Contextualizing Bring Your Own Device Policies

Lindsey Blair

Bring Your Own Device (BYOD) policies allow employees to use their devices for workplace functions such as accessing company applications and information. These policies were rapidly adopted in the 2000s, yet time has exposed legal issues for both employers and employees. This Note explores the development of BYOD policies, the risks and benefits for both employers and employees, and advocates for written policy as the primary method to successfully implement a BYOD system. Case law reveals that the three largest issues surrounding BYOD are e-discovery, privacy rights, and compensation: all of which can be mitigated or avoided by a strongly written policy. The Note concludes by providing recommendations for a written policy that outlines both employer and employee responsibilities in the management of personal devices.

I. INTRODUCTION TO BRING YOUR OWN DEVICE POLICIES

Whether a large corporation or a small local business, the need for mobile technology in the workplace has skyrocketed. By 2022, the bring-your-own-device (BYOD) market is predicted to reach nearly $367 billion, which is an unprecedented increase from just $30 billion in 2014.[1] Today, businesses have several mobile strategy options to choose from. However, BYOD is by far the most popular option. BYOD is typically a policy in which an employer allows an employee to bring their personally owned devices into the workplace in order to access company applications and information. Although BYOD initially seemed vastly beneficial, time has exposed issues for both employers and employees. In today's technological society, employers must weigh the risks of adopting a BYOD program against their industry needs, budget, IT, and organizational culture.

This Note explores the development of BYOD policies, the risks and benefits for both employers and employees, and advocates for written policy as the primary method to successfully implement a BYOD system. By analyzing current case law, statutes, and innovative BYOD policies, this Note addresses the three largest issues surrounding BYOD: e-discovery in legal proceedings, compensation, and privacy concerns. This in-depth examination reveals that these issues largely stem from unclear or unstructured policies. Finally, the Note provides recommendations for a strong and defined written policy that outlines both employer and employee responsibilities in the management of BYOD.

II. BYOD IN THE MODERN WORKPLACE AND LEGAL RESPONSES

BYOD policies rapidly expanded during the 2010s in IT communities and have become increasingly common in other professional fields.[2] However, the idea behind BYOD has existed ever since employees began bringing their own flash drives and installing preferred programs on their work computers.[3] Businesses have continually embraced employees' increasing access to technology. This especially is true of mobile devices—in 2015, 64% of Americans owned a smart phone,[4] and according to a TechPro

1. Anna Johansson, *Growth of BYOD Proves It's No Longer an Optional Strategy*, BETANEWS, https://betanews.com/2017/05/12/growth-of-byod-proves-its-no-longer-an-optional-strategy/ (last visited Aug. 26, 2018).

2. Josh McIntyre, *Managing the Risks of Bring Your Own Device Policies*, LANE & WATERMAN LLP (Mar. 9, 2017), https://www.l-wlaw.com/managing-risks-bring-device-policies/.

3. Nima Zahadat et al., *BYOD Security Engineering: A Framework and Its Analysis*, 55 COMPUTERS & SECURITY 81, 81 (Nov. 2015).

4. Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RES. CTR. (Apr. 1, 2015),

study, 74% of employers allow employees to use mobile devices for work purposes—or will within the next 12 months.[5] Employers immediately recognized some of the benefits inherent in BYOD, such as lower hardware and service costs and increased employee mobility and flexibility.[6] However, the law has been slow to address the issues arising from BYOD programs. Currently, there are no statutes directly addressing BYOD policies on a federal or state level. However, case law surrounding BYOD is slowly developing.[7]

A. BYOD E-Discovery Issues Arising in Legal Proceedings

Perhaps the most complex and least anticipated issue that arises with BYOD policies is what happens when the business is facing litigation. This Part focuses on data preservation issues that inherently arise in an e-discovery context. Applying established procedural rules to newly emerging technology presents a dilemma for the courts—and most cases that address discoverability on personal devices have not gone beyond the district court level.[8]

The primary concerns of BYOD policies in e-discovery are accessibility and control. The Federal Rules of Civil Procedure and similar state rules require that information for discovery be "accessible"[9] to the party and in its "possession, custody, or control."[10] However, an inaccessibility claim can be overcome by court order, allowing the requesting party to still seek production of the electronically stored information (ESI).[11] The primary issue then turns on whether an employer is in "control" since BYOD are not within the employer's direct possession. Early courts interpreted this standard to be disjunctive.[12] For example, in *Carrillo v. Schnieder Logistics, Inc.*, the court sanctioned a company for not producing e-mails its employees' sent using a client's e-mail system of a client.[13] However,

---

http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/. In spring of 2011, only 35% of Americans owned a smartphone. *Id.*

5. Teena Maddox, *Research: BYOD booming with 74% using or planning to use*, TECH PRO RES. (Jan. 4, 2015), http://www.techproresearch.com/article/research-byod-booming-with-74-using-or-planning-to-use/.

6. Andrew Taylor, *BYOD vs. CYOD vs. COPE – How to Choose the Right Enterprise Mobility Strategy*, CALERO (Apr. 6, 2017), https://www.calero.com/mobility-service-support/byod-vs-cyod-vs-cope-choose-right-enterprise-mobility-strategy/ (using space data is drawn from an International Data Corporation study).

7. *See generally* Melinda L. McLellan et al., *Wherever You Go, There You Are (with Your Mobile Device): Privacy Risks and Legal Complexities Associated with International 'Bring Your Own Device' Programs*, 21 RICH. J.L. & TECH. 11 (2015) (examining the differences in varying international responses to BYOD).

8. Danielle Richter, *"Bring Your Own Device" Programs: Employer Control Over Employee Devices in the Mobile E-Discovery Age*, 82 TENN. L. REV. 443, 447 (2015).

9. FED. R. CIV. P. 26(b)(2)(B) ("A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.").

10. FED. R. CIV. P. 34. The 2006 amendments focused on e-discovery and clarified that all electronically stored information met the definition of discoverable "documents" under FED. R. CIV. P. 34. Now, drafters seem more focused on reforming discovery in general and the need to reduce the burdens of modern discovery. *See* COMM. ON RULES OF PRACTICE AND PROCEDURE OF THE JUDICIAL CONFERENCE, 113TH CONG., PRELIMINARY DRAFT OF PROPOSED AMENDMENTS TO THE FEDERAL RULES OF BANKRUPTCY AND CIVIL PROCEDURE 281, 281, 289–93, 296, 300–05, 310–11, 314–17 (Comm. Print 2013), http://www.hib.uscourts.gov/news/archives/attach/preliminary-draft-proposed-amendments.pdf.

11. FED. R. CIV. P. 26(b)(2)(B) ("If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause . . . .").

12. *See, e.g.*, Stewart-Warner Corp. v. Staley, 4 F.R.D. 333, 335–36 (W.D. Pa. 1945) (holding that the moving party must, at minimum, claim the documents are in control of the plaintiff).

13. Carrillo v. Schneider Logistics, Inc., No. CV 11-8557-CAS, 2012 U.S. Dist. LEXIS 146903, at *34, *51 (C.D. Cal. Oct. 5, 2012).

the *Ubiquiti Networks, Inc. v. Kozumi USA Corp.* court found that a corporation could not be compelled, absent evidence of a legal right, to produce e-mails from a worker's private account.[14] This Note focuses on four decisions to understand how courts interpret "control" for the purposes of BYOD issues in legal proceedings.

