Tennessee Law Review

Volume 82
Issue 2 *Winter 2015*

Article 5

2015

"BRING YOUR OWN DEVICE" PROGRAMS: EMPLOYER CONTROL OVER EMPLOYEE DEVICES IN THE MOBILE E-DISCOVERY AGE

Danielle Richter

"BRING YOUR OWN DEVICE" PROGRAMS: EMPLOYER CONTROL OVER EMPLOYEE DEVICES IN THE MOBILE E-DISCOVERY AGE

DANIELLE RICHTER*

I. INTRODUCTION

Representing or prosecuting business clients who allow employees to bring their own devices to work presents a unique challenge to a presently undeveloped area of the law. This challenge has created a national split among district courts. Two widely-cited cases within this context are *In Re Pradaxa*[1] and *Cotton v. Costco Wholesale Corp.*[2] This article analyzes both decisions and addresses

---

* Candidate for Doctor of Jurisprudence, University of Tennessee College of Law, May 2015; *Tennessee Law Review*, Managing Editor. I would like to thank Professor Paula Schaefer for encouraging me to write and publish this article and for her guidance throughout the editing process.

1. *In Re* Pradaxa (Dabigatran Etexilate) Products Liab. Litig., No. 3:12-md-02385-DRH-SCW, 2013 WL 6486921 (S.D. Ill. Dec. 9, 2013), *order rescinded on other grounds sub nom., In Re* Boehringer Ingelheim Pharm., 745 F.3d 216, 218–20 (7th Cir. 2014). Judge Posner, writing for the 7th Circuit, overruled *In Re Pradaxa* as far as the district court judge's decision to move deposition locations. Judge Posner did not overturn the sanctions for loss of ESI on the mobile devices.

2. No. 12-2731-JW, 2013 WL 3819974 (D. Kan. July 24, 2013).

the ultimate question: Are employers considered to be in control of employee personal devices for purposes of litigation?

Within the past decade, discovery of electronically-stored information ("ESI") on employee laptops has become common practice. However, with technological increases and the growing appeal of mobile devices, employees now want to use their tablets, smartphones, and other devices at work.[3] Modern technology allows for greater productivity as employees can access company information at any time, in any place.[4] In fact, many would agree that the smartphone itself has become "an extension of its user," nearly eliminating the need for laptops and desktop computers.[5] While the ease of new technology is appealing, it also brings with it new challenges to the discovery process when these devices are involved.

II. THE BYOD PROBLEM IN E-DISCOVERY

Before exploring the e-discovery challenges associated with new technology, this section provides a basic understanding of BYOD programs in the private workplace. This section then analyzes the discovery issues caused by these programs as they relate to the federal rules and the ground-breaking district court opinions of *Pradaxa*, *Cotton*, and *Ewald*.

A. A "BYOD" Primer

Bring Your Own Device ("BYOD") programs are defined as "alternative strateg[ies] allowing employees, business partners, and other users to utilize a personally selected and purchased client device to execute enterprise applications and access data."[6] More simply put, BYOD programs allow employees to use their own personal phones and electronic devices at work and for work.[7] As other commentators have noted, BYOD programs are part of a greater technological revolution often referred to as

---

3. STEPHEN WU, A LEGAL GUIDE TO ENTERPRISE MOBILE DEVICE MANAGEMENT: MANAGING BRING YOUR OWN DEVICE (BYOD) AND EMPLOYER-ISSUED DEVICE PROGRAMS 9 (2013).

4. *Id.* at 9.

5. *Id.* at 10.

6. Susan Ross, *Unintended Consequences of Bring Your Own Device*, LAW TECH. NEWS ONLINE, Mar. 7, 2013, *available at* LEXIS.

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

"consumerization."[8] This term "generally refers to an information technology trend in which business users bring consumer devices, applications, and services into the workplace for use at work."[9]

Of course, in 2014, the term "devices" does not simply include phones and computers anymore. One e-discovery and digital forensics consultant noted that, in the past few years, his firm has extracted ESI from iPhones, iPads, Kindles, Androids, and even an Xbox 360.[10] Another e-discovery forensics expert has collected data from "personal thumb drives [used] to facilitate working from home on personal computers."[11]

Businesses may be unknowingly operating an "informal" BYOD program even without an explicit written agreement governing BYOD-use.[12] This is sometimes referred to as the "shadow IT" phenomenon.[13] For instance, even without a formal BYOD program or agreement, it is highly likely that employees regularly access company servers, data, and information with non-company-owned devices.[14] In fact, even businesses requiring the use of only company-issued devices may have employees using their personal devices, accounts, and resources, without the employer's knowledge.[15] Consequently, even limited BYOD practices may result in recognition of a BYOD program and subsequent responsibility to preserve, search, and produce documents from these devices.

