DEFENSIBLE ESI PRESERVATION AND COLLECTION AND ETHICS FOR IN-HOUSE AND OUTSIDE COUNSEL

BRENT COSSROW (PHILADELPHIA)
CHAIR OF E-DISCOVERY COMMITTEE

USAMA KAHF (IRVINE)
VICE CHAIR OF E-DISCOVERY COMMITTEE
FISHER PHILLIPS LLP

I. Introduction

The preservation and collection of electronically stored information (ESI) is at or near the top of the list of dreaded topics for in-house and outside counsel, and for good reason. A misstep in preservation can suddenly cast doubt on a winning case and make a difficult case a nightmare. As computers, smart phones, email, group chat, instant messaging, and text messages play a larger role in the American workplace, and the technology driving these devices and applications changes, the task of preservation and collection becomes increasingly complicated. In the past decade, we have seen two amendments to the Federal Rules of Civil Procedure meant to maintain a level playing field in litigation, and it seems like every week there is a new case involving spoliation of ESI. To top it all off, the costs of gathering ESI in a forensically sound manner has exploded, even in relatively small cases.

Against this backdrop, employment law cases have become a frontline in the battle over the proper preservation of ESI. One of the thorniest issues is something nearly every in-house counsel has faced: an employee has relevant ESI – emails, text messages, chats or some other electronic communication in a cutting-edge app – residing on a smart phone that does not belong to and was not paid for by the employer. Whether this ESI is incriminating or exculpatory, the employer invariably finds itself asking what is its obligation to preserve this ESI, particularly if the employee has not received a demand or preservation letter and has not been named as a defendant in a Complaint or Charge. It is legal or ethical to demand that the employee turn over his or her cell phone? What if it is the President, CEO or c-suite executive of the company? Or a mid-level manager?

These situations are the subject of today's discussion, which will focus on the ethical issues and the emerging case law regarding these questions. We will focus on two paradigm cases, which were inspired by actual cases handled by Fisher Phillips attorneys.

II. Two Paradigm Cases

A. Preservation In The #MeToo era

The #MeToo era has presented myriad challenges for in-house and outside counsel, some of which were discussed in Thursday morning's session. But with the heightened awareness of sexual harassment issues in the workplace and the procedures, policies and practices to prevent harassment comes a corresponding responsibility to preserve relevant evidence generated by these new approaches when claims arise.

One of the hallmarks of the #MeToo era has been the abuse of power and authority by "repeat" sexual harassers, and this has been particularly true of the higher profile cases reported on in the media. But these cases present special challenges when it comes to complying with the duty to preserve relevant ESI. Consider the following hypothetical:

Employer "X" receives a demand letter alleging that one of the company's most important and current employees, Employee "A", sexually harassed his direct report, Employee "B", and forced her to engage in a sexual relationship against her wishes before she resigned her employment shortly after the alleged harassment. The letter is not addressed to or copied to Employee A. The letter alleges that there is physical and electronic evidence that would support the claims and that there were other victims – fellow employees – of this harasser. The electronic evidence consisted of SMS text messages exchanged between Employees A and B, a few of which were presented as enclosures to the demand letter. But Employee B's attorney notes that there

are more incriminating text messages, though the copies of these messages were not recoverable by Employee B and she was unable to retrieve copies from her cellular service provider.

The preliminary investigation of the underlying facts confirms that Employee A and B worked together and that B reported to A. Also, the Office Manager where A and B worked confirmed that there might have been a social or amorous relationship between A and B, and that A considered himself a "ladies' man" who flirted with female colleagues in and outside of the office. But there were no complaints or expressions of concern lodged regarding the conduct of A. Importantly, Employer X did not issue A or B a workplace smart or cell phone and the cell phone number used on the text messages shared by B's attorney was known to be her personal cell phone number. This suggests that these text messages were exchanged on the personal – meaning not Employer-issued or Employer-paid for – cell phones of A and B, squarely raising the question of what Employer X should do about these text messages from a preservation perspective.

Central to determining the nature and scope of Employer X's preservation obligation is that there is an objectively verified showing that text messages relevant to the claim were exchanged through a personal cell phone used by a current employee. This also raises the question of whether Employee A and B also communicated via email or other means on their personal electronic devices and media, and whether such communications would have to be preserved by Employer X.