1. In re Pradaxa*: Employer in Control Model*

The first option courts have considered is that employers do have "control" of their employees' devices. From the outset of a complex pharmaceutical products liability case, the plaintiff in *In re Pradaxa*[15] requested that the defendant produce text messages from the defendants' sales representatives.[16] The messages were essential to the plaintiff's case as support for the claims of failure to warn, design defect, and negligent misrepresentation.[17] The defendants did not introduce text messages into the litigation hold until several months later, claiming they "did not realize" the employees had the messages on their personal phones.[18] The defendants also claimed the auto-delete function of SMS systems as an affirmative defense, which the court quickly dismissed.[19] In its decision, the court heavily considered the fact that the defendant had directed employees to use their own phones for work and recognized that "[t]he litigation hold and the requirement to produce relevant text messages . . . applies to that space on employees [personal] cell phones dedicated to the business which is relevant to this litigation."[20] The court awarded the plaintiff nearly one million dollars in financial sanctions.[21]

2. Cotton*: Employer Does Not Have Control Model*

As opposed to the decision *In re Pradaxa*, the district court in *Cotton v. Costco Wholesale Co.* found the employer did not have the same control over the employees' personal devices.[22] In *Cotton*, the plaintiff filed a Motion to compel the Defendant to produce text messages sent and received from two co-workers' personal cell phones as evidence in support of the charges of racial discrimination, harassment, and retaliation.[23]

---

14. Ubiquiti Networks, Inc., v. Kozumi USA Corp., No. 12-cv-2582 CW, 2013 U.S. Dist. LEXIS 53657, at *7, *7–8 (N.D. Cal. Apr. 15, 2013).

15. *In re* Pradaxa (Dabigatran Extexilate) Prod. Liab. Litig., No. 3:12-md-02385-DRH-SCW, 2013 WL 6486921, at *1 (S.D. Ill. Dec. 9, 2013) *rescinded on other grounds In re Boehringer Ingelheim Pharm*., 735 F.3d 216 (7th Cir. 2014).

16. Complaint at 1–2, *In re* Pradaxa, No. 3:13-cv-509009-DRH-SCW, 2013 WL 3171772 (S.D.Ill. June 17, 2013).

17. *In re Pradaxa*, 2013 WL 6486921, at *1, *16.

18. *Id.* at *16.

19. *Id.* at *18. *See also In re Boehringer Ingelheim*, 745 F.3d at 218–20 (overruling *in re* Pradaxa as far as the district court judge's decision to move deposition locations, but not overturning the sanctions for loss of ESI on the mobile devices).

20. *In re Pradaxa*, 2013 WL 6486921, at *18.

21. *Id.* at *18, *20. The court fined the defendants a total of $931,500 based on $500 per case to encourage the defendants to comply with the court's orders. *Id.* at *20. After this decision, the parties settled in May of 2014. Elaine Silvestrini, *Pradaxa Lawsuits*, DRUGWATCH, https://www.drugwatch.com/pradaxa/lawsuits/ (last updated Sept. 13, 2018).

22. Cotton v. Costco Wholesale Co., No. 12-2731-JW, 2013 WL 3819974 (D. Kan. July 24, 2013) (order granting in part and denying in part Motion to Compel Defendant to Search for and Produce Electronically Stored Information and Other Documents and Answer Interrogatories).

23. Memorandum in Support of Plaintiff's Motion to Compel Defendant to Search for & Produce ESI &

However, *Cotton* never mentioned why the co-workers' texts were relevant—rather, the plaintiff relied on the theory that he was entitled to all relevant information to his claim.[24] The defendant argued that there was a lack of evidence in the record regarding the existence of the co-workers' text messages and that it would be an invasion of privacy.[25] The plaintiff's motion was denied and the court stated that the employees' phones were not within the employer's "possession, custody, or control," because the plaintiff failed to contend that "Costco issued the cell phones to these employees, that the employees used the cell phones for any work-related purpose, or that Costco otherwise has any legal right to obtain employee text messages on demand."[26]

Although the courts in *Cotton* and *In re Pradaxa* reached opposite conclusions as to whether the company had to produce its employees' devices, both courts focused on a fact-specific analysis.

3. Small *and* Ewald*: Contrasting Results with Little Analysis*

Two other notable cases involving the preservation of data on mobile devices during e-discovery are *Small v. University Medical Center of Southern Nevada*[27] and *Ewald v. Royal Norweigan Embassy*.[28] In *Small*, an e-discovery special master recommended the "'harsh sanction' of dismissal" for a defendant in an FMLA case for failing to preserve data stored on mobile devices.[29] The defendant failed to issue any litigation hold even after the court, addressing BYOD devices, ordered one after several key employees confirmed they used their personal mobile devices for work-related purposes.[30] The defendant's failure to comply with the hold caused over two years of messages that were potentially relevant to the litigation to be lost.[31] The special master called the defendant's actions "extraordinary misconduct and substantial and willful spoliation of relevant ESI."[32] Although the *Small* and *In re Pradaxa* courts both held the employer in control, the court's analysis in *In re Pradaxa* focused on the employer's consent to use personal device for work-related contexts whereas the *Small* court held actual employee use of personal devices, regardless of permission, was enough to hold the employer to be in control of the messages.[33]

In contrast, the court in *Ewald* allowed production of ESI located on a cell phone provided by the defendant, but the court denied the plaintiff's request for ESI on personal

---

Other Documents & Answer Certain Interrogatories at 6–8, Cotton v. Costco Wholesale Corp., No. 12-cv-2731-JWL/KGS, 2013 WL 381997 (D. Kan. May 3, 2013).

24. *Id.* at *2–*3.

25. Defendant's Response in Opposition to Motion to Compel at 14, Cotton v. Costco Wholesale Corp., No. 12-cv-2731-JWL/KGS, 2013 WL 3819974 (D. Kan. July 24, 2013) [hereinafter Defendant's Response].

26. *Cotton*, 2013 WL 3819974, at *6.

27. Small v. Univ. Med. Ctr. of S. Nev., No. 2:13-cv-00298-APG-PAL, 2014 WL 4079507 (D. Nev. Aug. 18, 2014) (noting the defendant did not have a BYOD policy in place).

28. Ewald v. Royal Norwegian Embassy, No. 11-CV-2116 SRN/SER, 2013 WL 6094600 (D. Minn. Nov. 20, 2013).

29. *Small*, 2014 WL 4079507, at *32.

30. *Id.* at *29.

31. *Id.* at *28.

32. *Id.* at *36.

33. *In re* Pradaxa (Dabigatran Etexilate) Prod. Liab. Litig., No. 3:12-md-02385-DRH-SCW, 2013 WL 6486921, at *16 (S.D. Ill. Dec. 9, 2013).

phones.[34] In this case, the plaintiff brought a gender discrimination and retaliation suit, and requested smart devices used by 12 coworkers.[35] Although the plaintiff showed the defendant had a company policy to store text messages in the official archives, and established the messages existed through email evidence, the court held that the plaintiff "ha[d] not demonstrated her entitlement to such devices."[36] The court did not clarify what circumstances would be appropriate to hold an employer in control, but it is clear from the facts of the case the court considered it a high bar.[37] Both cases provide little legal guidance for their respective outcomes and frustrate the already complicated interpretation of what constitutes control in the context of e-discovery as applied to employee devices.