Employees may want to work with their personal technology because they are more comfortable and familiar with it than company-provided devices. However, for employers, the decision regarding whether to allow BYOD practices in the workplace is more challenging. In a traditional work environment, employers usually issue company-owned devices to employees.[16] This "traditional approach" or "non-BYOD approach" allows greater employer control of and access to these devices, which facilitates a smoother discovery process when the company-owned devices are at issue.[17] However, BYOD programs do offer benefits to employers. Aside from

---

8. WU, *supra* note 3, at 9.

9. *Id.*

10. Peter Coons, *iPhones, BlackBerrys and Androids, oh my!*, THE DAILY RECORD: EDISCOVERY UPDATE (Dec. 31, 2013).

11. Erik Hammerquist, *Vendor Voice: BYOD is the No. 1 E-Discovery Challenge for 2014*, LAW TECH. NEWS ONLINE, Jan. 16, 2014, *available at* LEXIS.

12. WU, *supra* note 3, at 19–20.

13. *Id.* at 19.

14. Ross, *supra* note 6.

15. WU, *supra* note 3, at 19.

16. *Id.*

17. *Id.*

accommodating employee requests and desires for new technology, employers can also save money by avoiding the cost of the device and its service.[18] "According to a 2013 global survey of chief information officers conducted by Gartner Inc., 38 percent of companies are expected to stop providing devices to employees by 2016. By 2017, half of employers will expect employees to supply their own devices for work purposes."[19]

B. BYOD in E-Discovery: Accessibility and Proportionality

When opposing counsel has requested ESI located on an employee-owned device, the employer-custodian and his attorney are faced with a tough decision. The employer-custodian's attorney should first look to statutory law to decide whether the requested ESI is discoverable. The Federal Rules of Civil Procedure and similar state rules governing discovery initially require that information be "accessible" to a party and in its "control."[20]

First, Federal Rule of Civil Procedure 26(b), which covers the scope and limitations of discovery, addresses accessibility.[21] Specifically, the rule states that "[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."[22] However, this claim of inaccessibility can be overcome by court order, allowing the requesting party to still seek production of the ESI.[23]

In addition to the requirement of accessibility, Rule 26(b) also requires the information sought to be relevant to a party's claim or defense.[24] Likewise, a court may limit discovery if "the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues."[25] Therefore, courts are given discretion to consider the overall proportionality of the discovery request along with the accessibility

---

18. *Id.*

19. Marino & Nguyen, *supra* note 7.

20. FED. R. CIV. P. 26(b)(1), 26(b)(2)(B), & 34(a)(1)(A).

21. *Id.* at R. 26(b).

22. *Id.* at R. 26(b)(2)(B) (emphasis added).

23. *Id.* at R. 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, considering the limitations of Rule 26(b)(2)(C).").

24. *Id.* at R. 26(b)(1).

25. *Id.* at R. 26(b)(2)(C)(iii).

of the information. The issue of ESI accessibility on BYOD devices is briefly addressed in some of the following cases; however, the crux of discovery of these devices is the issue of control.

During the discovery process, a party may request that the opposing party produce "items in the responding party's possession, custody, or *control*."[26] The relevant questions for discovery purposes then become: Is the employer in control of information stored on an employee-owned device? Do employers have to hold and produce text messages on these devices? Will the employer be liable for failing to produce the requested information? Faced with questions similar to these, the district courts of Illinois, Kansas, and Minnesota have reached differing conclusions. While each case arises in a different context, these decisions offer valuable insight into a rapidly evolving area of law and offer developing legal standards to provide guidance to presently unanswered questions.

C. Pradaxa, Cotton, *and* Ewald*: Control and Proof*

Applying well-established procedural rules to newly emerging technology issues has presented an interesting dilemma for the courts. At this time, most cases addressing ESI discoverability on personal devices have not advanced past the district court level. As these issues multiply, courts at higher levels will undoubtedly be faced with similar cases. Two widely-cited cases in the current BYOD context are *In Re Pradaxa*[27] and *Cotton v. Costco Wholesale Corp.*[28] These cases reached opposite conclusions on the issue of whether employers are considered to be in control of employee personal devices which may contain ESI relevant to litigation. Another key case is *Ewald v. Royal Norwegian Embassy*,[29] which partially denied the requested production of ESI located on personal employee devices but provided a thorough discussion on the importance of proof to a successful claim of employer control over employee devices.[30]

---

26. *Id.* at R. 34(a)(1) (emphasis added).