In-house counsel has framed the question bluntly: do we just go to Employee A and tell him to hand over his cell phone, which we as his employer have neither paid for nor reimbursed him for its use? Can we even do this? What if the phone is locked? Can we ask Employee A for the password? What if he refuses to provide the password? Can we just tell opposing counsel to

send a preservation letter to Employee A because it's not our cell phone and not our carrier? What if there are text messages that undermine the claims: some people believe there was a consensual relationship between the two.

Just when in-house and outside counsel thought they had their arms around the questions surrounding the preservation obligations, Employer X received another demand letter from an attorney representing Employee "C". According to this letter, Employee A sexually harassed Employee C, who also recently resigned her employment. To no one's surprise, attachments to Employee C's demand letter were several text messages exchanged between Employees A and C. Interestingly, in some of the text messages A and C discuss the claim filed by Employee B, raising several additional issues regarding the proper scope of the preservation and litigation hold in what is shaping up to be a troubling harassment case in the #MeToo era.

B. Preservation In The Employee Defection And Trade Secrets Cases

Some of the trickiest ESI preservation issues arise in employee defection and trade secrets cases. These cases frequently involve restrictive covenants – non-competition, non-solicitation, confidentiality/non-disclosure and non-recruitment clauses – and the movement of employees from one employer to another. These cases often involve not only contractual restrictions but also claims arising under the federal Defend Trade Secrets Act and Computer Fraud and Abuse Act and the state Uniform Trade Secrets Act. As employees move to their new employer, at times they retain or take with them confidential information, trade secrets, customer lists and other proprietary ESI, and sometimes they take this information by accessing the former employer's computers and email systems without authorization.

The preservation duty and litigation hold can be especially challenging for a company hiring new employees, as those of you know who have defended such cases or been on the receiving end of cease-and-desist demand letters. Let's take the following hypothetical:

Company Y recruits and hires Employee A from Company Z. Employee A is a software engineer, who wrote the code for Company Z's virtual reality software, which brick-and-mortar retail companies use to determine the optimal configuration and layout of inventory on their shelves. This software is used to conduct focus group-type experiences with shoppers, who provide feedback on alternative layouts of retail products. The software and focus groups are coveted by the retail industry, which is looking for any way to make the shopping experience more efficient and easier for consumers. In the transition to Company Y, Employee A transferred the voluminous code that made the virtual reality software operate.

But after Employee A resigned and joined Company Y, Employee A realized that there were lines of code, updates and patches that Employee A left behind at Company Z. With the blessing of Company Y, Employee A convinced a close former colleague, Employee B, at Company Z to resign and join Company Z. Employee B agreed to bring with him copies of the code, updates, and patches that Employee A needed but left behind.

After Company Z realized that Employees A and B improperly transferred the code, updates, and patches out of Company Z's computer systems, Company Z sent a cease-and-desist demand letter to Company Y, demanding among other things that Company Y preserve all relevant ESI. Company Z conducted a forensic analysis of its computer systems and the computer and email accounts used by Employee B. Based on this analysis, Company Z accused Employee B of improperly transferring internal engineering emails, code, updates, and patches – all ESI – from Company Z's computer systems, using a large-volume external hard drive, a flash drive and emails

sent to personal email accounts owned by Employees A and B. According to Company Z, this misconduct could give rise to causes of action against the Company Y for:

- aiding and abetting Employees A and B's breach of the restrictive covenants;
- tortious interference with restrictive covenants;
- violation of the Defend Trade Secrets Act;
- violation of the Computer Fraud and Abuse Act;
- violation of the Uniform Trade Secrets Act;
- unfair competition; and
- aiding and abetting breach of fiduciary duty

The cease-and-desist letter also includes a specific demand that Company Y obtain from Employees A and B copies of the misappropriated ESI, the external hard drive, the flash drive, and the personal emails containing Company Z's proprietary information.

C. Legal Background Of Preservation And Collection

With increasing frequency, courts are asked to determine whether employers have a legal duty to preserve and hold ESI residing on not just the employer's corporate computers but on personal external hard drives, mobile phones, tablet computers, and flash drives owned and used by employees. Where employees use their own computers and devices for work purposes, and electronic communications that are relevant to litigation can be found on the personal computers and devices, in some instances, employers have been required to preserve such communications, giving rise to some of the awkward situations mentioned above, where an employer must ask an employee to turn over a personal cell phone or emails in order to perfect a litigation hold.