B. BYOD and the Interaction with Personal Privacy Concerns

Since an employer may have a legal duty to preserve employee data on BYOD devices, it seems natural for the employer to want to monitor a BYOD device to ensure compliance with data retention standards. However, this may raise serious Fourth Amendment concerns in the context of government employers. The Supreme Court, in *City of Ontario v. Quon*, weighed in on this issue when a California police officer sued his department for collecting and reviewing personal text messages on his employer-issued device during the course of an investigation.[38] The Court ruled that the plaintiff's Fourth Amendment rights were not violated, but emphasized the narrow construction of the ruling because "a broad holding concerning employees' privacy expectations . . . might have implications for future cases that cannot be predicted."[39]

The *Quon* Court assumed for the sake of the decision that an employee does have a reasonable expectation of privacy on an employer-issued device. The Court held that the employer in this case did not violate that right because the search was motivated by a "legitimate work-related purpose, and because it was not excessive in scope."[40] Therefore, although the Supreme Court has validated the work-relatedness test, they have not formally ruled as to whether an employee may have a reasonable expectation of privacy in an employer-issued device.

Privacy controls other than the Fourth Amendment also may apply to a private employer's access to BYOD devices. Several states have passed laws requiring employers to notify employees before monitoring their electronic communications.[41] On the federal level, the Stored Communications Act (SCA) protects an individual's right in certain electronic communications.[42] SCA "establishes a civil cause of action against anyone who

34. Ewald v. Royal Norwegian Embassy, No. 11-CV-2116 SRN/SER, 2013 WL 6094600, *28 (D. Minn. Nov. 20, 2013).

35. *Id.* at *1–2.

36. *Id.* at *10.

37. *See id.*

38. City of Ontario v. Quon, 560 U.S. 746, 746 (2010).

39. *Id.* at 760.

40. *Id.* at 748. *See also* O'Connor v. Ortega, 480 U.S. 709, 709 (1987) (finding a non-investigatory work-related purpose reasonable grounds to satisfy the Fourth Amendment).

41. *See* DEL. CODE ANN., tit. 19, § 705 (2005) (codifying notice of monitoring electronic mail and internet usage); CONN. GEN. STAT. § 31–48d (2017) (requiring employers to notify employees prior to electronic monitoring).

42. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1213–14 (2004) (detailing the scope of privacy protections for customers and subscribers of network service providers).

(1) accesses, (2) without authorization, (3) a facility through which an electronic communication service is provided, and (4) thereby obtains access to a wire or electronic communication (5) while it is in electronic storage."[43]

Courts have found that using an employee's password stored on a company-owned device to access a private e-mail violated the SCA.[44] Employers have also been held in violation of SCA for coercing an employee to show an employer an electronic communication protected under the SCA.[45] In addition, under the National Labor Relations Act, if an employer singles out "union-related communications for application of a communications or electronic use policy" the action would constitute a discriminatory application, thus violating the Act.[46] Generally, there is a weak constitutional right to privacy, and, a few federal and state frameworks that provide piecemeal privacy regulation. These sources of protection are often seemingly inconsistent with one another and unclear, which has resulted in varied body of case law as to privacy rights of both public and private employees. As the law continues to develop, having policies in place to handle BYOD issues is in the best interest of both employers and employees.

C. BYOD Windfall Compensation Concerns

According to a 2013 study, 38% of companies might stop providing devices to employees by 2016, while over half of employers will expect employees to supply their own devices by the end of 2017.[47] Although BYOD reduces technology costs, it raises concerns about the ability of companies to pass their operating costs onto their employees, an employee's ability to work "off the clock," and employee's risk in using their personal device for work purposes.

Typically, an employee with a flexible schedule is an employer's dream. However, this may not be the case when faced with a wage-and-hour claim for off-the-clock work. This occurred in *Mohammadi v. Nwabuisi*, in which an employer was found liable for not paying an employee for overtime work, including work coordinated with a personal mobile device.[48] In a more nuanced decision, *White v. Baptist Memorial Health Care Corp.*, an employer policy required employees to record any time disrupted from their meal breaks in order to be compensated, which the plaintiff failed to do after signing a document stating she understood the policy.[49] The court, ruling for the employer, stated "if an employer establishes a reasonable process for an employee to report uncompensated work time the employer is not liable for non-payment if the employee fails to follow the established

43. *See* Johnathan Redgrave et al., *Understanding and Contextualizing Precedents in E-Discovery: The Illusion of Stare Decisis and Best Practices to Avoid Reliance on Outdated Guidance*, 20 RICH. J.L. & TECH. 8, 43 (Mar. 2014) (explaining criteria to establish a private action under the SCA). *See also* 18 U.S.C. § 2707(a) (2012) (listing causes of civil action under the statute). The SCA defines an electronic communication service as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510 (15) (2002).

44. Lazette v. Kulmatycki, 949 F. Supp. 2d 748, 755 (N.D. Ohio 2013).

45. Pietrylo v. Hillstone Rest. Grp., No. 06-5754(FSH), 2009 U.S. Dist. LEXIS 88702, at *8–*9 (D.N.J. Sept. 25, 2009).

46. *See* MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW 354, 373 (3d ed. 2009).

47. Fabio Marino & Teri Nguyen, *Perils of the "Bring Your Own Device" Workplace*, LAW TECH. NEWS ONLINE, Nov. 18, 2013, *available at* LEXIS.

48. Mohammadi v. Nwabuisi, No. 8A:12-cv-00042-DAE, 2013 WL 1966746, at *8 (W.D. Tex. 2013), *aff'd in part, rev'd in part*, 605 Fed. Appx. 329 (5th Cir. 2015).

49. White v. Baptist Memorial Health Care Corp., 699 F.3d 869, 872 (6th Cir. 2012).

process."[50]

Another issue, which was raised in *Cochran v. Schwan's Home Services Inc.*,[51] is whether employers are required to reimburse employees who use their personal devices for work-related purposes. The *Cochran* court, based on Section 2802(a) of California's Labor Code[52], held an employer liable for a "reasonable percentage" of the employee's cell phone bill.[53] The section was "designed to prevent employers from passing their operating expenses on to their employees."[54] The court noted this reimbursement was required for all work-related expenditures, but the requirement even applies if the worker did not incur any additional expenses.[55]

Finally, *Rajaee v. Design Tech Homes, Ltd.*[56] raised the issue of whether an employee could be compensated for employer caused damage to a personal device. In *Rajaee*, the employer remotely wiped the smart device of a sales representative when he resigned—removing both personal and work-related data.[57] The employee brought a suit under the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act.[58] The Fifth Circuit held that a smart device was not a "facility" under the ECPA.[59] The CFAA requires a "loss" defined by "the cost of responding to an offense . . . or other consequential damages incurred because of interruption of service" aggregating to $5,000.[60] The court concluded the plaintiff's loss of photographs and data was not caused by an interruption of service.[61]

BYOD practices may be vastly beneficial to the efficiency and mobility of a company, however, this Part highlights that the law has been slow to respond to the risks inherent to BYOD policies. Case law has varied on how to address e-discovery data preservation, privacy right, wage-and-hour, and cost-shifting issues that have arisen in the context of BYOD.

