New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 255—NO. 108
TUESDAY, JUNE 7, 2016

FEDERAL E-DISCOVERY

Personal Devices Increasingly Part of New E-Discovery Normal


By **H. Christopher Boehning** And **Daniel J. Toal**

The technical ability to work "on the go" has blurred the lines between personal and business life. Personal mobile devices and email accounts are increasingly being used for work,[1] meaning that they are more likely than ever to contain potentially relevant electronically stored information (ESI) and, therefore, to be targets for collection as part of e-discovery in litigation.

Although the dust has yet to settle regarding the legal implications of the use of personal devices and personal email for work, judges are increasingly grappling with the topic. Three recent decisions help illustrate how the integration of personal devices and email into the corporate environment, whether authorized or not, is changing discovery in the corporate litigation context.

H. CHRISTOPHER BOEHNING *and* DANIEL J. TOAL *are litigation partners at Paul, Weiss, Rifkind, Wharton & Garrison.* ROSS M. GOTLER, *e-discovery counsel, and* LIDIA M. KEKIS, *e-discovery attorney, assisted in the preparation of this article.*

'Living Color'

In *Living Color Enters. v. New Era Aquaculture*,[2] text messages from a personal phone potentially relevant to the underlying business dispute were the subject of a motion for sanctions under recently amended Federal Rule of Civil Procedure 37(e). In this case, the plaintiff Living Color and defendant "New Era entered into a business relationship in which Plaintiff became the exclusive distributor for New Era products in the United States," resulting in the plaintiff's subsequent hiring of defendant JT as a sales manager and defendant Leyden as a sales representative.[3] The plaintiff alleged that defendants New Era, JT, Leyden, and distributor Aqua-Tech devised and executed "a plot to divest Living Color of the business relationship with New Era, its relationships with JT and Leyden, and Living Color's customers and other trade secrets." Defendants New Era, JT, and Leyden terminated their relationships with the plaintiff, the defendants JT and Leyden gained employment with defendant New Era, and defendant "Aqua-Tech became the exclusive distributor for New Era's products bearing the Mark owned by Living Color," which led to the plaintiff's lawsuit.[4]

BIGSTOCK

In a prior discovery order, the court ordered defendant Leyden, who had stated he had no additional

responsive documents to produce, to immediately file an affidavit, "under oath, whether or not he possessed any text messages or emails that he had not yet produced[.]" In his affidavit, the defendant stated that he replaced his personal phone twice during the litigation and "that he did not archive or save text messages on his phones when they were replaced."[5]

In response, the plaintiff filed a motion for sanctions, alleging that the defendant "knowingly destroyed evidence" that he had an ongoing duty to preserve, thereby warranting a default judgment award as well as an adverse inference instruction.[6] The defendant admitted his "usual practice to periodically remove text message exchanges from [his] phone to maintain the operational speed and efficiency of [his] phone," his regular usage of "the cell phone feature that automatically deletes text messages after 30 days[,] and that he, admittedly, neglected to disable the feature when the lawsuit was filed."[7] While the defendant acknowledged his duty to preserve the deleted text messages, he countered that the plaintiff "cannot establish the requisite elements for spoliation because it cannot show that the missing evidence is crucial to its ability to prove its prima facie claims or that [he] acted in bad faith by neglecting to archive or save the text messages" based on the "circumstantial evidence" presented.[8]

Conducting an analysis under Rule 37(e),[9] the court determined that certain of the preconditions for sanctions under the rule had been met since defendant Leyden, due to a failure to take reasonable steps, failed to preserve electronically stored information that he was under an obligation to preserve, and the information could not be replaced.[10]

Despite that conclusion, the court declined to impose sanctions after finding that the plaintiff had failed to show "prejudice … from loss of the information[.]"[11] The court found the plaintiff's argument that the missing text messages were crucial to its claims to be "an extremely conclusory statement that really does not establish any prejudice to Plaintiff."[12] Thus, the plaintiff failed to establish "any direct nexus between the missing text messages and the allegations in its Complaint."Finding "no prejudice suffered by"the plaintiff due to the loss of information, the court could not issue sanctions under Rule 37(e)(1).[13]

> Although the dust has yet to settle regarding the legal implications of the use of personal devices and personal email for work, judges are increasingly grappling with the topic.