27. *In Re* Pradaxa (Dabigatran Etexilate) Products Liab. Litig., No. 3:12-md-02385-DRH-SCW, 2013 WL 6486921 (S.D. Ill. Dec. 9, 2013), *order rescinded on other grounds sub nom.*, *In Re* Boehringer Ingelheim Pharm., 745 F.3d 216, 218–20 (7th Cir. 2014). Judge Posner, writing for the 7th Circuit, overruled *In Re Pradaxa* as far as the district court judge's decision to move deposition locations. Judge Posner did not overturn the sanctions for loss of ESI on the mobile devices.

28. No. 12-2731-JW, 2013 WL 3819974 (D. Kan. July 24, 2013).

29. No. 11-CV-2116 SRN/SER, 2013 WL 6094600 (D. Minn. Nov. 20, 2013).

30. *Id.* at *7, *10.

1. *In Re Pradaxa*: Employer Has Control

In Re Pradaxa arises out of years of complex pharmaceutical products liability litigation concerning a prescription medication used to prevent strokes and blood clots in patients with atrial fibrillation.[31] At the time of this writing, the litigation was not resolved, although the manufacturer announced a large settlement in May of 2014.[32] The multidistrict litigation was plagued with discovery disputes and sanctions, primarily arising from the pharmaceutical defendants' alleged failure to preserve various types of evidence, including various "business related text messages" located on employees' cell phones.[33]

Even before the creation of a multidistrict litigation, the original *Pradaxa* plaintiff requested that the pharmaceutical defendants produce relevant text messages from the defendants' sales representatives.[34] In the original complaint, the plaintiff claimed that:

> [p]laintiff's prescribing physician received promotional materials and information from sales representatives of [d]efendants that Pradaxa was more effective than [W]arfarin [sic] in reducing strokes in patients...and was more convenient, without also adequately informing prescribing physicians that there was no reversal agent that could stop or control bleeding in patients taking Pradaxa.[35]

These were categorized as "misrepresentations" by the plaintiff, which "concealed from [p]laintiff and [p]laintiff's physicians the true and significant risks associated with Pradaxa use."[36] The plaintiff went on to cite these alleged misrepresentations against the pharmaceutical defendants in claims for failure to warn, design

---

31. Complaint at 1–2, *In Re Pradaxa*, No. 3-13-cv-51582-DRH-SCW, 2013 WL 6486921 (S.D. Ill. Dec. 9, 2013) [hereinafter *In Re Pradaxa* Complaint].

32. Katie Thomas, *$650 Million to Settle Blood Thinner Lawsuits*, N.Y. TIMES, May 28, 2014, http://www.nytimes.com/2014/05/29/business/international/german-drug-company-to-pay-650-million-to-settle-blood-thinner-lawsuits.html. Press Release, Boehringer Ingelheim, Boehringer Ingelheim Announces Comprehensive Settlement of U.S. Pradaxa (Dabigatran Etexilate) Litigation (May 28, 2014), *available at* http://www.boehringer-ingelheim.com/news/news_releases/press_releases/2014/28_may_2014_dabigatranetexilate.html.

33. *In Re Pradaxa*, 2013 WL 6486921, at *1, *16.

34. *Id.*

35. *In Re Pradaxa* Complaint, *supra* note 31, at 5.

36. *Id.* at 11.

defect, and negligent misrepresentation among others.[37] These text messages between *Pradaxa* sales representatives and prescribing physicians were crucial to the plaintiffs' case.

Despite conceding that the text messages were requested, the defendants did not extend the litigation hold to include text messages until many months later.[38] Defendants claimed they "did not realize" that employees had these business related text messages on their phones and that this was the fault of their employees.[39] The court did not accept this attempt at blame shifting, stating that "[t]he defendants had a duty to ensure that their employees understood that text messages were included in the litigation hold."[40] In fact, the defendants themselves had directed employees to use text messaging for work, as confirmed through various documents in evidence and the deposition of a defendant employee.[41]

The *In Re Pradaxa* court recognized that "[t]here is no question" the defendants were required to preserve employee text messages on company-issued phones.[42] However, in a surprising twist, the court stated 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."[43] Important to the court's analysis was the fact that the defendants had themselves raised the assertion that their employees used their personal phones for business purposes, including text messaging.[44] Addressing any potentially uncooperative employees, the court stated that "[a]ny employee who refuses . . . will be subject to a show cause order of this Court to appear personally in order to determine why he or she should not be held in contempt of Court."[45] These facts were more than enough for the *In Re Pradaxa* court to determine that the defendants had control over their employees' text messages on personal devices, and the court awarded financial sanctions amounting to nearly one million dollars.[46]

---

37. *See generally In Re Pradaxa* Complaint, *supra* note 31 (listing each count for the complaint).