III. ANALYSIS OF BYOD POLICY ISSUES IN LIGHT OF CURRENT CASE LAW

Law tends to follow technology. The law surrounding BYOD practices has been slow to develop; yet the implementation of such BYOD policies in business settings has risen steeply. When faced with a BYOD concern, courts are put in the position of deferring to stare decisis and using the best law to decide issues of new technology or to avoid

50. *Id.* at 876.

51. Cochran v. Schwan's Home Servs. Inc., 176 Cal. Rptr. 3d 407 (Cal. Ct. App. 2014).

52. CAL. LAB. CODE § 2802(a) (West 2016) ("[a]n employer shall indemnify his or her employee for all necessary expenditures or losses incurred by the employee in direct consequence of the discharge of his or her duties, or of his or her obedience to the directions of the employer. . . .").

53. *Cochran*, 176 Cal. Rptr. 3d at 409.

54. *See* Gattuso v. Harte-Hanks Shoppers, Inc., 169 P.3d 889, 893 (Cal. 2007) (discussing the legislative history of Section 2802 and Section 2804).

55. *Cochran*, 176 Cal. Rptr. 3d at 412. The court also noted the specific details of an employees' plan and whether a third party is paying the employee's bill are irrelevant factors in employer contribution to BYOD expenses. *Id.* at 413.

56. Rajaee v. Design Tech Homes, Ltd., No. H-13-2517, 2014 WL 5878477, at *1 (S.D. Tex. 2014).

57. *Id.*

58. *Id.*

59. *Id.* at *2. The ECPA provided that whoever "intentionally accesses without authorization a facility . . . and thereby obtains . . . electronic communication . . . shall be punished." 18 U.S.C. § 2701(a)(1) (1981).

60. 18 U.S.C. § 1030 (2008).

61. *Rajaee*, 2014 WL 5878477, at *3.

answering important issues relating to developing technological norms.[62]

A. BYOD and E-Discovery Concerns

Innovation has been, perhaps, the crux of American business in the twenty-first century; however, changing technology inherently impacts the realm of electronically stored information. BYOD policies give employees the autonomy to smudge the sharp line between personal and professional roles. This Part addresses the growing divide between law and reality as business models adapt to modern technological trends, while case law continues to defer to outdated established law.

Courts have shifted focus from the "accessible" issue of early ESI decisions to proportionality. In the past, even if the ESI could be accessed through restoration, courts typically allowed at least a sampling of the data. Responding to technological advances, the Federal Rules of Civil Procedure require that requested information be "reasonably accessible"[63] and relevant to the party's claim.[64] Through dicta, courts have also stated that extraordinary efforts are not required for data preservation.[65] Even with these changes, the "not reasonably accessible" test can no longer manage the vast amounts of data available due to new technologies.[66] Rule 26(g) requires certification that discovery is executed proportionally.[67] This rule gives the court discretion to balance the proportionality of the request alongside the accessibility of the communication.

When considering whether the information is accessible, Rule 34 allows for discovery that is within the party's "possession, custody, or control."[68] Possession and custody have been clearly defined by most courts, yet the scope of what constitutes control remains widely debated and varies depending on the jurisdiction. According to some jurisdictions, the definition of control centers on the party's "right, authority, or practical ability to obtain the documents from a non-party to the action,"[69] whereas other courts have held that control exists solely when a party has the legal right to the discoverable information.[70]

There is an inherent tension created by BYOD programs between employer and employee as to the accessibility of potentially discoverable information on a personally owned device. Although a business is likely not in possession or control of an individual device when compared to traditional cases involving work email servers or even company-provided devices, the business may still be considered in control of the ESI. The two

---

62. Redgrave et al., *supra* note 43.

63. FED. R. CIV. P. 26(b)(2)(B).

64. FED. R. CIV. P. 26(b)(1).

65. *See, e.g.*, Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) (discussing the burdensome and costly implications of requiring a party to implement all conceivable preservation methods).

66. Redgrave et al., *supra* note 43, at 14.

67. FED. R. CIV. P. 26(g).

68. FED. R. CIV. P. 34. Rule 34 was last amended in 2015 and codifies existing case law by requiring preservation efforts to be analyzed by a reasonableness standard for parties seeking sanctions for failure to preserve ESI. *Significant Changes to the Federal Rules of Civil Procedure Expected to Take Effect December 1, 2015: Practical Implications and What Litigators Need to Know*, JONES DAY (Sept. 2015), http://www.jonesday.com/significant-changes-to-the-federal-rules-of-civil-procedure-expected-to-take-effect-december-1-12015-practical-implications-and-what-litigators-need-to-know-09-25-2015/.

69. Bank of N.Y. v. Meridien Biao Bank Tanz., Ltd., 171 F.R.D. 135, 146 (S.D.N.Y. 1997). *See also* Chaveriat v. Williams Pipe Line Co., 11 F.3d 1420, 1427 (7th Cir. 1993) (noting that even if information could be obtained by a party by exerting all efforts, it does not mean it is in the party's "possession, custody, or control").

70. *In re* Citric Acid Litig., 191 F.3d 1090, 1107–08 (9th Cir. 1999).

primary opinions cited on this issue, *In re Pradaxa* and *Cotton*, conflict as to whether an employer is in control of a personally owned employee device for e-discovery purposes.

The argument favoring employer control over personal employee devices is voiced in *In re Pradaxa*. The court ultimately held that the defendants had control over their employee's text messages on their personal devices.[71] The court's holding centered largely on the individual circumstances of the case, employing a tailored, fact-specific analysis. Whereas the employer undoubtedly would have been required to preserve text messages stored on a company-issue phone, the duty to produce relevant text messages only applies to the space dedicated to business relevant to the litigation on an employee's personal device.[72] With that holding, the *In re Pradaxa* court maintains that the distinction between personal and private identity is a valid concern in the modern context of employee-owned devices.

The opposite argument that the employer should not be in control of an employee-owned device is adopted in *Cotton*. In reaching its conclusion, the court stated the plaintiff failed to raise three important claims: (1) that the defendant issued the devices containing potentially relevant ESI, (2) "that the employees used the cell phones for any work-related purpose," and (3) that the defendant had "any legal right to obtain employee text messages on demand."[73] Thus, the holding seems to center on plaintiff error rather than substantive discussion of the legal duties of an employer. The court never stated what the outcome would have been if the plaintiff had proven text messages between the employees relevant to the allegations existed or if the employees used their phones for work-related purposes.[74]

Although the *Cotton* and *In re Pradaxa* courts reached opposite conclusions, the rationales underlying the two decisions may not be incongruous. The *Cotton* court enumerated three prongs: possession, custody, and control. These factors would have potentially altered the outcome of the case, whereas the *In re Pradaxa* court weighed the totality of the circumstances and did not list any factors as particularly important to find the employer in control of messages stored on a personal device. Working under the fact-specific decision of *In re Pradaxa*, it seems reasonable to conclude that the plaintiff in *Cotton* did not produce enough evidence to hold the employer was in control of the employee device. Presumably, if the requesting party proves any of the three prongs enumerated by the *Cotton* court, the employer would have to produce the ESI on the employee's cell phones. Therefore, because the plaintiffs in *In re Pradaxa* established that the employer encouraged employees to use their personal devices to communicate with clients, the *In re Pradaxa* defendants would face the same result under the *Cotton* court's implied factors.