The court then examined whether there was intent to deprive, which would allow for granting severe sanctions under subsection 2 of Rule 37(e).[14] Determining that the defendant "simply acted negligently in erasing the text messages either actively or passively[,] the court did "not find any direct evidence of either 'intent to deprive' or bad faith."[15] As such, the court could not issue sanctions under Rule 37(e)(2) and ultimately denied the plaintiff's motion for sanctions.[16]

'Brown Jordan'

In another recent decision, spoliation of evidence on a mix of personal and business devices featured prominently in a complex case involving a claim of wrongful termination and potential violations of the Computer Fraud and Abuse Act and the Stored Communications Act. In *Brown Jordan Int'l v. Carmicle*, defendant Carmicle was "a high-ranking employee running two subsidiaries" of Brown Jordan.[17] Carmicle, whose job was in jeopardy for various reasons, had exploited the existence of a generic password in the company's new email system to access the email of company employees and his supervisor, the company CEO. Carmicle claimed he did so due to his suspicions that the CEO and other employees were lying to him and because he was looking into potential financial misconduct related to the valuation of the company in connection with a potential purchase or management buyout. He "used his personal iPad to take screenshots of hundreds of emails over" a six-month period.[18]

Carmicle eventually emailed a letter to several board members setting forth his allegations of fraudulent financial activity. That same day, Carmicle, who "primarily used a Company-owned laptop," purchased a personal laptop computer and migrated data "from the Company-owned laptop to his personal laptop."[19] He

also "wiped the company-issued iPhone and restored it to factory settings." The defendant was terminated soon thereafter, "primarily due to his accessing others' email accounts" in direct contravention of the company's "Computer and Internet Policy" found within the corporate Employee Handbook.[20] Upon termination, Carmicle "used the 'Find My iPhone' application to remotely lock [the company-owned laptop], rendering it inaccessible," but claimed to have intended only to "lock his personal laptop."[21] He additionally "remotely wiped [his] Company-owned iPad and restored it to factory settings."[22]

During discovery, Carmicle "claim[ed] to have subsequently lost the personal iPad with which he had taken screenshots of emails" and, thus, insisted that he could not produce them. He also was unable to produce "various other data and devices [he] claim[ed] to have deleted or lost despite the near certainty of impending litigation."[23] Additionally, "a forensic examination of Carmicle's personal laptop revealed that 2.4 million files—nearly all of the files on that laptop—had last been accessed within the 48 hours prior to the date on which Carmicle surrendered the laptop for forensic examination in June of 2015,"[24] thereby modifying potentially relevant metadata.

Brown Jordan moved for spoliation sanctions based on the defendant's "handling of [corporate and personal] devices, both prior to and following the termination of his employment." The court reviewed whether Carmicle's "repeated access of other employees' email accounts … using a single generic password provided to all employees in connection with the transition to a new email service amounted to gross negligence or willful misconduct."[25]

The court conducted an analysis under Rule 37(e) to decide whether sanctions were appropriate. It determined that Carmicle should have preserved ESI from many devices, including "his personal iPad, his personal laptop computer, the Company-owned laptop, the Company-owned iPad, Carmicle's personal iPhone, and Mrs. Carmicle's computer[.]"[26] Additionally, "this information was lost because Carmicle failed to take reasonable steps to preserve it" and "[t]his information—including the metadata relevant to Carmicle's accessing and taking screenshots of others' emails with his personal iPad, and the last access dates for 2.4 million files on Carmicle's personal laptop—cannot be restored or replaced through additional discovery."[27] Since it also found that "Carmicle acted with the intent to deprive the Brown Jordan Parties of the information's use in litigation," the court found severe sanctions under Rule 37(e)(2) to be appropriate and imposed the sanction that "certain adverse inferences [would be] drawn from the absence of evidence lost, deleted, or destroyed by Carmicle."[28]

> Courts, such as in 'Matthew Enterprise', are showing an appreciation for the fact that a corporation does not always have control of or ability to access the personal devices or systems of employees.