38. *In Re Pradaxa*, 2013 WL 6486921, at *16.

39. *Id.* at *16–17.

40. *Id.* at *17.

41. *Id.* at *16.

42. *Id.* at *17.

43. *Id.* at *18.

44. *Id.*

45. *Id.*

46. *Id.* at *18, *20. The *Pradaxa* plaintiffs requested a corporate fine of $20 million, however, the court ultimately fined the defendants a total of $931,500 based

2. *Cotton v. Costco*: Employer Doesn't Have Control

The district court in *Cotton v. Costco* arrived at a different conclusion than the *In Re Pradaxa* court.[47] In *Cotton*, the plaintiff sued his former employer, Costco Wholesale Corporation ("Costco"), for racial discrimination, harassment, and retaliation.[48] The plaintiff, in his first set of requests for production, asked Costco to produce text messages sent or received from two of his former co-workers' personal cell phones.[49] In his Motion to Compel, the plaintiff stated that "the documents may reveal discriminatory acts against [p]laintiff" which are "live issues in the case."[50] However, in neither the Complaint nor any other document filed by Cotton is there a mention of why text messages were relevant. For example, there is never any mention that the co-workers sent texts or that Cotton received harassing text messages. Rather, Cotton's Motion to Compel takes a general stance that he is entitled to all information that is relevant "to any party's claim or defense," pursuant to Federal Rule of Civil Procedure 26(b)(1).[51] Costco responded that searching these private cell phones would be an invasion of privacy, and it pointed out the lack of evidence in the record regarding the existence of the co-worker text messages.[52]

Whether this request was a "fishing expedition,"[53] as Costco contended, or whether the facts were inadequately pleaded, the *Cotton* court nonetheless found that Costco could not be compelled to

---

on $500 per case for the number of cases pending. These fines were designed to "encourage defendants to respect this Court and comply with its orders." *Id.* at *20. The court acknowledged that more sanctions could follow "to determine what aspects of the plaintiffs' case have been prejudiced or even so damaged as to interfere with their ability to prove what they legally have to prove." *Id.*

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

48. *See generally* Complaint, Cotton v. Costco Wholesale Corp., No. 12-cv-2731-JW/KGS, 2013 WL 3819974 (D. Kan. July 24, 2013) (No. 12-cv-2731-JWL/KGS) [hereinafter *Cotton* Complaint].

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

50. Memorandum in Support of Plaintiff's Motion to Compel Defendant to Search for & Produce ESI & Other Documents & Answer Certain Interrogatories at 11, *Cotton*, 2013 WL 3819974 (No. 12-cv-2731-JWL/KGS) [hereinafter *Cotton* Plaintiff's Motion to Compel].

51. *Id.* at 2–3.

52. Defendant's Response in Opposition to Motion to Compel at 14, *Cotton*, 2013 WL 3819974 (No. 12-cv-2731-JWL/KGS) [hereinafter *Cotton* Defendant's Response]. Cotton did not contest this fact in his reply brief either, as pointed out by the court. *Cotton*, 2013 WL 3819974, at *6, n.17.

53. *Cotton* Defendant's Response, *supra* note 52, at 14.

produce the text messages.[54] Specifically, the court stated that any text messages located on Costco employees' personal cell phones were not within Costco's "possession, custody, or control" because "Mr. Cotton does not 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."[55] Regarding this request for text message production, Cotton's Motion to Compel was denied.[56] As other commentators have pointed out, it is unclear whether the outcome would have been different if Cotton was able to prove that Costco employees were either: (1) discussing him and his allegations via text message or (2) using their personal cell phones for work-related purposes.[57] Notably, neither party in the case framed the issue as one of "possession, custody, or control" of the text messages under the Federal Rules—although the court did so.[58]

3. *Ewald v. Royal Norwegian Embassy*: Text Message Proof

At least one other district court has addressed the importance of proof to a successful claim of employer control over employee personal devices. In *Ewald v. Royal Norwegian Embassy*, plaintiff Ewald brought a gender discrimination lawsuit against her former employer, the Royal Norwegian Embassy.[59] Ewald claimed she was treated differently than her male co-workers and that her employer retaliated against her when she expressed her concerns.[60] The relevant request for production asked to review "the cellular/smart or other phones, memory cards and tablets" used by twelve different individuals (former co-workers identified as key custodians).[61] Plaintiff was successful in compelling the production of evidence located on cell phones provided by the defendant and used by defendant's employees.[62] Similar to *Cotton*, however, the *Ewald*