Contrarily, *Ewald* complicates the analysis by imposing a high standard of proof

---

71. *In re* Pradaxa (Dabigatran Etexilate) Prod. Liab. Litig., MDL No. 2385 3:12-md-02385-DRH-SCW, 2013 WL 6486921, at *18, *20 (S.D. Ill. Dec. 9, 2013). The court's failure to distinguish between a defendant's duty to preserve emails versus text messages has been highly criticized. In disagreeing, scholars often point to the fact that text messages and emails operate differently—primarily that corporations can control email servers on a systemic level, but cell phones have a specific messaging interface with a mobile carrier. Redgrave, *supra* note 43, at 38.

72. *In re Pradaxa*, 2013 WL 6486921, at *18.

73. Cotton v. Costco Wholesale Corp., No. 12-2731-JW, 2013 WL 3819974, at *6 (D. Kan. July 24, 2013).

74. *See* Richter, *supra* note 8, at 450–51 (addressing other scholars' interpretations of issues raised by the *Cotton* decision). *See also* Jennifer Rearden & Goutam Jois, *Litigation, Legal Holds, and 'Bring Your Own Device'*, 14 DDEE 183 (BNA) (Apr. 10, 2014) (discussing the questions raised by the *Cotton* decision).

before holding an employer in control of employee text messages. The plaintiff provided several different types of seemingly relevant evidence, yet the court still found the plaintiff had not provided enough evidence to entitle her to the messages.[75]

How the *Ewald* opinion fits within *Cotton* and *In re Pradaxa* is less clear. The plaintiffs in *Ewald* and *In re Pradaxa* both showed that there was a company policy to use texting for work-related purposes, but that was enough for the *In re Pradaxa* court to grant the discovery request.[76] Unlike *Cotton*, the *Ewald* court offered no explanation for what evidence could have entitled it to compel the defendant to produce the text messages. The only apparent consistency is that the *Ewald* court also heavily relies on individual facts in its decision. Perhaps a way to distinguish the decision is to look to the nature of the claims. *In re Pradaxa* granted the discovery of work-related text messages from those accused of misrepresenting pharmaceutical material.[77] Conversely, in *Ewald*, the requested production of employees' personal cell phones to search for evidence of discrimination does not permit the same clear division between personal and work-related conversations.

These cases illustrate the ways in which BYOD policies may complicate e-discovery. While it may seem desirable for a company to edge toward less control, the lack of control will lead to missed opportunities to scan the data for relevance and privilege, resulting in less control over the discovery process. Businesses may be operating a BYOD workplace unknowingly without a formal written agreement,[78] and may be held responsible for employee's work-related text messages later on. *Small* and *In re Pradaxa* warn employers of the consequences of not placing a timely litigation hold on all potentially relevant information, including communication held on BYOD devices: harsh sanctions and penalties.[79]

B. BYOD and Employee Privacy Concerns

As discussed in the previous section, companies have to tread carefully to ensure they preserve relevant ESI in litigation or else they could face spoliation problems in court. BYOD programs can complicate the issue of control regarding employee owned devices, largely due to employee privacy concerns.[80] In nearly all states, companies are allowed to monitor their employees' use of the company's network.[81] However, on a BYOD device, the same level of monitoring may not be appropriate due to the personal data being fundamentally intertwined with the professional.

---

75. Ewald v. Royal Norwegian Embassy, No. 11-cv-2116 SRN/SER, 2013 WL 6094600, at *10 (D. Minn. Nov. 20, 2013).

76. *See generally In re* Pradaxa, 2013 WL 6486921.

77. *Id.*

78. This is called shadow IT.

79. Small v. Univ. Med. Ctr. of S. Nev., No. 2:13-cv-00298-APG-PAL, 2014 WL 4079507, at *30 (D. Nev. Aug. 18, 2014). In *Small*, the required preservation would have occurred before the defendant instituted a BYOD policy. *See* Doug Austin, *Failure to Preserve Data on Various Devices Causes Special Master to Recommend Default Judgment*, EDISCOVERY DAILY BLOG (Oct. 15, 2014), https://ediscovery.co/ediscoverydaily/case-law/failure-to-preserve-data-on-various-devices-causes-special-master-to-recommend-default-judgment-edisc/.

80. *See supra* Part II.A (discussing relevant case law regarding data preservation in the context of e-discovery). *See also* Pedro Pavón, *Risky Business: "Bring-Your-Own-Device" and Your Company*, BUS. LAW TODAY (Sept. 2013), https://www.americanbar.org/publications/blt/2013/09/01_pavon.html.

81. *See Workplace Privacy and Employee Monitoring*, PRIVACY RIGHTS CLEARINGHOUSE (May 14, 2018), https://privacyrights.org/consumer-guides/workplace-privacy-and-employee-monitoring (discussing general employee monitoring restrictions within the workplace) [hereinafter *Workplace Privacy*].

In the context of BYOD programs, monitoring a public employee's personal device raises Fourth Amendment privacy concerns. An employee must have a reasonable expectation of privacy in the place being searched for the Fourth Amendment to apply.[82] Unfortunately, there are no existing regulations or case law addressing whether an employee can have a reasonable expectation of privacy in his or her personal device, especially those used for work-related purposes. As more employees subscribe to BYOD policies, there is an increasing need for employers, policymakers, and courts to address this issue head on. Until then, both employees and employers are forced to glean implications from closely related decisions.

However, there have been legal advances as to whether an employee has an expectation of privacy when using company-owned devices. The inferences posed by the Supreme Court in *City of Ontario* are relevant to BYOD programs in two ways. First, if the Court was willing to assume there was a reasonable expectation of privacy of personal data stored on an employer-issued device, then at minimum, the same expectation should exist on a personal device.[83] The manner in which personal ownership is treated in other contexts under the Fourth Amendment lead to the assumption that there may even be an increased expectation of privacy for BYOD devices.[84] Second, in stating that work-related purposes are reasonable, as long as not unduly invasive, the Court provides employers insight on the proper manner in which to conduct litigation holds and monitoring. As a result, agreeing to a BYOD policy reduces the reasonableness of an employee's expectation of privacy.[85]

The Fourth Amendment does not apply to a private employer; however, there are still common law sources for an employee privacy interest. Both of these models effectively require the same thing: the employee's expectation must be reasonable. The right to privacy on a state level is often provided via the tort of intrusion on seclusion.[86] When considering whether an employee has an expectation of privacy in electronic communications, courts have often balanced the following factors: (1) account ownership;[87] (2) device

82. *See The Security, Privacy and Legal Implications of BYOD* (*Bring Your Own Device*), INFOLAWGROUP LLP (Mar. 28, 2012), http://www.infolawgroup.com/blog/2012/03/articles/byod/the-security-privacy-and-legal-implications-of-byod-bring-your-own-device/ (discussing employee privacy in relation to BYOD).

83. Pavón, *supra* note 80.

84. *See* Boyd v. United States, 116 U.S. 616, 630 (1886) (holding personal security, liberty, and private property each are unalienable rights protected by the Constitution under the Fourth Amendment). *But see* Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 304 (1967) (rejecting the notion that property rights are unalienable, but protected only to the extent property interferes with the protection of privacy).

85. *Bring Your Own Device (BYOD) . . . At Your Own Risk*, PRIVACY RIGHTS CLEARINGHOUSE (Sept. 1, 2013), https://www.privacyrights.org/consumer-guides/bring-your-own-device-byod-your-own-risk#4 (last updated Oct. 1, 2014).

86. Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 660 (N.J. 2010) (explaining the common law right to privacy derives from the tort of intrusion on seclusion). Intrusion on seclusion occurs when "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS § 652B (A.L.I. 1977).

87. *See, e.g.*, Mintz v. Mark Bartelstein & Assocs., 906 F. Supp. 2d 1017, 1033 (C.D. Cal. 2012) (stating that the plaintiff had an expectation of privacy in his personal e-mail despite the fact that plaintiff used the account for work-related matters).

ownership;[88] (3) the security level of the communication;[89] (4) published employer policies and whether they were routinely enforced.[90] No one factor is dispositive and often individual courts will often limit the examination to anywhere from two to three factors. Although the common law in most states offers piecemeal protection of privacy, state legislatures have also been slow to respond. State statutes are varied, and currently only two states require employers to provide notice before monitoring electronic communications, such as emails.[91]

The Fourth Amendment, the common law, and individual state codification of rules relating to electronic monitoring have led to a large variance in BYOD treatment of employee privacy. Although the law is still developing and claims have not yet been brought under all of these avenues, the state of existing law suggests employers consider all jurisdictions where a suit may arise before implementing a BYOD policy within the workplace.

C. BYOD Compensation Concerns

Employee compensation concerns regarding BYOD policies have largely fallen into the hands of states to develop and administer. The law generally favors the employer on the issues of data security, wage-and-hour claims, and cost sharing. However, public concern seems to have pushed a few courts and legislators to create innovative solutions to compensation issues inherent to BYOD programs.

1. Employee Rights to Protect Personal Data

Personal data has value. This value rests in the money, time, and the sentimental worth of the data. Examples may range from the money it costs to back-up or replace devices, the time it takes to collect all the data, and the perhaps priceless attributes of certain documents, images, and other information commonly stored on personal devices. In addressing what rights employees have to protect their personal data stored on BYOD devices, *Rajaee* is the first and only court opinion addressing the topic. After the plaintiff's ex-employer wiped both personal and work-related data on the plaintiff's BYOD device, he brought claims under the EPCA and the CFAA.[92] The implication of the dismissal of both claims points to the current trend of narrowly construing statutes applying to electronic

88. *See, e.g.*, Sitton v. Print Direction, Inc., 718 S.E.2d 532, 537 (Ga. Ct. App. 2011) (noting the use of an employee's laptop to review that employee's emails did not invade the employee's privacy).

89. *See, e.g.*, *Mintz*, 906 F. Supp. 2d, at 1033 (explaining the appropriateness of the plaintiff's use of a password on his email account).

90. *See, e.g.*, *In re* Asia Glob. Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005) (establishing a four-prong test to determine the effectiveness of the employer's electronic policies).

91. *See* MARK W. ROBERTSON & ANTHONY DILELLO, STATE BY STATE EMPLOYEE MONITORING LAWS, LAW360 (Apr. 17, 2009), http://docplayer.net/5836112-State-by-state-employee-monitoring-laws.html (including Connecticut and Delaware and mentioning five more prospective state amendments following this trend). *See also* CONN. GEN. STAT. § 31–48d (2008); 19 DEL. CODE ANN. tit. 9, § 708 (2008). There are also several states, which have case law addressing expectation of privacy issues for electronically stored personal data in an employment context. For a detailed analysis of how different states handle privacy rights in different contexts see generally V. JOHN ELLA, A.B.A., EMPLOYEE MONITORING AND WORKPLACE PRIVACY LAW (2016), https://www.americanbar.org/content/dam/aba/events/labor_law/2016/04/tech/papers/monitoring_ella.authcheckdam.pdf.

92. Rajaee v. Design Tech Homes, Ltd., No. H-13-2517, 2014 WL 5878477, at *1–2 (S.D. Tex. 2014).

communications.[93] Recent decisions have held that information stored to a personal hard drive or cell phone is not electronic storage under the statute.[94] This tendency severely restricts the availability of recovery under the ECPA, and completely blocks employees from enforcing rights to information stored on mobile BYOD devices from recovering.

The implication in dismissing the plaintiff's CFAA claim is that an employee has no protection against an employer completely wiping a BYOD device. The literal interpretation of "an interruption of service" has dire consequences for an employee's ability to recover under the act.[95] In addition, the court refused to assign a monetary value to the plaintiff's personal data—making it nearly impossible for an employer to meet the $5000 damage requirement for a mere mobile device.[96] Although this is only one district court decision, which is certainly not binding law, the court followed developing trends in the interpretation of federal statutes addressing electronic data.

2. Is Cost-Sharing the Future of BYOD Implementation?

An employer's objection to paying for all or part of an employee's device based on the argument the employee would pay for the device anyway is not unfounded. After all, 64% of Americans owned a smart phone in 2015.[97] Courts have been slow to respond though, with only one decision from a California appellate circuit court interpreting a California state statute.[98] *Cochran* had vast sway on California's law, yet its influence on other states is uncertain. The court's holding that an employer is always obligated to reimburse an employee for requiring they use their personal device for work-related purposes was based on the equitable theory that an employer would receive a windfall if the statute was not interpreted in this manner.[99] The court's authority is very limited; however, it may still serve as a model for other jurisdictions facing a claim regarding BYOD devices under an existing incurred loss statute similar to California's Labor Code.

For the states that do not have a similar statute to California, there may be a viable argument for employee reimbursement for personal devices under the doctrine of unjust enrichment in common or civil law.[100] At common law, the basic principle is that "[a] person who is unjustly enriched at the expense of another is subject to liability in

93. *See* Deb McAlister, *What Employers and Employees Need to Learn from a Texas Court Case About Smartphone Security*, MKTG. WHERE TECH. INTERSECTS LIFE (May 6, 2016), https://debmcalister.com/2016/05/06/what-employers-and-employees-need-to-learn-from-a-texas-court-case-about-smartphone-security/ (discussing case law influencing the *Rajaee* holding).

94. *See* Garcia v. City of Laredo, 702 F.3d 788, 793 (5th Cir. 2012) (holding that "information that an individual stores to his hard drive or cell phone is not an electronic storage under the statute").

95. *See* Carl Spataro, *Recent Texas Case on BYOD Holds Important Lessons for Employers and Employees Alike*, MOBILEIRON (Mar. 27, 2015), https://www.mobileiron.com/en/blog/recent-texas-case-byod-holds-important-lessons-employers-and-employees-alike (discussing potential consequences of *Rajaee* on future interpretations on the CFAA).

96. *Rajaee*, 2014 WL 5878477, at *1–2; Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2017).

97. Smith, *supra* note 4.

98. Cochran v. Schwan's Home Serv., Inc., 176 Cal. Rptr. 3d 407, 413 (Cal. Ct. App. 2014).

99. *Id.* at 412.

