Bloomberg BNA

Digital Discovery & e-Evidence®

BNA INSIGHT

Litigation, Legal Holds and 'Bring Your Own Device'

JENNIFER H. REARDEN AND GOUTAM U. JOIS

Introduction

The past few years have witnessed a dramatic increase in the number of companies permitting (and in some cases, even encouraging) employees' use of personal devices for work purposes. This practice—often referred to as ''Bring Your Own Device,'' or BYOD—potentially benefits employers and employees alike. BYOD, however, also poses both practical and legal challenges.

Jennifer H. Rearden is a litigation partner in the New York office of Gibson, Dunn & Crutcher and co-chair of the firm's Electronic Discovery and Information Law Practice group. She represents clients in complex business litigation matters and also frequently counsels clients regarding effective crisis management planning and response. Jennifer can be reached at jrearden@gibsondunn.com

Goutam U. Jois is a litigation associate Gibson, Dunn & Crutcher, also based in New York. In addition to a practice focused on general commercial litigation, he is a member of The Sedona Conference® Working Group 1 on electronic discovery. Goutam can be reached at GJois@gibsondunn.com.

A threshold question in discovery is whether a litigant has ''possession, custody, or control'' of the information sought.[1] The cases suggest that, ultimately, whether a company will be deemed to have ''possession, custody, or control'' of an employee's personal device or data is a fact-specific inquiry. Certain decisions also imply that companies' control (or lack thereof) over employees' personal devices cannot be used as both a sword and a shield.

Potential Benefits

BYOD can benefit companies in various ways. For example, corporate IT departments face lower long-term support costs if employees bear at least some of the responsibility for purchasing and maintaining their devices. Employees may also feel a greater sense of ownership and be more productive and engaged when they can work on their personal devices, rather than having to carry separate work and personal devices.

Potential Challenges

Federal Rule of Civil Procedure 34 refers to documents ''in the responding party's possession, custody, or control.''[2] If an employee sends work-related e-mails from a personal e-mail account on a personal device, those e-mails—or, for that matter, the device itself—may be deemed to be under the company's ''possession, custody, or control.'' But in that circumstance, what if the employee refuses to turn over her phone to her employer? Internal BYOD policies can address some of these issues, but they have been relatively untested in the courts, leaving many questions unresolved.

Practical considerations seem to abound as well. For example, even if a company might legitimately assert control over its employees' devices or data, the risk of demoralizing employees (who may resent an employer

[1] Fed. R. Civ. P. 34(a)(1).
[2] Fed. R. Civ. P. 34(a)(1).

 ISSN 1941-3882

who copies data from their cell phones) may deter the company from implementing such a practice. Moreover, a company that frequently finds itself in litigation may hesitate to declare in a policy that it ''owns'' data on employees' personal devices, lest it draw an argument that the company should be required to produce that data.

Some of companies' most significant concerns, of course, relate to security: companies need to protect their trade secrets, financial data and other sensitive information. Various device manufacturers make increased security available on their devices for enterprise use.

But unless a company is willing to invest in security software and mandate its use by employees, the levels of security on employees' devices will differ. And some devices may be less capable of implementing the full range of security that a company may want.

Although security issues have not come up squarely in any case, they may add another layer of complexity to whether companies can ''control'' the data on their employees' devices. For example, an employee may put a password on her device, effectively preventing any third party, including her employer, from accessing it.

Conversely, a company may demand that employees install certain security software that provides the company with the ability to access (and/or delete) data on a device, regardless of the employee's own settings.

Case Law: Use of Personal Devices

The case law relating to BYOD is relatively thin. In recent months, however, two cases have addressed the discoverability of text messages on personal devices. One permitted the discovery of such data, and the other did not.

The cases are distinguishable—in one, at least some of the cell phones at issue were company-issued and were used for work purposes, and in the other, there was no showing to that effect. Going forward, the analysis may turn on these factors.

In *In re Pradaxa*,[3] the court held that a litigation hold should extend to personal devices (at least some of which were company-issued), in order to preserve any text messages that might be relevant to the lawsuit.

Plaintiffs had requested text messages that were sent by the defendant pharmaceutical company's employees. As characterized in the opinion, the company acknowledged ''that some [of its] employees use[d] their personal cell phones while on business and utilize[d] the texting feature of those phones for business purposes,'' notwithstanding the company's policy against doing so, ''yet balk[ed] at the request of litigation lawyers to examine these personal phones.''[4] Under these circumstances, the court held, ''[t]he litigation hold and the requirement to produce relevant text messages without question applies'' to employees' personal devices.[5] The court also concluded that, if defendants believed they were not required to produce text messages, then ''they should have responded with a specific objection to the request or otherwise sought relief from the Court.''[6]

Just a few months earlier, in *Cotton v. Costco Wholesale Corporation*, the District of Kansas held that a company did not have ''possession, custody, or control'' over text messages sent by its employees.[7] In that employment discrimination case, Plaintiff sought text messages from other employees that referred to him or his allegations. The court denied Plaintiff's motion to compel production of the text messages, reasoning that, because the defendant company did not have the legal right to obtain on demand any text messages on employees' personal cell phones, those messages were not within the ''possession, custody, or control'' of Defendant. The court also noted that Plaintiff ''does not contend that [Defendant] issued the cell phones to these employees, that the employees used the cell phones for any work-related purpose, or that [Defendant] . . . otherwise has any legal right to obtain employee text messages on demand.''[8] It is unclear whether the outcome would have been different had Plaintiff shown that other employees were indeed communicating about him and his allegations via text message.