54. *Cotton*, 2013 WL 3819974, at *6.
55. *Id.*
56. *Id.*
57. Jennifer Rearden & Goutam Jois, *Litigation, Legal Holds, and 'Bring Your Own Device,'* BLOOMBERG BNA: DIGITAL DISCOVERY & E-EVIDENCE, 14 DDEE 183 (April 10, 2014).
58. FED. R. CIV. P. 34(a)(1).
59. Ewald v. Royal Norwegian Embassy, No. 11-cv-2116-SRN/SER, 2013 WL 6094600, at *1 (D. Minn. Nov. 20, 2013).
60. *Id.*
61. *Id.* at *8.
62. *Id.* at *10.

court denied the plaintiff's request for text messages located on a personal phone of an employee of the defendant.[63]

Ewald provided "witness testimony and other evidence" to prove the messages she sought indeed existed.[64] Similar to *Pradaxa*, Ewald noted that the defendant had a company policy to enter text messages into the defendant's "official archives."[65] Ewald also claimed to know the messages existed because texting was frequently referred to as a form of business communication in emails that had already been produced by the defendant.[66] Nevertheless, in a memorandum opinion and order, the *Ewald* court held that the plaintiff "ha[d] not demonstrated her entitlement to such devices, and . . . had ample opportunity to conduct that discovery."[67] The court offered no additional explanation as the court in *Cotton* did to suggest how Ewald could have been "entitled" to compel her former employer to produce text messages located on employee personal cell phones. However, it is clear that the proof Ewald offered in her supporting memorandum was simply not adequate for the Minnesota court.

These cases and those that follow will guide litigants in addressing the BYOD discovery dilemma, however, the general question remains: Does an employer have a duty to preserve and collect information from employees' personal devices? (i.e., does the employer have "possession, custody, or control" over the employee's device?) And furthermore, does the answer to this question hinge on whether the device is used for business purposes? Should the duty turn on whether a requesting party can prove that discoverable information exists on these devices? As courts wind their way through answering these questions, a general framework for guiding future courts has emerged.

III. SOLVING THE BYOD PROBLEM IN E-DISCOVERY: NOW WHAT?

Courts, employers, and attorneys now face reconciliation of the opposite conclusions reached in *Pradaxa* and *Cotton*. The following

---

63. *Id.*

64. *Id.* at *9.

65. *Cotton* Plaintiff's Motion to Compel, *supra* note 50, at 18; Plaintiff's Memorandum of Law in Support of Motion to Compel Discovery at 18, Ewald v. Royal Norwegian Embassy, No. 11-cv-02116, 2013 WL 6094600 (D. Minn. Nov. 20, 2013) (No. 11-cv-2116-SRN/SER) [hereinafter *Ewald* Motion to Compel].

66. *Ewald* Motion to Compel, *supra* note 65, at 18.

67. *Ewald*, 2013 WL 6094600, at *10. The additional discovery the court refers to includes issuing subpoenas, which Ewald asked for a time extension to produce. The importance of subpoenas in these cases are discussed in section III.C, *infra*.

section attempts to provide this guidance. First, a summary of the common legal framework and standards suggested by the *Pradaxa*, *Cotton*, and *Ewald* courts is provided. Then, suggested practice points are given for employers and also for attorneys on both sides of a BYOD discovery dispute.

A. Judicial Guidance: The Unspoken Distinction

Although the *Ewald* plaintiff included more factual grounds to prove that text messages existed than the *Cotton* plaintiff did, the *Ewald* court still did not find them persuasive. In fact, the court minimized the issue despite a substantial discussion of the text messages in both Ewald's memorandum in support of her motion to compel and in the defendant's response.[68] Decisions like *Ewald* and *Cotton* are likely to become the minority approach, as courts begin to develop common standards and rationales for analyzing whether an employer can be compelled to preserve and produce relevant information located on an employee's personal cell phone.

Although court's decisions are currently conflicting, the trend is towards a determination of the purpose for which the employee device was used. Specifically, the determination is whether the employee's device was used for "work-related purposes," a term used in *Pradaxa*,[69] *Cotton*,[70] and more recent cases.[71] Employers are deemed to have "possession, custody, or control" of the requested information when the employee's personal cell phone or device is used for work-related purposes, even if just a "designated space" on the phone is used for this purpose and not the entire phone.[72] This rationale provides guidance for courts but flexibility in allowing a factual determination on a case-by-case basis along with general discovery considerations of accessibility and proportionality.[73]

In addition to the work-related purpose test, courts should also require a sufficient showing of proof that these text messages exist.

