E-Discovery and Bring Your Own Device to Work: The New Norm

Beth S. Rose, Esq.
Sills Cummis & Gross P.C.
One Riverfront Plaza
Newark, NJ 07102
Tel: (973) 643-5877
Fax: (973) 643-6500
brose@sillscummis.com

Beth S. Rose is a partner at Sills Cummis & Gross P.C. in Newark, New Jersey where she chairs the Firm's Product Liability Practice Group. She has served as national counsel to several pharmaceutical and medical device companies defending mass tort litigation including claims relating to pelvic mesh products, a generic form of Accutane, PPA, and latex gloves. She has also served as lead/liaison counsel for a contract research organization, foreign defendants and discovery counsel in a multi-district litigation as well. Ms. Rose has trial experience in product liability cases and has secured defense verdicts on behalf of her clients. Ms. Rose was recently named by NJ BIZ to its list of Best 50 Women in Business for 2015. She was named in the 2015 edition of Benchmark's Top 250 Women in Litigation: The Definitive Guide to the Leading Female Attorneys in the US and the 2014 Guide to the World's Leading Women in Business Law (3rd Edition) under Product Liability. Since 2008, she has been recognized in the Chambers USA® Guide to America's Leading Lawyers for Business. Ms. Rose received her B.A. with honors from Wesleyan University and her J.D. from Georgetown University Law Center.

The author appreciates the research assistance of summer associate, Lauren Valli, in the preparation of this article.

The views and opinions expressed in this article are those of the author and do not necessarily reflect those of the Firm or its clients.

Introduction

Let's face it. We have all become e-addicts. Whether we want to admit it or not, we are physically (and emotionally) attached to our electronic mobile devices. We bring personal smart phones, tablets and laptops with us everywhere. We feel naked without them. In the not so distant past, we stowed these devices away in our desks once we arrived at work. But as technology has evolved, we now use them *for* work. Employee use of personal devices for business purposes – often referred to as "Bring Your Own Device" or "BYOD" has become the new norm.

Employees and employers alike welcome BYOD programs. Employees are increasingly managing their lives through personal devices which are often newer and more user friendly than company issued devices. Employees don't want to carry multiple devices – they would rather use just one. And they can use them 24/7. In this respect, BYOD has the potential to increase employee satisfaction and productivity. Employers incur fewer IT costs when employees pay for their personal devices. So everyone's happy, right? Not so fast.

BYOD presents its own unique set of issues when it comes to e-discovery. Because BYOD blurs the line between employer and employee property, it further complicates the challenges related to preservation, discovery and collection of electronically stored information ("ESI") on personal devices, especially text messages. This article explores how BYOD has the potential to impact defense e-discovery obligations in mass tort litigation.

Preservation

Most courts analyzing the issue have found that data on BYOD is subject to the same preservation obligations as other ESI. In *In re Pradaxa (Dabigatran Etexilate) Products Liability Litigation*, MDL No. 2385, Civil No. 3:12-md-02385(DRH/SCW), 2013 U.S. Dist. LEXIS 173674 (S.D. Ill. Dec. 9, 2013), *order rescinded on other grounds sub nom., In re Boehringer Ingelheim Pharm.*, 745 F.3d 216 (7th Cir. Ill. 2014) ("In re Pradaxa") (litigation hold should cover ESI stored on personal devices); *Ewald v. Royal Norwegian Embassy*, Civil No. 11-CV-2116 (SNR/SER), 2013 U.S. Dist. LEXIS 164828 (D. Minn. Nov. 20, 2013) ("Ewald") (rejecting argument that a party was not aware of its obligations to preserve texts); *But cf. Easley v. U.S. Home Corp.*, Civil No. 2:11-CV-00357 (MMD/CWH), 2013 U.S. Dist. LEXIS 36972, at *5-7 (D. Nev. Mar. 18, 2013) (affirming party's refusal to produce text messages due to lack of reasonable accessibility, undue burden and cost to produce the information).

But here's the rub that most courts do not acknowledge generally, let alone address with any specificity. The defendant manufacturer (employer) - which is typically the party with the most ESI in a complex product liability lawsuit - does not physically own or control the device. BYOD data – or at least some of it – does not reside on a network server. Much of the data is decentralized

and is not easily preserved. Take text and voicemail messages for example. Or documents and photographs stored on an iPad outside of the corporate network environment. While smartphones and tablets have large storage space these days, they are not infinite. Users typically receive a warning or other notification that they are running low on storage space and need to delete or move items to free it up. These warnings are not specific to a particular form of ESI. There is no recognized standard for how users subject to a litigation hold address such warnings. Thus, the user may be left on his/her own to "free up" storage space in a manner that preserves old and new ESI alike. This is no easy task in the simplest of cases let alone mass tort litigation which often continues for several years.

Preservation issues also arise when an employee returns his/her BYOD for an upgrade or leaves the company without turning over relevant texts. An employee's good faith effort to address technical problems on a BYOD device through a hard reset or device wipe can have implications as well.

