e.g., legal, security, privacy, IT, risk management, etc.) that takes the company's existing infrastructure and risk tolerance into account.

For employers, resisting BYOD is becoming an increasingly untenable policy. Cloud-based software creates new issues and cause for distrust of employers. While employers have a right to monitor employees, they have to keep in mind that they are dealing with human beings.[271] Over extending monitoring policies can hurt morale in the workplace, which is contrary to companies' goals of creating an honest and open environment.[272] However, at the same time, employers must be able to act in what it deems to be its best interests.

Currently federal and state law is outdated in terms of providing a legal framework for technological advancements. The lawmakers are playing a waiting game until technology stops advancing. This method has proven untenable in the workplace. The development of technology is inevitable, and our laws must either adapt with it or be left behind.[273]

*Ashtyn Hemendinger**

271. *See* Schulman, *supra* note 232. ("As thinking actors, human beings are more than cogs in an organization—things to be pushed around so as to maximize profits. They are entitled to respect, which requires some attention to privacy.").

272. *See* Ciocchetti, *supra* note 78, at 6.

273. *See, e.g.*, United States v. Jones, 565 U.S. _, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) ("New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.").

* Ashtyn Hemendinger is a J.D. candidate at the Maurice A. Deane School of Law at Hofstra University, where she anticipates graduation in May of 2017. Ms. Hemendinger is a Notes and Comments Editor of the *Hofstra Labor & Employment Law Journal*. She would like to give a special thank you to her amazing parents, Nancy and Gerald, and her talented sister, Emily, for their unconditional love and support throughout her life ("I do all of this for you guys!"). In addition, Ms. Hemendinger would like to thank William Oswald and her friends for being her cheerleaders these past three years. She would also like to thank her Faculty Advisor, Professor Susan Joffe, for encouraging her to think outside the box and for providing her with expertise and guidance during the writing process. Finally, Ms. Hemendinger would like to thank the current Staff and Managing Board of Volume 34 for their assistance through the publication process.