---

68. *Ewald* Motion to Compel, *supra* note 65, at 9–10; *Ewald*, 2013 WL 6094600, at *10 (discussing portions of the defendant's response memorandum).

69. *In Re Pradaxa*, No. 3:12-md-02385-DRH-SCW, 2013 WL 6486921 (S.D. Ill. Dec. 9, 2013), *order rescinded on other grounds sub nom*, *In Re* Boehringer Ingelheim Pharm., 745 F.3d 216, 218–20 (7th Cir. 2014).

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

71. *See, e.g.*, Small v. Univ. Med. Ctr. of S. Nev., No. 2:13-cv-00298-APG-PAL, 2014 WL 4079507 (D. Nev. Aug. 18, 2014) (holding that the defendant had an affirmative duty to preserve information on personal mobile phones used for work).

72. FED. R. CIV. P. 34(a)(1); *In Re Pradaxa*, 2013 WL 6486921, at *18.

73. FED. R. CIV. P. 26 advisory committee note.

Movants should provide enough objective facts to convince the court that the requesting party is not going on a "fishing expedition" as the *Cotton* defendant successfully contended.[74] Currently, the standard of proof appears to be a high one, but it has not been well-defined by courts. Additionally, some courts will require the moving party to show how the requested evidence would be favorable to its case.[75] Considering this ambiguous pleading standard, movants would be best served by alleging as much as possible in favor of their position when requesting text messages from employees' personal cell phones.

Mentioning these cases in a "BYOD" context would also unite these opinions and bring clarity to the case law. Of all the cases discussed in this article, only one explicitly mentioned a company having an official BYOD program.[76] However, as discussed above, the term "BYOD" means simply that employees bring their personal electronic devices to work, and use them. Therefore, even absent an official, written, and implemented BYOD program, BYOD practices can still create the same obligation to produce ESI from an employee device in discovery.

B. Employers and BYOD Programs

Admittedly, BYOD is not for everyone. There are some business models and employees who simply have no need to access technology in the workplace.[77] For the majority of employers, however, it is best practice to have a formal BYOD program implemented with clear guidelines that establish expectations for both the employer and the employee, should litigation arise. While BYOD obligations can arise with or without a formal program, having a formal program is recommended. For employees, agreeing to a formal BYOD program clarifies the expectations of their technology use at work. For employers, a formal BYOD program provides more guidance if litigation arises.

Employers should first weigh the pros and cons of an official BYOD program with the assistance of counsel before moving forward with development and implementation. Considerations include the issues discussed in Section II Part A above, as well as the type of data held by the business (sensitive customer information, trade

---

74. *Cotton* Defendant's Response, *supra* note 52, at 14.

75. 49 Mass. Practice, *Discovery* § 7:14 (updated Dec. 2014).

76. *Small*, 2014 WL 4079507, at *10 n.41 (noting that the preservation efforts regarding employees' personal mobile phones all occurred prior to the defendant instituting a BYOD policy in 2014).

77. WU, *supra* note 3, at 19.

secrets, etc.).[78] If an official BYOD program is right for a particular business, the first step is to create and maintain documentation for the program.[79] The most important document will be the written BYOD agreement, which can be included in the employee handbook or created as a stand-alone document.[80]

BYOD agreements may include provisions detailing the diminished expectation of privacy employees have under the program, the security requirements for the employee devices, an acknowledgement that employees are responsible for all costs of the device, and consequences for failure to comply with the program.[81] Agreements may also include a provision addressing the possibility of future litigation and requiring the employee to preserve necessary information relevant to any litigation which may arise. In addition to the agreement itself, employers will need to create procedures for deleting company data from an employee's personal device if the device is stolen or if the employee's employment is terminated.[82] Employers can also "require complex password protection, limit employees' device options or restrict access to particularly sensitive company data."[83]

Next, these policies and procedures need to be implemented in the workplace. An official BYOD program will not get an employer very far if it is not effectively communicated to employees. When the requirements of a BYOD program are not effectively communicated to an employee, the employee may not understand and therefore may not follow the program. Employers need to be transparent and should hold training sessions if necessary to make sure employees understand the diminished privacy they may have by using their personal devices at work.[84] As one commentator remarked, "employers need to practice more transparency in terms of notifying their employees that what they are doing with their smartphones may be subject to a legal process."[85] Compliance and continued education about technology in the workplace will protect the

---

78. *Id.* at 18.