Determining an employer's preservation responsibilities is complicated by several factors, the first of which is the Federal Rules of Civil Procedure. Amended twice in the past ten years to

help jurists, attorneys, and parties conduct electronic discovery, Rule 26(a) allows for the discovery of "documents, electronically stored information, and tangible things" in the responding party's "possession, custody, or control." Similarly, Rule 34(a) and Rule 45(a) obligate a party responding to a document request or subpoena to produce "documents, electronically stored information, and tangible things" in that party's "possession, custody, or control." Herein lies the problem: the Rules provide no guidance on what "possession, custody, or control" mean. The result is that the courts must interpret these words and give them meaning.

The meaning of "possession, custody, or control," provided by the courts has been inconsistent and lacking in meaningful guidance for in-house and outside counsel. The inconsistent interpretation and application of Rules 26, 34 and 45 in the litigation hold setting is troubling for employers because, as parties to litigation, they are responsible for preserving and producing information within their "possession, custody, or control" and face material consequences – including dismissal of a case, entry of default judgment, adverse inference jury instructions, monetary penalties, fee shifting, and other sanctions – for their failure to do so.

The lack of clarity from the Rules and the courts is compounded by innovation. The technologies and the functionality of electronic devices are constantly improving, and employers logically move to harness and leverage these innovations to help their businesses succeed. But one of the hidden, and underestimated costs, is the lack of a clear, real-time understanding of who, between and employer and an employee, actually "controls" data for purposes of preservation and production. The American workplace has become a Petri dish in which these issues have thrived.

The crux of the problem has less to do with "possession and custody," although these terms can create vexing uncertainty, and more to do with the definition of "control." Where, as

the two hypotheticals above demonstrate, an employer is faced with deciding whether it has a legal duty to preserve relevant ESI in the possession of an employee, three (3) different definitions of "control" have emerged from the case law: control exists when an employer has (1) the right or (2) practical ability to obtain the documents from an employee and (3) the employer's awareness of the employee's possession. How courts have interpreted "the right, authority, or practical ability to obtain the documents" has varied – unfortunately with different definitions from one federal circuit to another. Moreover, in some instances different courts within one circuit have applied different standards without any reconciliation of the application of the different definitions of "control."

1. An Employer Has Control Over ESI Where It Has The Legal Right To Obtain It From An Employee On Demand

Federal courts in the First, Third, Fourth, Sixth, Ninth and Eleventh Circuits have defined "control" as limited to situations in which a party has the legal right to obtain the communications or devices on demand.[1] The legal right to obtain ESI from an employee can come from an employment agreement, which requires an employee to return business files or records upon a reasonable demand. It also might come from workplace policies that require cooperation in

---

[1] The definition of legal right to obtain ESI can be found in *Mercy Catholic Med. Ctr. v. Thompson*, 380 F.3d 142, 160 (3d Cir. 2004); *Stream Companies, Inc. v. Windward Advertising, et al.*, No. 12-cv-4549, 2013 U.S. Dist. LEXIS 100319 (E.D. Pa., Jul. 17, 2013); *Pasley v. Caruso*, No. 10-cv-11805, 2013 WL 2149136, at *5 (E.D. Mich., May 16, 2013); In re Citric Acid Litig., 191 F.3d 1090, 1107 (9th Cir. 1999); *Siddiq v. Saudi Arabian Airlines Corp*., No. 6:11-cv-69-ORL, 2011 WL 6936485 (M.D. Fla., Dec. 7, 2011) (*citing Searock v. Stripling*, 736 F.2d 650, 653 (11th Cir. 1984)); *Vazquez-Fernandez v. Cambridge Coll., Inc.*, 269 F.R.D. 150, 164 (D.P.R. 2010); *Calzaturficio S.C.A.R.P.A. s.p.a v. Fabiano Shoe Co., Inc.*, 201 F.R.D. 33 (D. Mass. 2001); *Engel v. Town of Roseland*, No. 3:06-cv-430, 2007 WL 2903196, at *3 (N.D. Ind., Oct. 1, 2007); *Morningware, Inc. v. Hearthware Home Products, Inc.*, No. 09-C-4348, 2011 WL 4715189 (N.D. Ill., Oct 6, 2011); *U.S. v. Approx. $7,400 in U.S. Currency*, 274 F.R.D. 646, 647 (E.D. Wis. 2011); *Al Naomi v. Zaid*, 283 F.R.D. 639, 641 (D. Kan. 2012); *Ebersole v. Kline-Perry*, 85 Fed. R. Serv. 3d 1004 (E.D. Va. 2013) (control pertains to documents that one has a legal right to obtain on demand); *Beyer v. Medico Ins. Group,* No. CIV 09-5058, 2009 WL 736759 (D.S.D., Mar. 17, 2009).