100. *See* Taylor Crousillac, *Bring Your Own Bill? Reimbursing Employee Use of a Personal Cell Phone for Work-Related Purposes*, LA. L. REV. (Mar. 21, 2016), https://lawreview.law.lsu.edu/2016/03/21/bring-your-own-bill-reimbursing-employee-use-of-a-personal-cell-phone-for-work-related-purposes-2/ (discussing application of *Cochran* decision to Louisiana Civil Code article 2298, the codification of the doctrine of unjust enrichment).

restitution."[101] Again, the same relative theory applies—the employer would receive a windfall by shifting the cost of purchasing and maintaining the device, which the employee needs to adequately perform his or her job, to the employee. However, actively acquiescing or signing an employment agreement diminishes an employee's claim to this form of relief.[102]

3. BYOD Wage-and-Hour Pitfalls

Another underdeveloped area of law is potential wage-and-hour issues that arise due to the flexible nature of BYOD programs. Under the Fair Labor Standards Act (FLSA), employers must pay at least minimum wage to non-exempt employees for all hours the employee is "suffered or permitted" to work by the employer, and obligates employers to pay overtime for hours worked over forty hours per week.[103] Under the *Mohammadi* decision, it seems reasonable that this would extend to hours spent responding to emails or time spent communicating for work-related purposes regardless of location.[104]

However, the *White* ruling makes it clear that employers can mitigate the vast expansion of qualifying overtime hours by establishing a reasonable process for reporting overtime.[105] Inherent in the decision is the idea that an employer should have final control over the amount of hours an employee can work.[106] This implies that an employer may also be able to place limits on the scope of after-hour work via BYOD devices.

IV. BYOD POLICY RECOMMENDATIONS AND IMPLEMENTATION GUIDANCE

BYOD policies serve two fundamental goals: to summarize the employee's responsibilities and afford notice of the employer's rights. The legal complications that have arisen in the BYOD context, discussed in the previous sections of this Note, could largely have been prevented by a robust BYOD policy.[107] Employers potentially assume legal, security, and reputational risks when they allow their employees to use their own device for work-related purposes. For this reason, it is important for an employer to maintain control when allowing their employees to use their own devices to store and transfer company data. At the same time, employees often do not trust their employers with personal data and resist employer control over their personal devices.[108] This Part explores the ways in which employers can mitigate risks through a strong written BYOD policy

101. RESTATEMENT (THIRD) OF RESTITUTION & UNJUST ENRICHMENT § 1 (2011).

102. *See* § 2(3) ("There is no liability in restitution for an unrequested benefit voluntarily conferred, unless the circumstances of the transaction justify the claimant's intervention in the absence of contract.").

103. U.S. DEP'T OF LABOR, WAGE AND HOUR DIV., FACT SHEET #22: HOURS WORKED UNDER THE FAIR LABOR STANDARDS ACT (FLSA), DOL.GOV (2008), http://www.dol.gov/whd/regs/compliance/whdfs22.pdf

104. *See* Mohammadi v. Nwabuisi, 605 F. App'x. 329, 332–33 (5th Cir. 2013) (discussing the policy rationales behind ensuring fair compensation of employees under wage-and-hour laws).

105. White v. Baptist Mem'l Health Care Corp., 699 F.3d 869, 872 (6th Cir. 2012).

106. *See id.* (discussing the policy rationales behind maintaining the employer's ultimate control of the workplace).

107. *See supra* Part III (addressing BYOD issues in legal proceedings, privacy concerns, and compensation concerns).

108. *See* Sophie Curtis, *Workers don't trust employers with their mobile data and privacy*, TELEGRAPH (July 17, 2013), http://www.telegraph.co.uk/technology/news/10183765/Workers-dont-trust-employers-with-their-mobile-data-and-privacy.html ("31 per cent [of employees] in the US . . . completely trust their employer to keep personal information private and not use it against them in any way.").

while considering fairness to employees. Therefore, it is important for an employer, when creating or revising a BYOD policy, to consider the following factors.

A. Corporate Data on a BYOD Device

As exhibited by *Ewald* defendants, the biggest risk to companies implementing a BYOD program is corporate data loss.[109] An effective policy should underscore security and clearly provide instructions for what activities are permitted on BYOD devices. Few companies have the infrastructure and resources to protect all corporate data stored on BYOD devices. Instead, many companies are turning to a mobile device management (MDM) service, which offers the software and security tools to protect data. MDM permits a company to complete several key security functions including: encrypting data on mobile devices, remotely locking or wiping devices, tracking the device, creating and enforcing a PIN number, accessing personal data, and tracking worker activity.[110]

Because MDM software gives companies the ability to control and manipulate an employee's personally owned device, the device owner should consent to the MDM software installation, "before installation and should understand exactly what information is collected, how the MDM software is used, which capabilities are enabled, what happens during an incident, and what the employees' expectations are upon termination of employment."[111] Security risk procedures, such as what will happen if an employee reports a missing BYOD device, must be explained in the BYOD policy. In such instances, it is best to have IT disable access to company resources and remotely lock the device.

In cases of security data breaches, MDM software has developed a way to allow programs to run in an isolated environment on the device. This is called "sandboxing," which can then be managed from MDM software.[112] This is a cost-effective way to allow only the portion of the phone containing company data to be encrypted or wiped, while the employee's personal data remains protected. For sandboxing to be effective, corporate data must remain within the sandboxed portion of the phone. Employers implementing BYOD should think carefully before also permitting bring-your-own-app or bring-your-own-cloud policies because a combination makes it difficult for companies to employ sandboxing software to adequately safeguard data and for employees to maintain their privacy.[113]

As employees gradually become aware of their own BYOD risks, it will become harder for companies to implement widespread security solutions and control over BYOD devices. The best practice is to manage sensitive corporate data at the app level rather than at the device level.[114] This ensures that the employee's rights are not infringed upon while managing, updating, modifying, and deleting corporate data from mobile enterprise applications.

---

109. Ewald v. Royal Norwegian Embassy, No. 11-cv-2116 SRN/SER, 2013 WL 6094600, at *10 (D. Minn. Nov. 20, 2013). A company may have the legal obligation or business-related right to protect certain information including: human resources information, health information, confidential or privileged information, financial information, and trade secrets. *See Workplace Privacy*, *supra* note 81.

110. Pavón, *supra* note 80.

111. *Id.*

112. *Id.*

113. *See id.* (describing inevitable "cross-pollination" of corporate data being stored on a third-party cloud).

114. *Workplace Privacy*, *supra* note 81.

B. Comprehension and Consent

Consent is the most powerful tool in implementing a successful BYOD policy. The e-discovery issues in *In re Pradaxa* and *Small* could have been reduced or avoided if the employer would have made the employees aware of and consent to work-related data preservation. A company can control several practices, such as remote data deletion, access to personal data on a device, requirements to save and produce information for e-discovery or legal proceedings, and device costs, as long as it first obtains an employee's consent. Therefore, an employer should obtain consent before implementing a BYOD policy or changing an existing policy.

Communication also plays a critical role in a successful BYOD policy. The policy should appear in a contract for employment, and reappear in an employee manual and when the employee initially installs an employer's MDM software onto the BYOD device. Employers should make sure there is a forum where employees can ask questions about the policies and that someone regularly offers training sessions. Only after the policy has been fully explained should the employer have an employee sign the written policy agreement.