79. *Id.* at 20.

80. BRING YOUR OWN DEVICE TO WORK (BYOD) POLICY (Feb. 2014), *available at* Practical Law Resource ID 1–521–3920.

81. *Id.*

82. *Bring Your Own Device to Work (BYOD) Policies: Expert Q&A*, PRACTICAL LAW, Mar. 1, 2013, *available at* Practical Law Resource ID 6-524-2425.

83. *Id.*

84. BRING YOUR OWN DEVICE TO WORK (BYOD) POLICY, *supra* note 80.

85. Meagan Crowley-Hsu, *E-Discovery Trends: 2014 Year in Review*, PRACTICAL LAW, Nov. 15, 2014, *available at* Practical Law Resource ID 3-588-7525.

employer if they are involved in litigation in the future.[86] The bottom line employers should remember is this: While a court may take in to consideration whether a company has implemented an official written BYOD program, employees may still use their personal devices at work, and even informal BYOD practices in the workplace can implicate serious consequences when litigation arises.

For employers who refuse to implement a BYOD program, the second-best option would be to issue employer-owned devices for employees to use for work purposes and to be clear about the separation between their work phone and personal phone. This option ensures that employers have adequate control over these employee-used phones when litigation arises. However, this option will only be effective if employees actually comply with the employer's policy and do not covertly use their personal cell phones for work purposes.

C. Attorney Best Practices in BYOD Cases

Discovering the relevant electronic data is only half the battle in an e-discovery case. Attorneys also have to be on the defensive to preserve ESI and ensure that spoliation does not occur.[87] For attorneys representing the custodians of relevant data, efficient preservation and litigation hold procedures are key.[88]

First, there are simple steps that attorneys can advise their clients to take in order to quickly preserve relevant information and avoid spoliation sanctions. These options are also efficient for smaller employers or those with limited technology budgets. For instance, employees can be encouraged to take screenshots of important text messages and email them to counsel.[89] While this option is not ideal because chain of custody issues or metadata issues may still exist, it may be appropriate in smaller cases where resources are limited.[90] Additionally, the auto-delete function of cell phones is consistently a concern in cases where text messages are at issue, and it is almost never a successful defense against alleged preservation and spoliation violations.[91] Blackberry phones, for

---

86. *Id.*

87. *Id.*

88. Coons, *supra* note 10.

89. *Id.*

90. *Id.*

91. *See In Re Pradaxa*, No. 3:12-md-02385-DRH-SCW, 2013 WL 6486921 (S.D. Ill. Dec. 9, 2013), *order rescinded on other grounds sub nom., In Re* Boehringer Ingelheim Pharm., 745 F.3d 216, 218–20 (7th Cir. 2014) (recognizing the "egregious failure" of the employer to intervene in the automated deletion of employee text

example, have a text message auto-delete function that is set, by default, for thirty days.[92]

For attorneys representing custodians of documents, however, nothing is more important than implementing an effective and timely litigation hold. Recently, in *Small v. University Medical Center of Southern Nevada*,[93] a Special Master recommended default judgment against a defendant who failed to put in place a litigation hold until after the plaintiffs had deposed a defendant witness more than 250 days after the plaintiffs initiated the action.[94] The *Small* defendant did not include devices used pursuant to its company BYOD program in the litigation hold at all, resulting in about two years of lost ESI and a plethora of sanctions.[95] The *Small* Special Master wrote that "[a] party must not only suspend routine document destruction policies and put in place a hold, but, corporate officers with notice of discovery obligations 'must communicate those obligations to employees in possession of discoverable materials.'"[96] In short, potentially relevant information stored on employee devices *must* be considered when implementing a litigation hold.

Attorneys representing parties that request electronically stored data must be proactive early in the litigation process to avoid an outcome similar to the *Cotton* or *Ewald* plaintiffs. This can be achieved by considering the use of subpoenas and specifying discovery of BYOD ESI in the parties' 26(f) report.

Subpoenas are a potential tool that the parties in *Cotton* and *Ewald* failed to use. In fact, the *Ewald* court specifically mentioned that the plaintiff missed her opportunity to subpoena the relevant custodians of the requested ESI.[97] There is obviously a timeliness issue. However, subpoenas should not be issued before a party attempts to request production of the text messages through a request for production of documents. Additionally, the requesting

---

messages and requiring a potential "show cause order" for employees who did not turn off the auto-delete function on their phones).

92. *See* Coons, *supra* note 10.