workplace investigations; allow employees to use their own personal devices for work purposes; or define ESI that can be found on the employer's computers as the property of the employer.

2. *An Employer Has Control Over ESI That The Employer Has The Practical Ability To Obtain*

Federal courts in the Second, Fourth, Eighth, Tenth, Eleventh and District of Columbia Circuits have held that control includes devices and documents "to which a party has 'access and the practical ability to possess.'"[2] As The Sedona Conference has noted, Federal Rule of Evidence 34 does not require legal ownership or actual physical possession of the ESI and that the "practical ability" to obtain the ESI on demand is sufficient to establish control. This definition of control has implications in the employment setting, where a company could demand that an employee give the employer relevant ESI as part of a litigation hold and collection. The employee is then placed in a position where he or she might provide an employer with incriminating evidence and no meaningful ability to refuse without a risk of some adverse employment action. The potential for such a coercive outcome was the subject of criticism by The Sedona Conference.[3]

---

2 The practical ability to possess definition can be found in *Thai Lao Lignite (Thailand) Co., Ltd. v. Gov't of Lao People's Democratic Republic*, 924 F. Supp. 2d 508, 515 (S.D.N.Y. 2013); *Scherbakovsky v. Da Capo Al Fine, Ltd*., 490 F.3d 130, 138 (2d Cir. 2007); *D.J.'s Diamond Imports, LLC v. Brown*, No. WMN-11-2027, 2013 WL 1345082 (D. Md., Apr. 1, 2013); *Grayson v. Cathcart*, 2013 WL 1401617 (D.S.C., Apr. 8, 2013); *Lafleur v. Ean Holdings LLC*, No. 12-233, 2013 WL 2490613 (M.D. La., Jun. 10, 2013); *Anz Advanced Techs. V. Bush Hog, LLC,* No. Civ. A. 09-0028-KD-N, 2011 WL 814612 (S.D. Ala., Jan. 26, 2011); *Shell Global Solutions (US) Inc. v. RMS Eng'g, Inc.*, No. 09-cv-3778, 2011 WL 3418396 (S.D. Tex., Aug. 3, 2011); *New Alliance Bean & Grain Co. v. Anderson Commodities, Inc.*, No. 8:12-cv-197, 2013 WL 1869832 (D. Neb., May 2, 2013); *Handi-Craft Co. v. Action Trading, S.A.*, No. 02-cv-1731, 2003 WL 26098543 (E.D. Mo., Nov. 25, 2003); *Digital Vending Services Int'l, Inc. v. The University of Phoenix*, No. 2:09-cv-555, 2013 WL 311820 (E.D. Va., Oct. 3, 2013) (noting legal right and practical ability definitions); *Prokosch v. Catalina Lighting, Inc.,* 193 F.R.D. 633 (D. Minn. 2000) (same).

3 The Sedona Conference Commentary on Rule 34 and Rule 45, 17 Sedona. Conf. J. 1, 44 (2016).

3. Is An Employer's Awareness That Employees Are Using Personal Devices For Work Purposes Sufficient To Find Control?

At least two cases have found that an employer's awareness that its employees were using personal devices for work purposes gave rise to the employer's duty to preserve the ESI on the devices or the devices themselves. In *Puerto Rico Telephone Company, Inc., et al., v. San Juan Cable LLC*, No. 11-2135, 2013 WL 5533711 (D.P.R., Oct. 7, 2013), the Plaintiff contended that San Juan Cable spoliated evidence by failing to preserve relevant emails from the personal email accounts of three of its former officers who were not parties to the litigation. The court found sufficient evidence to establish the Defendant's failure to preserve relevant emails within its control (even though said emails were from the officers' personal email accounts) because the officers had used their accounts to manage the company for as long as seven years.