When litigation has commenced or is reasonably anticipated, prudence dictates that employers notify employees with BYOD that they need to: (1) adjust/disable the default settings (if any) on their mobile devices so that potentially responsive text messages can be preserved and are not automatically deleted; and (2) be alert for warnings regarding limitations in storage space. IT support should be offered as well. In mass tort litigation with multiple custodians in different locations, this can be a logistical nightmare. Employee cooperation is essential to any successful effort to preserve ESI on a BYOD. While there is no one size fits all solution to BYOD preservation, there are some general principles which are emerging, including requiring employees to allow employer access to personal devices and saving work files on a BYOD to an official employer repository. For a helpful list of preservation related pointers, *see* Carolyn Casey, *Avoiding BYOD Preservation Problems,* Law Technology News (June 17, 2015), http://www.legaltechnews.com/id=1202729630582/Avoiding-BYOD-Preservation-Problems-?slreturn=20150627154832.

Discovery of ESI on BYOD

Not surprisingly, the case law is not well developed on this topic. Courts that have considered discovery disputes surrounding personal devices have generally focused on one of two issues: (1) whether the employer is in possession, custody or control of the personal mobile device; or (2) a custodian's expectation of privacy in the ESI on his/her device. More recently, however, some courts have not addressed either of these issues and have simply held that relevant ESI on personal devices is fair game for discovery if the personal device is used for work.

Possession, custody and control

The question of whether discovery obligations attach sometimes turns on whether the ESI on the BYOD device in question is within the "possession,

custody or control" of the employer. *Fed. R. Civ. P.* 34. These are fact specific inquiries which typically have nothing to do with the merits of the case.

For example, in a race discrimination case, *Cotton v. Costco Wholesale Corp.*, Civil No. 12-2731 (JWL), 2013 U.S. Dist. LEXIS 103369 (D. Kan. July 24, 2013), the court considered plaintiff's request for production of text messages of other employees. Virtually all of its analysis focused on whether the defendant had possession, custody or control of the mobile devices containing the requested texts, and therefore the legal right to obtain them on demand. In denying the motion, the court stated: "Cotton does not contend that Costco issued the cell phones to these employees, that the employees used the cell phones for any work-related purposes, or that Costco otherwise has any legal right to obtain employee text messages on demand." *Id.* at 17. What is left unsaid is whether the court would have allowed discovery of texts on personal devices if there had been a showing that the devices contained work related information. *See Han v. Futerewei Techs., Inc.*, Civil No. 11-CV-831 (JMA), 2011 U.S. Dist. LEXIS 104538 (S.D. Cal. Sept. 15, 2011) ("Han") (court denies request for search of personal computer absent showing that it was used for business purposes and contained information relevant to the parties' claims and defenses).

<u>*Reasonable expectation of privacy*</u>

Other courts focus on whether a party has a reasonable expectation of privacy in ESI residing on a personal device. In *Mintz v. Mark Bartelstein & Assoc.*, 885 F. Supp. 2d 987 (C.D. Cal. 2012), plaintiff moved to quash a subpoena to AT&T for information on his mobile phone. Plaintiff asserted a right to privacy in the ESI on what he claimed to be his personal device. Defendant claimed that no such right to privacy existed. The court's analysis centered on whether plaintiff had a privacy interest in his cell phone and considered the following: the fact that the cell phone in question was plaintiff's personal cell number before he began working for defendant employer; that plaintiff used his personal cell phone to make business calls and the employer knew that; that the employer paid for plaintiff's cell bill; at some point in time, plaintiff's personal cell phone account was transferred to the employer's cell phone account; and plaintiff purchased a blackberry which was funded partially by his employer. The court found that while plaintiff had a limited expectation of privacy, the limited discovery (disclosure of telephone numbers, cell site information as well as the date, time and duration of the calls) did not represent a significant intrusion in that privacy interest because the court could issue an appropriate protective order. *See also Han*, 2011 U.S. Dist. LEXIS 104538, at *6, *9 (defendant's proposal to examine plaintiff's personal computer which would give them access to correspondence with friends, family, on-line banking information and other private data and passwords would result in the needless access of plaintiff's personal/private information; that the defendant suspects that plaintiff stole confidential and proprietary information does not give them the "unfettered right to see whatever they wish" from plaintiff); *Special Mkts. Ins. Consultants, Inc. v. Lynch*, Civil No. 11-C-9181, 2012 U.S. Dist. LEXIS 61088 (N.D. Ill. May 2,

2012) (fact that employer provided the communication technology may not eliminate any privacy interest the employee may have in the content of their text messages, as the Supreme Court has observed").