'Matthew Enterprise'

The definition of control, from a legal perspective, was a key issue in a recent case out of California, *Matthew Enterprise v. Chrysler Group*. In this matter, the court was faced with, inter alia, the question of whether an employer must produce corporate ESI from its employees' personal email accounts. The plaintiff, a car dealership, had alleged that the defendant, Chrysler, engaged in discriminatory practices by excluding it from participating in a sales incentive program with hidden price discounts offered to competing dealerships.[29]

After receiving only three email messages in a document production by the plaintiff in response to its document requests, the defendant moved to compel production of work-related communications from the personal email accounts of the plaintiff's employees used for business-related purposes.[30] Federal Rule of Civil Procedure 34(a)(1) allows a party to serve on another party a request to produce documents or ESI "in the responding party's possession, custody, or control."[31] Arguing that such ESI was not within its possession, custody, or control, the plaintiff took the position that these items were, thus, outside the permissible scope of discovery. The defendant countered, arguing that

the plaintiff "still has control over its company information," irrespective of whether such information is stored in personal email accounts.[32]

The court initiated its analysis by determining whether the plaintiff, in fact, had control over the personal email accounts that contained the work-related messages. Noting the circuit court split regarding the definition of control, the court stated that the Ninth Circuit, in line with the majority of circuits, "has explicitly rejected an invitation 'to define "control" in a manner that focuses on the party's practical ability to obtain the requested documents.'"[33] Instead, it followed the frequently relied upon definition of control from *In re Citric Acid Litig.*,[34] "the legal right to obtain documents upon demand."[35] The court elaborated that the "[d]ocuments are not discoverable under Rule 34 if the entity that holds them 'could legally—and without breaching any contract—continue to refuse to turn over such documents'" and also noted that the "party seeking production of the documents … bears the burden of proving that the opposing party had such control."[36]

Chrysler sought the employees' personal email accounts since the plaintiff "does not furnish all its employees with email accounts [and] many of them use their personal accounts for business purposes."[37] The court, though, found that Chrysler had not met its burden to show that the plaintiff had control over this ESI. Chrysler had cited to the plaintiff's employee handbook, which instructed employees "to keep 'internal information' in the 'sole possession'" of the plaintiff, but the court found that the handbook "is not a contract and so does not create a legal right for [the plaintiff] to take back any such information now stored in personal accounts."[38] The court also noted that, even if it did order production from the personal email accounts, Chrysler "had not identified any authority under which [the plaintiff] could force employees to turn them over." Since Chrysler had not met its burden here, the court denied the motion to compel production from the personal email accounts.[39]

Conclusion

The cases discussed above highlight the evolution of corporate litigation and related discovery, which is moving away from focusing exclusively on corporate-owned devices and systems. Personal devices and systems such as email accounts are increasingly becoming a standard part of the corporate environment. "Approximately 40 percent of U.S. consumers who work for large enterprises said they use their personally owned smartphone, desktop or laptop daily for some form of work purposes[.]"[40] Moreover, companies are increasingly providing incentives for or requiring employees to use their personal devices for work-related communications through bring-your-own-device (BYOD) programs, with "[h]alf of enterprises say[ing] they intend to move exclusively to BYOD for smartphones in 2017[.]"[41] With personal devices and systems increasingly becoming potential sources of discoverable ESI in corporate litigations, companies should take note by reevaluating and updating their information governance, litigation readiness, and discovery response practices accordingly to manage potential related discovery obligations.