C. Personal Data on a BYOD Device

The best guidance in regard to personal employee data handling is to maintain proportionality within the implementation of a BYOD policy. Implementing policies relevant to the specific job will help to avoid unduly restrictive policies and to maintain employee faith in the policy. An employer should first consider their business-related interests in an employee's BYOD device, and that should be the focus of the BYOD policy. Generally, an employer should avoid accessing an employee's personal data in order to avoid potential Fourth Amendment violations of a public employee's reasonable expectation of privacy, as affirmed by the Supreme Court in *Quon*, or a similar expectation under tort law for private employees. Such access should be limited to relevant work-related data that is best viewed locally, such as SMS messages.[115] Most company resources on BYOD devices can be accessed through the company's server, which reduces the likelihood of violating employee privacy rights regarding their personal device. If the employer retains the right to obtain employee work-related text messages, they gain much more control in the context of e-discovery, and are better able to avoid harsh penalties for failure to produce evidence or comply with litigation holds. Furthermore, if a company complies with e-discovery requirements reflected in their written BYOD policy, but an employee failed to provide the requested communications, the employee, instead of the company, may face sanctions or personal consequences for failing to comply with e-discovery requirements.[116]

Also, if an employer has a device lock or wiping policy, they should urge employees to back up important personal data stored on their devices in case the device is stolen or lost. Current decisions under the ECPA and CFAA make it seem unlikely an employer

115. *See supra* Part III.B (discussing Fourth Amendment reasonable expectation of privacy concerns in regard to BYOD).

116. *See* Small v. Univ. Med. Ctr. of S. Nev., No. 2:13-cv-00298-APG-PAL, 2014 WL 4079507, at *32 (D. Nev. Aug. 18, 2014) (recommending dismissal for a defendant for failing to preserve data stored on mobile devices, and stating employees could be personally sanctioned for failure to comply with litigation holds even though the company had no BYOD policy in place).

would be held liable for damage to personal data for wiping a BYOD device in appropriate circumstances.[117] However, employee awareness is the best way to avoid potential lawsuits down the road.

D. Employee and Employer Rights and Responsibilities

When outlining a BYOD policy, a company should consider which responsibilities and rights it wishes to reserve and what duties it will impose on its employees. The *White* case serves as a testament that under current case law, employers have a lot of flexibility as long as it is contained in the written policy and the employer enforces the policy equally among employees.[118]

An employer must first consider which devices are allowed in a BYOD policy. This may depend on which devices IT can support and apply the appropriate security requirements. Most BYOD workplaces forbid rooted or jail broken devices, as they are more susceptible to malware.[119]

It may be helpful for employers to consider the following common requirements of BYOD policies affecting employees during their employment. Often, employers require an employee to report a lost or stolen device within a certain timeframe.[120] Another thing to consider is whether employees should be required to maintain certain security measures on the device. Employers should also provide a system for hour reporting and outline employee out-of-the-office expectations. Courts thus far have supported the policy rationale that employers should have ultimate control in how many hours an employee works.[121] Therefore, the best way for an employer to maintain control is to define expectations and limitations on business conduct outside of normal business hours on an employee BYOD device.

Device monitoring is likely the most important component of a BYOD policy to define clearly in regards to a worker's employment. Although many policies require the employee to permit access for any enumerated purpose and/or allow monitoring, courts have become increasingly distrustful of such expansive attitudes towards monitoring.[122] Instead, a company should have a legitimate business reason for any access or monitoring. For example, if the company wants to track user activity on its employees' devices in order to record off-work hours it must notify the employee what is being tracked and explain how that information is used and stored. Therefore, best practice requires an employer to provide notice before device monitoring.

Finally, employers should also consider and implement departure requirements for employees leaving the company. These may include deleting corporate data, deleting or monitoring certain apps, and restricting network access to the company.[123] It is important

---

117. *See supra* Part III.C.1 (discussing the court's EPCA and CFAA analysis in *Rajaee*).

118. White v. Baptist Mem'l Health Care Corp., 699 F.3d 869, 877–78 (6th Cir. 2012) (discussing the policy rationales behind maintaining the employer's ultimate control of the workplace).

119. A jail broken device is one containing an unlocked operating system, which allows for the installation of unapproved apps and other software. Rooting is the Android equivalent. *Workplace Privacy*, *supra* note 81; LISA GUERIN, SMART POLICIES FOR WORKPLACE TECHNOLOGIES: EMAIL, SOCIAL MEDIA, CELLLPHONES, & MORE 195–96 (5th ed. 2017).

120. McIntrye, *supra* note 2.

121. *See supra* Part III.C.3 (discussing FLSA and wage-and-hour based court decisions).

122. *Id.*

123. *Workplace Privacy*, *supra* note 81; *Bring Your Own Device to Work (BYOD) Policies: Expert Q&A*,

to outline whether the employees have to carry out the requirements themselves, be supervised in this process, or whether they must turn over their phone to IT to carry out these requirements.

E. BYOD Expenses

As seen in *Mohammadi*, when drafting a BYOD policy, it is vastly important to consider who is monetarily responsible for what.[124] Although only one state has required employers to reimburse employees for costs expended on BYOD programs, an employer may still be on the hook under the doctrine of unjust enrichment or similar state law statues.[125] An employer should provide a clear policy describing which party will bear what costs. Currently, the two most popular policies require the employee to bear all the costs or the company to pay a small stipend, which will often go towards a data plan.[126] Another common option for employers is to provide a stipend to purchase a device, and employees are responsible for any additional cost.[127] Employers in many states have incredible flexibility in their choice of cost bearing, as long as the policy is in writing and clearly communicated to the employee. In any case, a policy should clarify who is responsible for paying for the purchase, replacement, service, and repair of a device. It also may be important for some companies to consider international travelers. For companies that have employees that travel often for work, it will save both parties time and expense to be forthright about reimbursement policies for international data and service fees.

V. CONCLUSION

BYOD programs are not right for every workplace, and careful consideration must be given about the specific company's needs. However, BYOD programs have been tied to increased employee satisfaction, higher performance in the workplace, decreased costs, and increased competitiveness within any given industry.[128] Many of the risks involved in implementing a BYOD workplace can be mitigated through a strong written policy, which clearly assigns employer's rights and employee's responsibilities. However, a written policy is only as good as its implementation. To truly benefit, a business must uniformly and consistently follow its policy to protect itself against the dangers inherent in BYOD programs.

The quick and widespread adoption of bring your own device workplaces within the corporate context highlights that capital often responds faster to innovation than the law. Although often remarkably beneficial to both employers and employees, BYOD programs are not entirely faultless. A company implementing a BYOD program must balance risks against their industry needs, budget, IT, and organizational culture. Case law reveals that the three largest issues surrounding BYOD are e-discovery, privacy rights, and compensation: all of which can be assuaged or completely avoided by a strong, written

---

PLC LABOR & EMPLOYMENT (Mar. 1, 2013), available at Practical Law Resource ID 6-524-2425.

124. Mohammadi v. Nwabuisi, 605 F. App'x 329, 332 (5th Cir. 2015).

125. *See supra* Part III.C.2 (discussing *Cochran* and the future of cost-sharing).

126. McIntyre, *supra* note 2.

127. *Id.*

128. AN OSTERMAN RESEARCH WHITE PAPER, MANAGING BYOD IN CORPORATE ENVIRONMENTS 1 (2013), http://cdn2.hubspot.net/hub/225757/file-599198977-pdf/Managing_BYOD_in_CorporateEnvironments_-_GWAVA.pdf; *See also* Pavón, *supra* note 80.

policy. Actively and uniformly enforcing a BYOD policy is the best mechanism to assuage legal or reputational risks while the law continues to develop around the modern technological workplace.