Interestingly, it appears that no court has addressed how the European Data Protection Laws impact an order from a U.S. Court that employees of foreign companies turn over their BYOD in litigation. In Europe and elsewhere, data protection legislation protects employee personal data from unfettered search by the employer. Rather, the employee must give "fully informed and unambiguous consent" for the employer to access and process his/her electronic data (be it business or personal). Richard Absalom, *Informational Data Privacy Legislation Review: A Guide for BYOD Policies Ovum*, 2, (May 17, 2012), http://www.presidio.com/sites/default/files/wysiwyg/PDFs/Data%20Privacy%20Legislation%20Review%20MobileIron.pdf. Such consent is typically in writing and can be revoked at any time. How courts will address a scenario where a foreign employee refuses to make his/her BYOD available for search in litigation remains to be seen.

Relevance as the threshold and determining principle

Still other recent cases dispense with a "control" or "privacy" analysis altogether. For them, the sole issue appears to be relevance. If the court deems the requested information on a personal device to be relevant, it matters not if the party is in possession, custody or control of it or if a privacy right is asserted.

For example, in *In re Pradaxa*, the court was dismissive of defendant's "very real privacy concerns raised when an employer demands access to an employee's private cell phone and text messages." *See* November 26, 2013 Defendants' Response to Plaintiffs' Second Motion for Sanctions at 15 -16, filed Nov. 26, 2013. Instead, the court asserted its authority to hold in contempt any employee who refused to turn over his/her personal mobile device to counsel:

> The defendants raised the issue that some employees use their personal cell phones on business and utilize the texting feature of those phones for business purposes yet balk at the request of litigation lawyers to examine these personal phones. The litigation hold and the requirement to produce relevant text messages, without question, applies to that space on employee's cell phones dedicated to the business which is relevant to this litigation. Any employee who refuses to allow the auto delete feature for text messages turned off or to turn over his or her phone for the examination of the relevant space on that phone will be subject to a show cause order of this Court to appear personally in order to demonstrate why he or she should not be held in contempt of Court, subject to any remedy available to the Court for such contempt.

In re Pradaxa, 2013 U.S. Dist. LEXIS 173674, at *42-43. No definition of "relevant space" is provided. Of course, personal and business texts reside in the same space on a smartphone.

Similarly, in *Ewald*, plaintiff sought discovery of text messages and voicemails from both company issued and personal mobile devices to support claims of employment discrimination. Defendant objected on several grounds, arguing that "the Embassy cannot force its employees or former employees to produce personal devices for analysis." 2013 U.S. Dist. LEXIS 164828, at *30. The court's analysis focused solely on relevance, finding that plaintiff had established a sufficient basis for discovery of text and voice messages on certain company issued devices. The court did not permit discovery of texts from personal devices only because plaintiff did not adequately demonstrate that relevant information existed on them. For other cases requiring preservation and production of BYOD devices which did not consider possession custody or control or privacy issues, *see Small v. Univ. Med. Ctr. of S. Nev.*, Civil No. 2:13-cv-00298-APG-PAL, 2014 U.S. Dist. LEXIS 114406, at *19-20, *54-55 (D. Nev. Aug. 18, 2014) (Special Master finds defendant's failure to preserve personal mobile devices used to conduct business to be sanctionable conduct); *Southeastern Mechanical Services v. Brody*, 657 F. Supp. 2d at 1293, 1301-02(M.D. Fla. 2009) (defendants "wiping" of data on personal blackberry may have resulted in loss of more than three weeks of relevant data and is cited as basis to impose sanctions).

As BYOD programs proliferate, defendant employers should expect possession, custody and control and privacy arguments to fall by the wayside. The threshold and determining factors will likely be whether: (1) the employee used a personal device for business purposes; and (2) there has been a *prima facie* showing that the personal device contains relevant business information.

Collection from BYOD

Challenges associated with collection of ESI from BYOD abound. Email is often synched with the network server and can be collected in a centralized fashion. But text and voice messages, documents and photographs saved outside the network on BYOD are typically not synched, presenting practical and technical issues in their collection.

For starters, most employees balk at being separated from their BYOD devices for hours let alone days. As a result, employers must retain vendors to travel to the employee and collect ESI from the BYOD. For large corporations with numerous custodians throughout the U.S. and abroad, this no easy task. And it is not cheap either.

Not surprisingly, most employees do not want their respective employers to have access to or collect private ESI. Segregating personal from business data is time consuming. For example, taking screen shots of business texts and/or

printing them out are options but less than ideal. There are several technical solutions available, each with pros and cons that need to be evaluated based on the facts and circumstances of the case. For a thorough discussion and explanation of technical approaches, *see* Michael Arnold and Dennis R. Kiker, *The Big Data Collection Problem of Little Mobile Devices,* 21 Rich. J.L. & Tech. 10 (2015).

Conclusion

BYOD programs are here to stay. The mingling of business and personal information on mobile devices is forcing litigants and court alike to consider the appropriate balance between discovery obligations and protection of personal information. Formal BYOD policies allow employers to proactively address preservation, discovery in litigation, and collection of BOYD. Of course, such policies also undercut objections to producing BYOD information based on possession, custody or control and privacy. Guiding principles will most likely emerge as the case law develops.