While personal devices and systems are becoming part of the new e-discovery normal, this does not necessarily mean that courts are sweeping them in with corporate email and other systems as part of the scope of permitted discovery. In some situations, as in *Brown Jordan*, where an individual is a party, personal devices and systems may generally be considered as fair game for discovery. However, in other situations, where individual employees use personal devices and systems for work-related communications, such as in *Living Color* and *Matthew Enterprise* as well as in the high profile *Amalgamated Bank v. Yahoo!*[42] dispute, much more judicial analysis is required.

In addition to the critical threshold issues of discovery scope in Federal Rule of Civil Procedure 26(b)(1) of whether the information is relevant to a claim or defense and proportional to the needs of the case,[43] such ESI on personal devices and systems also necessarily invites a "possession, custody, or control" analysis under Federal Rule of Civil Procedure 34. Courts, such as in *Matthew Enterprise*, are showing an appreciation for the fact that a corporation does not always have control

of or ability to access the personal devices or systems of employees.[44] This is especially true in situations where there is no clear agreement between a company and its employees regarding control or ownership of such ESI. As a result, the issue of control will necessarily be a crucial aspect of sanctions analyses under Federal Rule of Civil Procedure 37(e), as a party cannot be expected to have had an obligation to preserve ESI over which it had no legal control.

1. A recent survey revealed that "67 percent of people are using personal devices in the workplace whether [it is] officially sanctioned by the organization or not." Jeff Jones, "BYOD—is it Good, Bad or Ugly from the User Viewpoint?," July 26, 2012, available at https://blogs.technet.microsoft.com/security/2012/07/26/byodis-it-good-bad-or-ugly-from-the-user-viewpoint/.

2. *Living Color Enters. v. New Era Aquaculture*, 2016 WL 1105297 (S.D. Fla. March 22, 2016).

3. *Living Color Enters. v. New Era Aquaculture*, 2015 WL 1526177 at *1-2 (S.D. Fla. 2015).

4. Id. at *2.

5. *Living Color*, 2016 WL 1105297 at *1.

6. See id. at *2. The plaintiff alleged that its former employee used his personal phone and email account during and after employment to communicate and conspire against it and that the destroyed "evidence would have established he was involved in the scheme to misappropriate Plaintiffs business and customers." Id. at *5.

7. Id. at *1-2.

8. Id. at *2.

9. Federal Rule of Civil Procedure 37(e) reads, in full:

> Failure to Preserve Electronically Stored Information. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:
>
> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> (A) presume that the lost information was unfavorable to the party;
>
> (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
>
> (C) dismiss the action or enter a default judgment.

10. See *Living Color*, 2016 WL 1105297 at *4-5.

11. FED. R. CIV. P. 37.

12. *Living Color*, 2016 WL 1105297 at *5.

13. See id. at *5-6.

14. See id. at *6.

15. Id. The court added, "it is common practice amongst many cell phone users to delete text messages as they are received or soon thereafter. There is nothing nefarious about such a routine practice under the facts presented here." Id.

16. See id. at *6-7.

17. *Brown Jordan Int'l v. Carmicle*, 2016 WL 815827 at *1 (S.D. Fla. March 2, 2016). Since the cases have been consolidated and the defendant here was also a plaintiff in a related matter, see *Brown Jordan Int'l v. Carmicle*, 2015 WL 6142885 at *1 (W.D. Ky. Oct. 19, 2015), for simplicity, we will refer to the parties as "Brown Jordan" and "Carmicle."

18. *Brown Jordan Int'l*, 2016 WL 815827 at *1, *3.

19. Id. at *27, *28.

20. Id. at *4, *9, *28.

21. Id. at *4. The court later found that the defendant "knew he was locking the Company-owned laptop rather than his personal laptop." Id. at *33.

22. Id. at *33.

23. Id. at *4.

24. Id. at *33.

25. Id. at *1, *6.

26. Id. at *37. Of note is that the W.D. Kentucky district court had previously granted the plaintiffs' motion to compel the production of ESI from the defendant's wife's cellular phone after a forensic report indicated that the phone may contain discoverable information. See *Brown Jordan Int'l*, 2015 WL 6142885 at *4.

27. *Brown Jordan Int'l*, 2016 WL 815827 at *37.