The court concluded the Defendant "presumably knew its managing officers used their personal email accounts to engage in company business, and thus its duty to preserve extended to those personal email accounts." Notably, no mention was made of the "legal right" or "practical ability" definitions mentioned in other cases. Instead, the "presumable knowledge" standard seems to suggest that employers could be expected to control any work communications, regardless of the device/network, used by their employees whenever the employer knows or should have known about such communications. Importantly, the Motion for Sanctions was denied without prejudice due to finding an absence of bad faith as well as a failure to demonstrate prejudice which, in part, is why the employer's "awareness" is an open question.

A similar result was reached in *Perez v. Shippers Transport Express, Inc.*, Case No. 2:13-CV-04255-BRO-PLA, 2014 WL 856201 (C.D. Cal., Jul. 8, 2014). In this wage and hour matter, a trucking and shipping company was investigated by the Department of Labor for its allegedly

unlawful wage and hour practices. One of the central issues in this matter was the timing when employer's driver-employees began work. The employer did not take custody of, image or preserve text messages from the personal cell phone of its dispatcher, who testified at his deposition that he regularly used his personal cell phone to text the drivers on their personal cell phones regarding their shifts and routes, particularly at the beginning of each day. Ultimately, the employer was sanctioned for failing to adequately preserve these text messages, which were relevant to the central issue of when the drivers began their work day.

III. Ethical Issues And The Privilege

The legal question of "control" of ESI and the employer's legal duty to preserve ESI that is in the possession of its employees also involves ethical issues and implicates the attorney-client privilege. There is significant discussion and important case law and ethics opinions around these two issues.

A. Litigation Hold Communications Are Protected By The Attorney-Client Privilege…Aren't They?

It is black-letter law that a communication between an attorney and his or her client in which legal advice is sought or provided is protected by the attorney-client privilege. Armed with this bedrock legal rule, many attorneys draft and provide litigation hold letters to their employer client with complete confidence that their litigation hold letters and memoranda are protected from litigation discovery and disclosure under the privilege. In some instances, this confidence is justified and, in other instances, it is misplaced.

The analytical starting point for identifying which litigation hold communications are privileged begins with differentiating between the different types of communications that are part of a proper litigation hold implementation process. First, there generally is a written

communication between outside counsel and in-house counsel or someone in management at the client-employer that provides legal advice regarding (1) the law of litigation holds, to the extent this is necessary, and (2) the steps needed to execute the legal hold necessary in the current matter.

In some instances, legal advice regarding the law of litigation holds is not necessary: some clients know this already; others do not know it but have experience in executing litigation holds and "know the drill." For such clients, a general explanation of the law of litigation holds might not be well received (and an invoice that contains a time entry for the drafting and editing of such a letter might not be well received either). But a letter to the client that identifies custodians, legal issues, documents and ESI that should be preserved, media that must be forensically imaged and the other critical steps needed to execute a legal hold tailored to the claims, allegations, investigations or legal process at issue is necessary and protected by the attorney-client privilege.

When drafted skillfully, this legal advice also will enclose a proposed memorandum (or other document) that the client should review and revise, if needed, that will constitute the internal litigation hold document itself. Then, after in-house counsel has approved of this internal hold memorandum, it should be circulated to the relevant custodians, executives and Information Technology administrators at the client-employer.

This internal memorandum, unlike the initial letter to the client's in-house counsel or executive that proposed the memorandum, should be drafted as though it is not protected by the attorney-client privilege. Whether this memorandum bears the moniker "Attorney-Client Communication" is up to the attorneys involved in drafting the memorandum. But recent case law has suggested that this internal hold memorandum is not legal advice. It is a managerial

directive to employees, which is the result of legal advice (1) that the client should implement a litigation hold and (2) how such a hold should be designed and executed.