The decisions in *Pradaxa* and *Cotton* appear to follow a trend. With regard to personal *computers*, courts have been willing to order data collection from personal devices when a showing has been made that the device was used for work purposes. For example, in *Genworth Financial Wealth Management v. McMullan*,[9] a trade secrets case by a company against its former employees, the court required defendants to subject their personal computers to forensic imaging. This ruling was based in part on evidence that at least one of the defendants had ''used his personal computer and personal e-mail address to download, access, and transmit the Plaintiff's proprietary information without a scintilla of a reasonable expectation to his entitlement thereto or other legitimate justification therefore.''[10] That the defendant ''admitted spoliation of incriminating evidence'' also factored into the decision.[11]

Both *Genworth Financial* and *Pradaxa* suggest that discovery of personal devices will be allowed (or, at least, that courts will conclude that the data on personal devices should have been subjected to a legal hold) where the requesting party can make some showing that potentially relevant data is located on the device, regardless of whether that device is a personal computer or a personal cell phone containing text messages.

The decision in *Cotton* is consistent: in that case, Plaintiff did not contend ''that the employees used the cell phones for any work-related purpose,'' and the court denied discovery of personal text messages.[12]

---

[3] *In re Pradaxa (Dabigatran Etexilate) Products Liability Litigation*, 2013 BL 347278 (S.D. Ill. Dec. 9, 2013), *rescinded on other grounds sub nom. In re Petition of Boehringer Ingelheim Pharm., Inc., & Boehringer Ingelheim Int'l GmbH, in Pradaxa (Dabigatran Etexilate) Products Liab. Litig.*, 13-3898, 2014 BL 19818 (7th Cir. Jan. 24, 2014).

[4] *Id.* at *42.

[5] *Id.*

[6] *Id.*

[7] *See Cotton v. Costco Wholesale Corp.*, Case No. 12-2731-JWL., 2013 BL 198309 (D. Kan. July 24, 2013); *see also Cotton v. Costco Wholesale Corp.*, Case No. 12-2731-JWL., 2013 BL 196548 (D. Kan. July 24, 2013).

[8] *Id.* at *6.

[9] 267 F.R.D. 443 (D. Conn. 2010),

[10] *Id.* at 447.

[11] *Id.* at 448.

[12] *Cotton*, 2013 BL 196548, at *6.

  DDEE ISSN 1941-3882

One also can reasonably infer from these cases that a litigant cannot use the ''possession, custody, or control'' standard as both a sword and a shield. A company with a BYOD policy that (i) provides that the company controls all data on an employee's personal device, (ii) requires employees to synchronize certain data with the company's servers, and (iii) requires installation of an application that permits the company to remotely ''wipe'' the device if it were lost, for example, might find it challenging to argue, in response to a motion to compel, that it did not ''control'' the data in question. This may suggest that companies should exercise caution in broadly asserting control over employee data, absent an effective means of exercising that control.

Conclusions

While there is not yet perfect clarity in judicial decisions regarding the discoverability of information on personal devices, some trends are emerging. First, courts are probably unlikely to order discovery of information on personal devices absent any showing that the personal devices were used for work purposes (or were in some other way relevant to the litigation).

Second, actual or perceived spoliation may make a court more likely to order broader preservation or production of electronic data.[13] Additionally, as in other contexts, litigants likely will not be able to use these concepts as both a sword and a shield—by arguing, for example, that it owns the work data on employees' personal devices but lacks ''possession, custody, or control'' over that data for the purposes of discovery.

Just as courts have begun to confront certain issues related to BYOD, other novel questions have started to arise. For example, some device manufacturers allow a user to run two different interfaces on the same device. How much, if any, discovery should be permitted on the ''personal side'' of such a device?

The principles addressed in this article may be relevant to resolving these and related questions. Although predicting the future is tricky business, it seems safe to say that issues like those surrounding BYOD will be with us for some time to come.

---

[13] *See, e.g., Landmark Legal Found. v. EPA*, Civil No. 12-1726., 2013 BL 212242 (D.D.C. Aug. 14, 2013); *Food Servs. of Am., Inc. v. Carrington*, No. CV-12-00175-PHX-GMS, 2013 BL 225510, (D. Ariz. Aug. 23, 2013).