28. Id. at *34, *37. "Although the Court concludes that drawing certain adverse inferences is an appropriate sanction for Carmicle's egregious conduct, such inferences ultimately have no effect on the outcome of this case. The Court would reach the same conclusions of law whether or not it imposed this particular sanction." Id. at fn. 38. Moreover, the court concluded that it could still find sanctions warranted under the previous Rule 37(e) standard as well as under its inherent authority to issue sanctions. See id. at 37.

29. *Matthew Enter. v. Chrysler Grp.*, 2015 WL 8482256, at *1 (N.D. Cal. Dec. 10, 2015).

30. See id. at *3.

31. FED. R. CIV.P. 34.

32. *Matthew*, 2015 WL 8482256 at *3.

33. Id. (quoting *In re Citric Acid Litig.*, 191 F.3d 1090, 1107-08 (9th Cir. 1999)). For comparison, several circuits, including the Second Circuit, define control based on the "somewhat more flexible," *Dietrich v. Bauer*, 198 F.R.D. 397, 397 (S.D.N.Y. 2001), and "more pragmatic approach focusing on practical ability to obtain documents." Id. at 401. Specifically, "'control' does not require that the party have legal ownership or actual physical possession of the documents at issue; rather, documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the documents …" *In re NTL, Inc. Sec. Litig.*, 244 F.R.D. 179, 195 (S.D.N.Y. 2007) (quoting *Bank of N.Y. v. Meridien BIAO Bank Tanzania*, 171 F.R.D. 135, 146-47 (S.D.N.Y. 1997)).

34. *In re Citric Acid Litig.*, 191 F.3d 1090 (9th Cir. 1999).

35. *Matthew*, 2015 WL 8482256 at *3 & fn. 36 (citing *In re Citric Acid Litig.*, 191 F.3d at 1107 (quoting *U.S. v. Int'l Union of Petroleum & Indus. Workers*, 870 F.2d 1450, 1452 (9th Cir. 1989))). For an in-depth discussion of possession, custody, and control in e-discovery, including a comparison of how the issue is treated in various circuits, see The Sedona Conference, "The Sedona Conference Commentary on Rule 34 and Rule 45 'Possession, Custody, or Control,'" 2015 Public Comment Version.

36. *Matthew*, 2015 WL 8482256 at *3, fn. 38 (quoting *In re Citric Acid Litig.*, 191 F.3d at 1107-08), and fn. 39 (quoting *Int'l Union of Petroleum & Indus. Workers,* 870 F.2d at 1452).

37. Id. at *3.

38. Id. at *4.

39. See id. Although not pursued in this matter, the sought after information may have been obtainable through a non-party subpoena issued directly to the individual employees under Federal Rule of Civil Procedure 45. Also of note, the court subsequently issued sanctions under Federal Rule of Civil Procedure 37(e)(1) against the plaintiff for spoliation of corporate ESI. See *Matthew Enter. v. Chrysler Grp.*, 2016 WL 2957133 (N.D. Cal. May 23, 2016).

40. Gartner, "Gartner Says 40 Percent of U.S. Employees of Large Enterprises Use Personally Owned Devices for Work," Oct. 21, 2014, available at http://www.gartner.com/newsroom/id/2881217.

41. Gartner, "Bring Your Own Device: The Results and the Future," May 5, 2014, available at https://www.gartner.com/doc/2730217/bring-device-results-future.

42. *Amalgamated Bank v. Yahoo!*, 2016 WL 707308 at *1 (Del. Ch. Feb. 19, 2016) (court ordered the defendant to produce "[a]ll document, including electronic documents, memos, notes and emails (whether located in personal or Company email accounts)[.]"), motion to stay granted, 2016 WL 2342815 (Del. April 14, 2016).

43. See FED. R. CIV. P. 26.

44. As noted in *Matthew Enterprise*, a majority of circuits follow the legal right standard for control, which focuses on the party's legal right to obtain the documents on demand. See *Matthew*, 2015 WL 8482256 at *3.