A thoughtful discussion of this distinction was the subject of a federal district court's opinion in *In Re Blue Cross Blue Shield Antitrust Litig'n,* No. 2:13-CV0-20000-RDP, 2013 WL 432298, at *7 (N.D. Ala., Sept. 2, 2015), wherein the court held that the internal litigation memoranda "were instructions from the corporation to its employees, not a confidential communication between counsel and the corporate client," even if counsel were involved in the drafting of this internal hold memorandum. Their "circulation to corporate employees was nothing more than giving managerial instructions, which are not privileged." Likening the internal hold memorandum to an employee policy manual, the court noted that the drafts circulated between outside counsel and the company might be privileged and work product but the final document is not. *Id.* Thus, outside counsel and in-house counsel need to be aware that there is support for the proposition that the internal hold memorandum is not a communication protected by the privilege or work product doctrine, even if outside and in-house counsel prepared it and the memorandum bears the label "Attorney-Client Communication."

While this distinction between the (1) legal advice that results in the client's internal hold memorandum and (2) the memorandum itself has the benefit of superficial clarity, and is consistent with how we conceptualize the role of privileged communications in the preparation and finalization of other employment documents, the *Blue Cross Blue Shield* analysis is not the last word on this issue. In fact, several courts have held that the initial legal advice from outside counsel to the corporate client regarding the litigation hold itself could be discoverable even though it was a privileged communication and work product.

This line of cases was discussed in *Major Tours v. Colorel,* Civ. No. 05-3091, 2009 WL 2413631 (D.N.J., Aug. 4, 2009), where the district court held that the initial legal advice in the hold letter was discoverable because there was a prima facie showing of spoliation of evidence. Central to this holding, the court reasoned that a persuasive showing of spoliation reflected a breakdown in the litigation hold, noting that other courts had reached a similar conclusion. This, in turn, meant that there might be a failure in the underlying legal advice itself, which justified setting aside the protection of the privilege to make the hold letters discoverable.

The precedential value and platform provided by *Blue Cross Blue Shield* and *Major Tours* is sturdy and actionable for outside and in-house counsel. There are several takeaways. First, counsel should draft more than one litigation-hold communication. There should be a writing in which outside counsel advises the corporate employer-client on the hold and then a proposed internal memorandum which ultimately becomes an internal managerial directive that is not protected by the privilege or work product doctrine. This would be consistent with this jurisprudence and the best practices in litigation hold and preservation.

Moreover, a record that reflects more than one writing to arrive at the proper litigation hold has utility on a rainy day: there are a disturbing number of cases that address the consequences for failing to provide any written guidance on litigation hold and preservation. Where outside and in-house counsel have exchanged more than one writing in their efforts to design and implement the appropriate litigation hold, a court would be less likely to find that your client or company intended to deprive a party of evidence under Fed. R. Civ. P. 37.

B. Ethics Opinions Regarding The Preservation of ESI

In the few years, several states and bar associations have revised their Rules of Professional Conduct and issued ethics opinions to underscore that attorneys must improve their

understanding of how information technology works. The purpose of these changes is to fortify the existing ethics rules and Rules of Professional Conduct rather than supplant them. The rationale is straight-forward: if confidential information essential to the representation of a client is written, transmitted or stored using a technology that could jeopardize its confidentiality, then the attorney must be sufficiently familiar with the operation and functionality of the technology to make sure that the confidential information is protected and the risk of disclosure is avoided.

For this reason, there is a movement to amend Rules of Professional Conduct to require attorneys to be knowledgeable and facile with the applications, tools, media, electronic devices and software used to store and transmit a client's confidential information. Leading changes to Rules of Professional Conduct and ethics opinions have been promulgated in several jurisdictions, including:

- The Rules of Professional Conduct in:
    - Pennsylvania Rules of Professional Conduct (2013)
        - Rule 1.1, Competence
        - Rule 1.6 Confidentiality of Information
        - Rule 5.3 Responsibilities Regarding Nonlawyer Assistance
    - The State Bar of California Standing Committee on Professional Responsibility and Conduct (Formal Opinion No. 2015-193)
        - Rules 3-100 and 3-110 of the Rules of Professional Conduct of the State Bar of California
    - Kentucky Bar Association Formal Ethics Opinion E-446 (July 20, 2018)

- Fed. R. Civ. P. 37(e)'s advisory committee note to the 2015 amendment: "It is important that counsel become familiar with their clients' information systems and digital data" in the discovery of ESI.