93. No. 2:13-cv-00298-APG-PAL, 2014 WL 4079507 (D. Nev. Aug. 18, 2014).

94. Doug Austin, *Failure to Preserve Data on Various Devices Causes Special Master to Recommend Default Judgment*, EDISCOVERY DAILY BLOG (Oct. 15, 2014), http://www.ediscoverydaily.com/2014/10/failure-to-preserve-data-on-various-devices-causes-special-master-to-recommend-default-judgment-edisc.html.

95. *Id.*

96. *Small*, 2014 WL 4079507, at *30 (quoting Nat'l Ass'n. of Radiation Survivors v. Turnage, 115 F.R.D. 543, 557–58 (N.D. Cal. 1987); *see* Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003)).

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

party should raise the issue early in the parties' 26(f) conference and should aim to include "text messages" on employees' phones and tablets (whether owned by the employee or employer) within the meaning of the term "document" as defined in the party's requests for production. The fact that the *Pradaxa* parties had done so was considered by the court when deciding to require the production of the employees' text messages.[98] However, when a party is uncooperative and increased motion practice is imminent, the requesting party should consider issuing a subpoena to the relevant individual employees or custodians before the discovery period ends.

For all sides, communication is key. This is especially true in light of the recent proposed amendments to the Federal Rules of Civil Procedure—projected to take effect in December of 2015—which will make communication and proportionality even more important in e-discovery.[99] These amendments will encourage "cooperation among counsel and early engagement by the judiciary in civil case management."[100] As technology advances, attorneys need to keep up with and consider relevant ESI before discovery commences, and foster open communication about the procedures for obtaining it throughout the discovery process.

IV. CHANGING E-DISCOVERY THROUGH THE BYOD MOVEMENT

In early 2014, it was predicted that BYOD would be the number one e-discovery challenge in the coming years.[101] The challenges of accessing information stored on an employee's personal devices are new to e-discovery and will provide significant obstacles for attorneys until more judicial guidance is provided. Once courts provide clearer expectations of when employers need to produce this information, motion practice will decrease and costs will go down. Controlling costs is especially important in e-discovery, an area in which litigation costs can accumulate to daunting levels when not handled properly.[102]

It is a common principle that "law follows technology."[103] While the state of the law regarding BYOD practices in e-discovery is in

---

98. *In Re Pradaxa*, No. 3:12-md-02385-DRH-SCW, 2013 WL 6486921, at *16 (S.D. Ill. Dec. 9, 2013), *order rescinded on other grounds sub nom*, *In Re* Boehringer Ingelheim Pharm., 745 F.3d 216, 218–20 (7th Cir. 2014).

99. Crowley-Hsu, *supra* note 85.

100. *Id.*

101. Hammerquist, *supra* note 11 (citing a survey of inside counsel at Fortune 1,000 companies by FTI Consulting).

102. Marino & Nguyen, *supra* note 7.

103. *Id.*

flux, increased communication and cooperation between attorneys will necessarily develop and provide change. Opposing counsel will be forced to work together in order to be clear about what is expected and how the parties should proceed when BYOD information is requested.

Additionally, having an officially documented BYOD program will almost guarantee that any requests for relevant ESI on an employee's phone must be turned over, because "[t]he more rights a company has or asserts to its employees' data, the more likely it is that company could be deemed to have an obligation to collect, review and produce data stored on employee-owned devices should litigation ensue."[104] As stated previously, officially documented BYOD programs will also provide employees with appropriate expectations for technology use at work and will provide guidance for all parties in the event that litigation arises. Overall, clarifying the expectations of ESI discovery subject to a BYOD program will streamline the litigation process and allow the legal system as whole to better adapt to future technology trends in e-discovery.

V. CONCLUSION: THE FUTURE OF BYOD

The growth of technology use in the workplace is unavoidable and imminent. It is estimated that "the number of mobile-connected devices [now] exceed[s] the number of people on Earth."[105] Many people bring their work home, and many people bring their personal devices to the office. As a society, we steadily blur the line between our work lives and personal lives.

Employers, attorneys, and courts must begin to address this technology growth in the workplace and prepare for the legal consequences. While employers can avoid an official BYOD program, they cannot avoid BYOD ESI discovery obligations. When litigation arises, employers will often be found "in control" of relevant ESI stored on their employees' personal phones. The BYOD environment further complicates litigation in the workplace and demands employers and attorneys alike to begin taking notice of this addition to the e-discovery landscape.

---

104. *Id.*

105. WU, *supra* note 3, at 1 (citing *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update*, 2012–2017, 3 (Feb. 6, 2013)).